International Journal of Law
www.lawjournals.org
ISSN: 2455-2194
Received: 08-11-2025, Accepted: 07-12-2025, Published: 22-12-2025
Volume 11, Issue 12, 2025, Page No. 148-151

Deepfakes in India: Legal provisons, challenges and way forward

Dr. Jyoti Panchal Mistri[1], Kavita Sharma[2]
[1] Head and Department of Law, Sage University, Indore, India
[2] Sage University, Indore, India

Abstract
Technological Advancement is both bane and bliss. As the society is advancing the mode of crime is also advancing. There are wide variety of cyber crimes which are committed by use of internet and artificial intelligence. One such very popular cyber crime is circulation of deepfakes. Deepfakes in simple terms refers to digital alteartion of a person's face or body or voice in a video, image etc so they may appear to be someone else, typically used maliciously or to spread false information. By enabling highly realistic manipulation of audio, images, and video, deepfakes challenge traditional notions of authenticity and trust.

Keywords: Deepfakes, legal provisions, challenges

Introduction
Deepfake is combination of deep learning and fake content. It involves swapping of a face from a person to a targeted person in a video and make the face expressing similar to targeted person and act like targeted person saying those words that actually said by another person. This process of face swapping specially on image and video or manipulation of facial expression is called as Deepfake method. Deepfake is an alarming concern because it directly violates the privacy of person and can also be harmful to the reputation of victim person. The popular use of social media has attributed to growth of deepfakes because it serves as a channel where such content is posted and viewed on large scale. In reference to India, we do have laws to deal with such modern crime but an equivalently advanced technology is required to identify the origination of crime. Due to technical difficulties, it becomes difficult to prosecute. Artificial intelligence is itself in its evolving era so are the crimes evolving. An attempt is made to understand the concept its effect, existing legal provisions and challenges relating to deepfakes.

Hypothesis
Laws in India are not sufficient enough to deal with deepfake cases.

Research Questions
1. What are deepfakes?
2. What are effects of deepfakes?
3. What are legal provisions prevailing in India for punishing deepfakes?
4. What are legal challenges in dealing with deepfake cases?
5. Whether there is need of some suggestive measures towards combating deepfakes?

Material & Methods
- This research is doctrinal legal research. The main focus is to understand concept of deepfakes, the present legal provisions and judicial response to it alongwith suitable suggestions.
- The material used includes law bare act, commentaries, cited case laws, online sources like e-journals, e-websites, e-articles.

Result
- It can be laid that deepfake is digital alteration of face, body, or voice for malicous purpose or to spread misinformation
- The effect of deepfakes includes threat to privacy, financial harm etc.
- After analysing all the legal provisions it can be laid that we do have certain legal provisions indirectly dealing with deepfakes but we do need to have explicit statue on this subject matter.
- The legal challenges include jurisdiction bar, lack of evidence, prolong investigation process due to lack of digital and forensic infrastructure.
- After analysing legal provisions and understanding challenges some suggestive measures like promoting digital awareness, advancemnt in IT technology etc are some of suggestive measures laid for combating menace of deepfakes.

Discussion
Concept of deepfake
The term deepfake is combination of two words deep i.e. deep learning technology a type of machine learning, and fake, which means that the content thus produced using the artificial intelligence is not real. It involves two algorithms. The first algorithm involves use of artificial intelligence system to study patterns in facial expressions, voice characteristics, speech patterns and visual features. Then second algorithm involves machine learning algorithms, particularly GAN technology (Generative Adversarial Networks), it learns to generate new content that mimics the original person's appearance or voice. The deepfake appears to be so real as the original one as it becomes very difficult to differentiate it with the original content.

Types of Deepfakes
Video Deepfakes
1. **Face Swapping:** The process of superimposing one person's face onto another person's body in a video to create a realistic, though fake, visual is face swapping.

2. **Lip Syncing:** It refers to Synchronizing a person's mouth movements to match a new, fabricated audio

track. This is often combined with voice cloning for a complete and convincing manipulation

3. **Attribute Manipulation:** This process involves changing or altering of one's specific features of a face, such as changing hair color, age, or gender, or adding things like glasses.

Audio Deepfakes

1. **Voice cloning:** The process involves Creation of a synthetic, realistic-sounding voice of a person from a limited number of samples. This is popular used in scams to impersonate executives or for other audio-only applications.

2. **Lip syncing with audio overlay:** It involves combinin g a video deepfake with cloned or manipulated audio to make it appear as if the person in the video is saying something they never actually said.

3. **Text-based deepfakes Written content generation:** It refers to use of artificial intelligence to create fake comments, social media posts, or reviews that imitate a person's writing style, tone, and opinions.

Effects of Deepfakes

- **Threat to privacy:** It is direct threat to privacy and may also lead to loss of reputation of person.
- **Emotional Distress:** Circulation of deepfakes may also lead to emotional distress for victim and in severe cases may also lead to suicide.
- **Spreading of misinformation:** In relation to politics such deepfakes are often used to Spread fake news, conspiracy theories, or fabricated statements from politicians to manipulate public opinion.
- **Threat to Democracy:** It also possess threat to democracy by threatening election integrity and stability by creating chaos and confusion.
- **Financial Fraud:** Deepfakes also includes impersonating executives to authorize fraudulent transactions or tricking customers leading to huge financial scam.

Legal Provisions for combating deepfakes

India does not have explicit legislation for deepfakes but there are certain other laws which indirectly deals with punishment for deepfakes.

Bhartiya Nyaya Sanhita,2023

1. **Section 111**
   It provides punishment for organised crime which includes cyber crime. The maximum punishment is death penalty under certain circumstances in this provision.

2. **Section 319**
   It provides punishment for cheating by personation which includes deceiving someone by pretending to be another person (real, dead, or imaginary) to gain an unfair advantage, punishable by up to 5 years of imprisonment or fine, or both.

3. **Section 356**
   This section provides punishment for defamation. If content of deepfake video is of such nature that it damages a person's reputation, it may amount to criminal defamation, punishable with up to two years of imprisonment, or a fine or both.

Information Technology Act,2000

1. **Section 66 C**
   This section deals with identity theft, providing punishment for anyone who fraudulently or dishonestly uses another person's electronic signature, password, or unique identification (like a credit card detail or login) with imprisonment up to three years and a fine up to ₹1 lakh or both.

2. **Section 66 D**
   It deals with cheating by impersonation using computer resources, like pretending to be someone else online to deceive others, punishable by imprisonment up to 3 years and a fine up to ₹1 lakh.

3. **Section 67**
   It provides for punishment publishing or transmission of "obscene" material in electronic form. For first-time offenders' punishment is imprisonment which may extend to three years and a fine may extend upto five lakhs or both while subsequent convictions carry a punishment is imprisonment which may extend to five years and a fine of which can be upto ten lakhs.

Information Technology Rules,2021

1. **Rule 3(1)(b)(vii):** It provides for mandate for social media intermediaries to ensure that the users of their platform do not host ana y content which impersonates another person**.**

2. **Rule 3(2)(b):** It requires if any complaint is received then such content must be taken down within 24 hours of receipt of a complaint against such content.

Digital Personal Data Protection Act,2023

1. **Section 6**
   It basically deals with consent that consent of data principal must be free, specific, informed, unconditional, and unambiguous. It requiring a clear affirmative action from the Data Principal (individual) for processing their data for a specified purpose, prohibiting bundled consents, and allowing for easy withdrawal of consent, making consent the cornerstone of lawful data processing in India.

Regulatory Advisory

1. **November 2023 Advisory**
   Ministry of Electronics and Information Technology mandated platforms to remove deepfakes within 36 hours, framing them as rights violation.

2. **March 2024 Advisory**
   Ministry of Electronics and Information Technology issued advisory that every intermediary and platforms must embed persistent labels/metadata in synthetic content for originator tracing, with compliance reports within 15 days. This aligns with privacy by design, advocating differential privacy against re-identification.

3. **ECI Directives (May 2024)**
   ECI in order to ensure fair election issued directives that political parties must remove deepfake posts within 3 hours during MCC enforcement, prohibiting AI misuse for misinformation.

4. **Constitution of India**
   Article 21 provides for right to life and personal liberty. Right to privacy is facet of right to life and personal liberty. Right to personality right is part of right to privacy under which person can approach court for protection of his/her right to privacy.

Legal Challenges in deepfake cases

It is not easy to prosecute deepfake cases due to several reasons. Lack of proper statue dealing with such issue is one of the major causes of concern. At present punishment for deepfakes can be given under certain provisions of Bhartiya Nyaya Sanhita,2023 and Information Technology Act,2000 but there is no specific law specifically dealing with it.

The deepfake technology is becoming so advance day by day that it is becoming difficult to flag or both humans and automated systems to distinguish fake from authentic content. Having no standardized deepfake detection methodologies or qualified forensic experts across Indian labs. difficult to authenticate digital evidence in court, which is a critical step under the Bharatiya Sakshya Adhiniyam, 2023.

VPNs i.e. virtual private network enable prepators to operate anonymously making it extremely difficult for law enforcement to trace the origin of the content and identify the creators. At times it becomes difficult to find the origin of content leading to delay in investigation process.

Also, deepfakes is a cyber crime having no restrain of geographical boundaries. Deepfakes can be created in one country and disseminated globally. If there is no global treaty or strong international cooperation, by home country i.e. India then Indian courts have limited power to compel foreign platforms or jurisdictions to remove content or share perpetrator details.

Crimes are result of ignorance or lack of awareness of people as users often do not question the authenticity of content shared on social media but keep on sharing it leading to increase in such crimes. There should be some directive statue for spreading awareness about deepfakes.

Even judges are not familiar with deepfake cases. Jurisdiction issues, lack of forensic techniques act as hinder in providing justice in such cases.

Judicial Response on Deepfakes

1. **Gaurav Bhatia v. Naveen Kumar & Ors:** In this case injunction was granted by Delhi High Court against circulation of deepfake videos defaming lawyer Gaurav Bhatia, recognizing the irreparable harm to reputation and potential for future misuse, emphasizing personality rights.

2. **National Stock Exchange v. Meta Platforms & Ors.:** The Bombay High Court ordered meta (facebook and whatsApp) to remove deepfake video of NSE chairman Ashishkumar Chauhan which were misleading investors with false stock tips and urging them to join scam WhatsApp groups.

3. **Suniel Shetty v. John Doe:** Bombay High Court granted interim injunction, ex-parte injunction against digital misuse and personality rights infringement thereby protecting personality right under Article 21.

4. **Karan Johar v Ashok Kumar, John Doe and Ors:** Famous director Karan Johar approached Delhi High Court for protection of his personality rights. Injunction was issued by Delhi High Court in favour of Karan Johar restraining misuse of Karan Johar's persona through artificial intelligence/deepfakes asserting celebrity rights against digital impersonation.

Way Forward

Deepfakes is a major issue in cyberspace which is great threat to person's privacy, autonomy for organisations and society at large. However, there are few suggestions to face this menace.

- Having explicit legislation is very important to combat deepfakes. As we do have rules and law but they do not directly deal with the issue of deepfake. It is high time we need to have some penal statute on deepfakes.
- It should be made mandatory for AI generated videos to have watermark as it will facilitate effective detection and attribution. Watermark enables to know about content's origin and ownership, serving various purposes. It aids by clarifying the content's creator or source, especially when shared in different contexts.
- India is advancing in technology but we still lack digital infrastructure in regards to having apps or software which directly flags up such deepfake content. If we have such app or software then it will become easy to detect and eliminate such cotent.
- Digital awareness is very important to combat deepfakes as if people; s awareness about such content will discourage its circulation leading to less creation of deepfakes. Also, if people will be aware that they can report such content then it will help in punishing the wrong doers. Every person is using social media in some manner now a days but it is very important to be digitally aware to safeguard oneself and society. Awareness can be spread through television advertisements, awareness programmes in schools and colleges etc.

Conclusion

It is to be concluded that India does have legal provisions that indirectly deals with deepfakes but they are not sufficent enough to combat this menace. There is a need to have explicit penal statute dealing with the issue of deepfakes. Also, we need to have some digital infrastructure by way of apps or software which helps in tracing origin of deepfakes and helping in identifying its origin. Digital awareness therefore plays a crucial part to be safeguarded against this menace and to protect one's right and autonomy and to protect society.

References

1. The Constitution of India, 1950.
2. Bhartiya Nyay Sanhita, 2023.
3. Information Technology Act, 2000.
4. Digital Personal Data Protection Act, 2023.
5. Gaurav Bhatia v. Naveen Kumar Ors. CS(OS) 274/2024.

6. National Stock Exchange v. Meta Platforms Ors: Interim Application (L) No. 21456 of 2024 in COM IPR Suit (L) No. 21111 of 2024.
7. Suniel Shetty v. John Doe 2025 SCC OnLine Bom 3918
8. Karan Johar v Ashok Kumar, John Doe and Ors CS(COMM) 974/2025.
9. Miss Rinkey, Krishna S. Tiwari, Cybersecurity, AI, and the Law: Legal Tools for Digital Threats, Issue, 2025, 15-15
10. Asifa Mustafa Khan, Regulating Deepfakes in India: A legal and ethical analysis of misinformationin the age of AI, VOL VII Issue III
11. S Nivedha, Samanvitha Mural, Deepfakes in India: Unraveling India's Legaislative uncertainity and jurisdictional dilemma
12. https://negd.gov.in/blog/deepfakes-in-india-legal-landscape-judicial-responses-and-a-practical-playbook-for-enforcement/
13. https://www.drishtiias.com/daily-updates/daily-news-editorials/deepfakes-opportunities-threats-and-regulation