Indian Journal of Law
ISSN: 3048-4936 | Vol. 3 Issue 2 | Mar– Apr 2025 | Peer Reviewed & Refereed

Deepfakes and Misinformation: Legal Remedies and Legislative Gaps

Abhay Jain
Research Scholar
New Delhi.

Published: 18/04/2025 * Corresponding author

How to Cite this Article:
Jain, A. (2025). Deepfakes and Misinformation: Legal Remedies and Legislative Gaps. *Indian Journal of Law*, 3(2), 23-28.
DOI: https://doi.org/10.36676/ijl.v3.i2.86

Abstract
The exponential rise of deepfake technology—synthetic media generated using artificial intelligence—has significantly transformed the digital information landscape. While it opens new avenues for creativity and innovation, it also poses severe challenges in terms of misinformation, defamation, identity theft, political manipulation, and cybersecurity. In India, the legal framework remains inadequate to address the unique threats posed by deepfakes and associated misinformation. This paper investigates the technological underpinnings of deepfakes, their socio-legal implications, and the current legal remedies available in India and comparative jurisdictions. It also identifies key legislative gaps and proposes reforms aimed at establishing a rights-based, technologically robust legal response to deepfakes in the digital era.
Keywords: Deepfakes, Artificial Intelligence, Misinformation, IT Act, IPC, Defamation, Legislative Gaps, Privacy, Freedom of Speech.

1. Introduction
In an age driven by digital content and social media, the line between truth and falsehood is increasingly blurred. One of the most dangerous manifestations of this phenomenon is the emergence of deepfakes—hyper-realistic videos, images, or audio created using generative adversarial networks (GANs) and other artificial intelligence (AI) technologies. Deepfakes can mimic a person's likeness with such accuracy that they often deceive even the most discerning viewers.

While the technology has legitimate uses in education, film, and accessibility, it is increasingly weaponized to spread fake news, harass individuals, manipulate elections, and undermine democratic institutions. Deepfakes represent not just a technological challenge, but a legal and ethical crisis. In India, there is no specific legislation addressing deepfakes, and existing laws under the Information Technology Act, 2000 and the Indian Penal Code, 1860, offer only fragmented remedies.

This paper critically examines the legal remedies available for combating deepfakes and misinformation in India, compares them with global best practices, and proposes a legislative roadmap for regulating AI-driven synthetic media.

2. Understanding Deepfakes and Misinformation

2.1. What Are Deepfakes?

Deepfakes are synthetic media in which a person in an existing image or video is replaced with someone else's likeness using machine learning algorithms, primarily GANs. These are capable of producing hyper-realistic simulations that are hard to detect without forensic tools.

2.2. Types of Deepfakes

Video Deepfakes: Often used for fake political statements or pornography.
Audio Deepfakes: Impersonating voices for fraud or manipulation.
Image Deepfakes: Used for fake social media profiles or revenge pornography.
Text-based Deepfakes: Generated using language models to create fake news or statements.

2.3. The Misinformation Ecosystem

Misinformation refers to false or misleading information spread regardless of intent. Deepfakes are a powerful tool in the misinformation ecosystem as they erode trust in digital media and are used for:
Electoral interference
Harassment and cyberbullying
Defamation and extortion
Market manipulation

3. Legal Framework in India

3.1. Information Technology Act, 2000

Section 66E: Punishes violation of privacy by capturing, publishing, or transmitting images of a person’s private parts without consent.
Section 67 & 67A: Penalizes publishing or transmitting obscene material or sexually explicit content electronically.
Section 69A: Allows the government to block public access to information for national security or public order.
These provisions are not tailored to AI-generated content and lack clarity regarding consent, manipulation, and accountability in deepfakes.

3.2. Indian Penal Code, 1860

Section 499 & 500: Addresses defamation through spoken or published words.
Section 292: Penalizes obscenity.
Section 419 & 420: Deal with impersonation and cheating.
Section 463-469: Address forgery and falsification.

These sections can be invoked in case of identity theft or reputational harm via deepfakes, but lack specificity for AI-based falsifications.

3.3. Personal Data Protection Bill / Digital Personal Data Protection Act, 2023

India's new DPDPA focuses on data consent and privacy but does not specifically address manipulated or synthetic content, leaving a critical gap in regulating non-consensual digital impersonation.

4. Judicial Interpretation and Legal Remedies

4.1. Right to Privacy (Puttaswamy v. Union of India, 2017)

The Supreme Court declared privacy a fundamental right, encompassing informational privacy and bodily integrity. Deepfakes, particularly non-consensual pornography, directly violate this right. However, the absence of specific legislation limits enforceability.

4.2. Vishaka Guidelines and Sexual Harassment

Deepfake pornography involving women is increasingly being used for cyberbullying. While IPC Sections and the IT Act address explicit content, the burden of proof and anonymity of perpetrators make prosecution difficult.

4.3. No Right to Be Forgotten (RTBF) Yet Recognized

Unlike the EU, India does not have an explicit "right to be forgotten," which is crucial for victims of deepfake attacks who seek permanent removal of manipulated content.

5. Comparative Legal Approaches

5.1. United States

The U.S. has no federal law on deepfakes but several states (e.g., California, Texas, Virginia) have enacted laws to penalize:

Deepfakes in elections

Non-consensual pornographic deepfakes

PROTECT Elections Act and DEEPFAKES Accountability Act are proposed bills to establish criminal liability and watermarking.

5.2. European Union

The GDPR offers some protections through the right to be forgotten, data portability, and consent requirements. The EU's AI Act (under negotiation) classifies deepfakes as high-risk AI applications, proposing strict transparency obligations.

5.3. China

China passed regulations in 2022 mandating that deepfake content be labeled and disclosed, holding platforms accountable for distribution and origin tracing.

6. Legislative Gaps in India

6.1. Lack of Definition

There is no legal definition of "deepfake" or "synthetic media" in Indian law. This hampers enforcement and accountability.

6.2. Consent and Harm

The IT Act does not address impersonation using AI, and there is no mechanism for victims to demand takedown or seek compensation.

6.3. Platform Liability

Current laws provide safe harbor to intermediaries under Section 79 of the IT Act. However, with the advent of deepfakes, there's a need to redefine intermediary responsibilities and encourage proactive content moderation.

6.4. Investigative Challenges

Due to encryption, anonymous accounts, and lack of technical expertise, law enforcement struggles to trace the creators of deepfakes.

7. Role of Intermediaries and Social Media Guidelines

The Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021 introduced:

Mandatory grievance officers

24-hour takedown timelines

Traceability requirements

However, these rules are challenged on grounds of free speech and do not explicitly cover synthetic media or AI manipulation.

8. Ethical and Human Rights Considerations

Deepfakes raise ethical dilemmas concerning:

Consent and bodily autonomy

Freedom of expression vs misinformation

Gendered violence and sexual exploitation

Right to reputation under Article 21

Legislation must balance innovation with accountability, ensuring free speech is not unduly curbed, but victims are adequately protected.

9. Policy Recommendations

Define Deepfakes in Law: Include legal definitions under the IT Act or DPDPA, distinguishing harmful from benign applications.

Criminalize Malicious Use: Introduce penal provisions for deepfake creation/distribution without consent, especially in sexual and political contexts.

Regulate Platforms: Mandate watermarking, origin tracing, and AI detection tools for social media platforms.

Establish RTBF Mechanism: Recognize the right to be forgotten for victims of synthetic defamation or harassment.
Awareness Campaigns: Launch digital literacy programs to help users identify manipulated content.
Encourage Ethical AI Development: Support transparency and accountability in generative AI development through public-private frameworks.
Cyber Forensics Capacity Building: Invest in training and equipping cybercrime units to handle AI-based offences.

10. Conclusion

Deepfakes and misinformation represent a new frontier in digital risk. Their ability to erode public trust, violate privacy, and disrupt democratic processes makes them a grave threat. While existing legal provisions in India offer some degree of protection, they are inadequate to handle the complexity of AI-generated threats.
A multidisciplinary and multi-stakeholder approach is essential. India must evolve its cyber laws to define and address synthetic media, ensure platform accountability, and empower individuals with robust legal remedies. Failure to act promptly could undermine the very foundation of informed discourse, digital safety, and constitutional rights in the information age.

References

Ministry of Electronics and Information Technology. (2024). India AI Strategy.
Standing Committee on Commerce. (2024). Review of the IPR regime in India.
Westerlund, M. (2019). The emergence of deepfakes. Technology Innovation Management Review, 9(9), 39–52. https://doi.org/10.22215/timreview/1267
Ruiter, A. (2021). The distinct wrong of deepfakes. Philosophy & Technology, 34(2), 307–328. https://doi.org/10.1007/s13347-021-00444-2
Nema, P. (2021). Understanding copyright issues entailing deepfakes in India. Indian Journal of Law and Information Technology, 17(3), 45–62.
Feeney, M. (2021). Deepfake Laws Risk Creating More Problems Than They Solve. Regulatory Transparency Project.
O'Halloran, A. (2021). The Technical, Legal, and Ethical Landscape of Deepfake Pornography (Doctoral dissertation, Brown University).
Godulla, A., Hoffmann, C. P., & Seibert, D. (2021). Dealing with deepfakes–an interdisciplinary examination of the state of research and implications for communication studies. SCM Studies in Communication and Media, 10(1), 72-96.
R. Katarya and A. Lal, "A Study on Combating Emerging Threat of Deepfake Weaponization," 2020 Fourth International Conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud) (I-SMAC), Palladam, India, 2020, pp. 485-490, doi: 10.1109/I-SMAC49090.2020.9243588.

Zhao, H., Zhou, W., Chen, D., Wei, T., Zhang, W., & Yu, N. (2021). Multi-attentional deepfake detection. In Proceedings of the IEEE/CVF conference on computer vision and pattern recognition (pp. 2185- 2194).