Page 650 - 655 **DOI:** *https://doij.org/10.10000/IJLMH.1110449*

INTERNATIONAL JOURNAL OF LAW MANAGEMENT & HUMANITIES

[ISSN 2581-5369]

Volume 8 | Issue 4

2025

Consent, Fabrication, and Proof: The Legal Dilemma of Deepfakes in the Indian Judicial System

AISHWARYA MUDGADKAR[1]

ABSTRACT

The rise of AI-powered deepfakes is becoming a big matter in India. Deepfakes tend to malign reputations, spread misinformation, or sometimes are used for blackmail or fraud. The Indian system is struggling with these new challenges, especially with consent issues, identification of fakes, and reliable proof being an accepted standard in courts. With the new proposed statutes of Bharatiya Nyaya Sanhita (BNS), Bharatiya Nagarik Suraksha Sanhita (BNSS), and Bharatiya Sakshya Adhiniyam (BSA), it looks like India is trying to take a stand. This paper explains deepfakes in layperson's language, shows how deepfake technology is being misused, examines new legal provisions, and probes more actions that can be taken to shield humankind from this dangerous technology.

Keywords: *Deepfakes, Consent, Fabrication, Proof, Bharatiya Nyaya Sanhita (BNS), Bharatiya Nagarik Suraksha Sanhita (BNSS), Bharatiya Sakshya Adhiniyam (BSA), Cybercrime, Digital Evidence, Defamation, Indian Law, Privacy*

I. INTRODUCTION

Technology keeps on changing and sometimes no laws exist to curb its developments. Deepfakes are a typical example; a deepfake is a video, audio clip, or image that has been manipulated with AI to make it look and sound real while it is fake. For example, a deepfake video can show someone saying or doing some For instance, a deepfake video could depict someone saying or doing anything they never actually did.

In India, there have been instances of deepfakes being utilized to produce bogus videos of wellknown people, politicians, and everyday citizens. These films have the potential to tarnish reputations, propagate falsehoods, and even result in blackmail or harassment.

The Indian legal system has a significant challenge to overcome: In what way can a video's authenticity be determined? If someone uses someone's likeness or voice without their consent, how can you safeguard their rights? What laws can be used to hold accountable those who produce and distribute deepfakes?

[1] Author is a Student at MP Law College, Aurangabad, Maharashtra, India.

 [ISSN 2581-5369]

India is attempting to solve these challenges via the new legislation (BNS, BNSS, and BSA). However, is it sufficient? The problems will be described in clear, plain language in this study, making it easy for readers to grasp the risks involved.

What exactly are deepfakes, and why are they so hazardous? What Exactly is a Deepfake?

Digital material that has been altered by artificial intelligence is known as a deepfake (such as a video, picture, or audio). The AI is capable of switching faces, changing voices, and even giving the impression that someone is saying something they never did. The unique software programs known as "deep learning" algorithms are used to generate deepfakes.

II. THE MAKING OF DEEPFAKES

A person uses a computer program to gather a large number of images or recordings of someone's face or voice in order to create a deepfake. After that, the program "learns" what that person looks and sounds like. The AI is able to generate new audio and video pieces that replicate the appearance and voice of the actual individual, even if they are entirely fictitious, after enough practice.

What Makes Deepfakes Risky?

- **Nonconsensual pornography:** Creating fictitious sexual videos of individuals without their consent.
- **Political manipulation:** making up bogus videos of politicians saying or doing things that they never did.
- **Defamation:** harming someone's reputation by creating fictitious audio or videos.
- **Scams and fraud:** using deception, such as a phony voice or face, to persuade someone to give up their money or personal data.
- **Cyberbullying:** Treating or humiliating others online.

It's quite difficult for the average person to distinguish between a deepfake and something real since they seem so authentic. This makes deepfakes a potent weapon for lawbreakers and troublemakers.

III. LEGAL PROBLEMS: PROOF, CONSENT, AND FABRICATION CONSENT

Giving permission is what consent entails. Consent in the context of deepfakes refers to whether the individual whose face or voice is being used gave their permission for it. The majority of deepfakes are created without the subject's permission. A significant breach of privacy, this can have psychological and emotional consequences.

 [ISSN 2581-5369]

For instance, someone's life might be destroyed if they create a deepfake video of a woman and post it online without her consent. She might experience mental anguish, lose her job, or be subject to harassment. People should be shielded from this kind of exploitation by the law.

Production

Manufacturing is the process of creating something that isn't real. Digital fabrication includes deepfakes. They are capable of:

- Assume someone's identity by pretending to be them.
- Disseminate lies (misinformation).
- Defamation is the act of hurting someone's reputation.

Because deepfakes are considerably harder to spot, they differ from conventional forgery. A handwriting expert can verify a fake signature, but a deepfake video can trick even the most seasoned detectives.

Evidence

Demonstrating evidence in court is what proof is all about. It might be difficult to provide evidence in deepfake cases. What evidence can you use to demonstrate that a video is fake?

How can you demonstrate that someone didn't provide consent? Although the Indian Evidence Act and the new Bharatiya Sakshya Adhiniyam (BSA) contain provisions for electronic evidence, deepfakes are now so sophisticated that they can fool even the most experienced observers.

The court requires trustworthy methods for determining whether a video or audio is genuine or counterfeit. The Indian judicial system faces a significant challenge.

Indian Law and Deepfakes: Old and New Regulations

Ancient Laws

Prior to the new legislation, India relied on the Indian Penal Code of 1860 (IPC) and the Information Technology Act of 2000 (IT Act) to address cybercrimes. The following were a few significant parts:

- Identity theft is punished under Section 66C of the IT Act.
- Cheating by using another person's identity is punishable under Section 66D of the IT Act.
- Punishes the posting of obscene content under Section 67 of the IT Act.

 [ISSN 2581-5369]

- The act of defamation is punishable under Section 499 of the IPC.

However, these regulations did not take deepfakes into account. They make no mention of artificial intelligence or manufactured media. This made it difficult for police and judges to employ them in deepfake cases.

New Legislation: BSA, BNSS, and BNS

- To replace the previous criminal legislation, India enacted three new laws in 2023:
- The IPC is replaced by the Bharatiya Nyaya Sanhita (BNS).
- The Code of Criminal Procedure is replaced by the Bharatiya Nagarik Suraksha Sanhita (BNSS).
- The Indian Evidence Act is replaced by the Bharatiya Sakshya Adhiniyam (BSA).

IV. DIFFICULTIES IN ENFORCING THE LAW

Despite the new regulations, numerous obstacles remain:

1. **There Is No Clear Definition:** The term "deepfake" is not defined in Indian legislation. It becomes difficult to tell whether a video has been edited or is a deepfake. What constitutes a deepfake needs to be clearly defined by the statute.

2. Technical Issues: Deepfakes can only be detected by specialists utilizing sophisticated computer technology. Most courts and police stations lack these resources. Even professionals can be duped by really excellent deepfakes.

3. Anonymity and Jurisdiction: The location and identity of deepfake makers can be concealed. Since they may conduct business from other nations, Indian police have a hard time apprehending them.

4. Rate of Propagation: Deepfakes have the potential to become popular on social media in a matter of minutes. The harm has already been done by the time the authorities act.

5. Establishing Consent: It is challenging to determine whether or not the individual gave consent to nonconsensual deepfakes. It's frequently the victim's responsibility to demonstrate that they are not guilty.

6. Significant Instances and Judicial Response: The risks of deepfakes are now being recognized by Indian courts. Some notable instances and events are:

7. Public Interest Litigation (PIL): To urge the government to regulate deepfakes, a number of public interest litigations have been filed. For example, after a phony video of him

went viral, journalist Rajat Sharma filed a public interest litigation (PIL). The Delhi High Court requested the government to consider creating legislation for deepfakes and respond.

8. **Cases Involving Privacy and Defamation:** Individuals who distribute bogus movies have been prosecuted under defamation laws by the courts. However, it is still challenging to identify and punish the initial authors of deepfakes.

9. **Necessity for Professional Proof:** Digital forensic specialists are frequently used by courts to determine if a video is genuine. However, the technology is constantly evolving, and there are not enough specialists.

V. GLOBAL PERSPECTIVE

The issue of deepfakes affects the entire planet. Other nations are likewise having trouble managing them:

- **United States:** Some states have enacted laws addressing election interference and deepfake pornography.
- **European Union**: The EU is developing the Artificial Intelligence Act, which would outlaw dangerous applications of AI, such as deepfakes.
- **China**: Has rigorous legislation mandating that AI-generated material be identified on platforms.

Solutions and Recommendations for the Future

1. **Explicitly stated legal definitions:** Legislators should precisely define what a deepfake is and what actions are unlawful. This will facilitate the law's more efficient application by law enforcement and the judicial system.

2. **Watermarking and Required Disclosure:** All AI-generated material should be labeled or watermarked on websites and social media sites. People will be better able to recognize deepfakes and lessen damage as a result.

3. **Improved Forensic Instruments:** The government should spend money on cutting-edge digital forensic tools and provide more training for professionals in identifying deepfakes.

4. **International Collaboration:** India should collaborate with other nations in order to identify and punish criminals since deepfake producers may be located anywhere in the globe.

5. **Increasing Public Knowledge:** Individuals should be taught about deepfakes and how to recognize them. Media campaigns, universities, and schools may all help raise awareness.

 [ISSN 2581-5369]

6. **Rapid Removal and Victim Support:** A quick procedure to eliminate dangerous deepfakes from the internet should be established, along with support for victims, such as legal assistance and counselling.

VI. CONCLUSION

Deepfakes pose a significant risk to India's privacy, reputation, and public confidence. Although the new laws (BNS, BNSS, and BSA) are a nice beginning, more needs to be done. In order to combat the risks of deepfakes, everyone the government, the courts, the police, and the public must collaborate, and the law must stay current with technology.

To safeguard its citizens from the harm caused by deepfakes, India requires explicit definitions, rigorous enforcement, improved technology, and worldwide collaboration. Only then can the judicial system in the digital era actually protect consent, guard against fabrication, and guarantee trustworthy evidence.

*****

 [ISSN 2581-5369]