INTERNATIONAL JOURNAL FOR LEGAL RESEARCH AND ANALYSIS

Open Access, Refereed Journal Multi Disciplinary
Peer Reviewed

www.ijlra.com

ISSN: 2582-6433

DISCLAIMER

No part of this publication may be reproduced or copied in any form by any means without prior written permission of Managing Editor of IJLRA. The views expressed in this publication are purely personal opinions of the authors and do not reflect the views of the Editorial Team of IJLRA.

Though every effort has been made to ensure that the information in Volume II Issue 7 is accurate and appropriately cited/referenced, neither the Editorial Board nor IJLRA shall be held liable or responsible in any manner what sever for any consequences for any action taken by anyone on the basis of information in the Journal.

ISSN: 2582-6433

EDITORIALTEAM

EDITORS

Dr. Samrat Datta

Dr. Samrat Datta Seedling School of Law and Governance, Jaipur National University, Jaipur. Dr. Samrat Datta is currently associated with Seedling School of Law and Governance, Jaipur National University, Jaipur. Dr. Datta has completed his graduation i.e., B.A.LL.B. from Law College Dehradun, Hemvati Nandan Bahuguna Garhwal University, Srinagar, Uttarakhand. He is an alumnus of KIIT University, Bhubaneswar where he pursued his post-graduation (LL.M.) in Criminal Law and subsequently completed his Ph.D. in Police Law and Information Technology from the Pacific Academy of Higher Education and Research University, Udaipur in 2020. His area of interest and research is Criminal and Police Law. Dr. Datta has a teaching experience of 7 years in various law schools across North India and has held administrative positions like Academic Coordinator, Centre Superintendent for Examinations, Deputy Controller of Examinations, Member of the Proctorial Board

Dr. Namita Jain

Head & Associate Professor
School of Law, JECRC University, Jaipur Ph.D. (Commercial Law) LL.M., UGC-NET Post Graduation Diploma in Taxation law and Practice, Bachelor of Commerce.

Teaching Experience: 12 years, AWARDS AND RECOGNITION of Dr. Namita Jain are - ICF Global Excellence Award 2020 in the category of educationalist by I Can Foundation, India. India Women Empowerment Award in the category of "Emerging Excellence in Academics by Prime Time & Utkrisht Bharat Foundation, New Delhi. (2020). Conferred in FL Book of Top 21 Record Holders in the category of education by Fashion Lifestyle Magazine, New Delhi. (2020).Certificate of Appreciation for organizing and managing the Professional Development Training Program on IPR in Collaboration with Trade Innovations Services, Jaipur on March 14th, 2019

ISSN: 2582-6433

Mrs.S.Kalpana

Assistant professor of Law

Mrs.S.Kalpana, presently Assistant professor of Law, VelTech Rangarajan Dr.Sagunthala R & D Institute of Science and Technology, Avadi. Formerly Assistant professor of Law,Vels University in the year 2019 to 2020, Worked as Guest Faculty, Chennai Dr.Ambedkar Law College, Pudupakkam. Published one book. Published 8Articles in various reputed Law Journals. Conducted 1Moot court competition and participated in nearly 80 National and International seminars and webinars conducted on various subjects of Law. Did ML in Criminal Law and Criminal Justice Administration.10 paper presentations in various National and International seminars. Attended more than 10 FDP programs. Ph.D. in Law pursuing.

Avinash Kumar

Avinash Kumar has completed his Ph.D. in International Investment Law from the Dept. of Law & Governance, Central University of South Bihar. His research work is on "International Investment Agreement and State's right to regulate Foreign Investment." He qualified UGC-NET and has been selected for the prestigious ICSSR Doctoral Fellowship. He is an alumnus of the Faculty of Law, University of Delhi. Formerly he has been elected as Students Union President of Law Centre-1, University of Delhi. Moreover, he completed his LL.M. from the University of Delhi (2014-16), dissertation on "Cross-border Merger & Acquisition"; LL.B. from the University of Delhi (2011-14), and B.A. (Hons.) from Maharaja Agrasen College, University of Delhi. He has also obtained P.G. Diploma in IPR from the Indian Society of International Law, New Delhi. He has qualified UGC – NET examination and has been awarded ICSSR – Doctoral Fellowship. He has published six-plus articles and presented 9 plus papers in national and international seminars/conferences. He participated in several workshops on research methodology and teaching and learning.

ISSN: 2582-6433

ABOUT US

INTERNATIONAL JOURNAL FOR LEGAL RESEARCH & ANLAYSIS ISSN- 2582-6433 is an Online Journal is Monthly, Peer Review, Academic Journal, Published online, that seeks to provide an interactive platform for the publication of Short Articles, Long Articles, Book Review, Case Comments, Research Papers, Essay in the field of Law & Multidisciplinary issue. Our aim is to upgrade the level of interaction and discourse about contemporary issues of law. We are eager to become a highly cited academic publication, through quality contributions from students, academics, professionals from the industry, the bar and the bench. INTERNATIONAL JOURNAL FOR LEGAL RESEARCH & ANALYSIS ISSN 2582-6433 welcomes contributions from all legal branches, as long as the work is original, unpublished and is in consonance with the submission guidelines.

ISSN: 2582-6433

COUNTERING DEEPFAKES: A STRATEGIC BLUEPRINT FOR MODERNIZING INDIAN CRIMINAL LAW

AUTHORED BY - SARFERAAZ KHAAN
Advocate, Madras High Court

Abstract:

The rapid rise of deepfake technology in India presents a severe and escalating threat to individual privacy, financial security, and public order. This paper argues that India's current criminal legal framework, anchored by the Information Technology Act, 2000, is inadequate for addressing these novel and technologically intricate crimes. Existing laws are not optimally suited to prosecute the unique harms of hyper-realistic synthetic media, creating a safe haven for malicious actors and leaving victims without recourse. The analysis begins by documenting high-profile deepfake cases in India, illustrating the tangible and severe harm inflicted upon victims. It then conducts a critical gap analysis of the current legal framework, demonstrating how provisions like Sections 66E and 67, are rendered inadequate by the technologically sophisticated and deceptive nature of deepfakes. The paper further explores the liability of intermediaries under Section 79 of the IT Act, questioning whether a mere 'safe harbour' is sufficient when platforms facilitate the viral spread of criminal content. To counter this threat, the article proposes a straightforward, three-pronged strategy for legal reform. The article suggests a three-pronged legal solution to specifically address the problem. Beyond the present strategy, the report further recommends for enhancing platform accountability by requiring proactive material identification and removal. The conclusion asserts that strengthening India's penal framework is not an optional future policy, but an immediate necessity to safeguard citizens and maintain trust in the digital ecosystem.

Keywords: Deepfakes, indian criminal law, information technology act 2000, legal reform.

ISSN: 2582-6433

INTRODUCTION

Artificial intelligence (AI) has the potential to transform the media and content sector, but it has also raised ethical and legal concerns, particularly with "deepfake technology." This technology allows for the creation of lifelike yet fake audio, video, or image snippets, which have been used for political manipulation, reputational damage, and misinformation. These deepfakes have severe repercussions for the targets and society as a whole.

While holding potential for creative industries, its malicious application poses an unprecedented threat to the very fabric of society—eroding trust, undermining individual dignity, and jeopardizing national security. In India, with its vast and rapidly digitizing population, the proliferation of deepfakes used for non-consensual pornography, financial fraud, and political disinformation reveals a critical vulnerability. The existing criminal legal framework, designed for a pre-AI era, is woefully inadequate to combat this new form of digital assault.

This article argues that India's penal laws, particularly the Information Technology Act, 2000, require urgent and structural fortification to effectively criminalize, prosecute, and deter deepfake-related offenses, thereby protecting citizens and preserving democratic integrity in the digital age.

Part I establishes the foundations of deepfake technology, how it works and the threats of deepfake technology to India. Part II addresses the legal inadequacies of existing laws in prosecuting deepfake-related crimes. Part III proposes a blueprint for reforms which contains a multi-pronged strategy to tackle a wholly advanced technology-based mode of crime. Part IV contains concluding remarks.

I. DEEPFAKE TECHNOLOGY – RISE AND THREAT

A. Deepfake Technology – What It Is & How It Works

The practice of data manipulation has existed for as long as history. In the early to mid-20th century, Soviet leader Joseph Stalin controlled his image and government through image editing and censorship.[1] With a few mouse clicks, data can be altered and manipulated, due to

[1] Erin Blakemore, 'How Photos Became a Weapon in Stalin's Great Purge', (History, 18 February, 2025) <https://www.history.com/articles/josef-stalin-great-purge-photo-retouching.> accessed 8 September 2025

ISSN: 2582-6433

involvement of artificial intelligence. Human voices and likenesses—especially, video clips—are being utilized to trick people into believing that what they are seeing or hearing is authentic.[2]

In the current scenario where so many people are coming online, imagine coming across a humorous meme while surfing through social media that makes you chuckle, like a person doing a funny dance move. However, the identical video appears later, but the face of the subject is different. This individual is now a well-known figure in the entertainment sector. What did you just see, you wonder? You clearly recall watching the original video, but confused. I experienced exactly this, after which I first heard the term "deepfakes" being used in the news.

Deepfakes are artificial intelligence (AI)-manipulated videos, images, or audio recordings that appear authentic. It can synthesize speech, replace faces, and alter facial emotions. The common purpose for these technologies is to show someone talking or doing things they never said or did.[3] All of it began when a Reddit moderator first used the word "deepfake" in 2017. He created a subreddit where people could share deepfake pornography they had made using face-swapping software and celebrity photographs.[4]

In 2015, Google released “TensorFlow”, the company’s internal tool for developing artificial intelligence algorithms.[5] But soon after, TensorFlow was used to transpose actor Gal Gadot’s face, along with the face of other celebrities, onto porn stars’ bodies in porn videos.[6]

B. Applications of Deepfakes

Deepfake content can be created for a variety of reasons, such as amusement, but it can also be used for identity theft, retaliation, blackmail, and many other purposes.[7]

---

[2] Ibid.
[3] Karen Howard, ‘Deconstructing Deepfakes—How do they work and what are the risks’, (U.S. Government Accountability Office, 20 October 2020) <https://www.gao.gov/blog/deconstructing-deepfakes-how-do-they-work-and-what-are-risks.> accessed 8 September 2025.
[4] Gabe Regan, ‘A Brief History of Deepfakes’ (Reality Defender, 1 June 2024) <https://www.realitydefender.com/blog/history-of-deepfakes> accessed 8 September 2025.
[5] Dave Gershgorn, ‘Google gave the world powerful AI tools, and the world made porn with them’ (Quartz, 7 February 2018) <https://qz.com/1199850/google-gave-the-world-powerful-open-source-ai-tools-and-the-world-made-porn-with-them> accessed 8 September 2025.
[6] Samantha Cole, ‘AI-Assisted Fake Porn Is Here and We’re All F**ed’ (Vice, 11 December 2017) <https://www.vice.com/en/article/gal-gadot-fake-ai-porn/> accessed 8 September 2025.
[7] Bahar Uddin Mahmud, Afsana Sharmin, ‘Deep Insights of Deepfake Technology: A Review’ (2020) 5 Dhaka University Journal of Applied Science & Engineering, 14

ISSN: 2582-6433

Pornography: Rana Ayyub, an Indian investigative journalist, was notified in April 2018, that a pornographic film of her was made and disseminated.[8] Ayyub was in the news, advocating for justice when an eight-year-old Kashmiri girl was raped and killed.[9] She was startled to discover a "nonconsensual deepfake pornography" (NCDP) film made with artificial intelligence and publicly accessible images of Ayyub when she clicked on a link.[10] Between 90% and 95% of internet deepfake films are nonconsensual porn, according to research firm Sensity AI.[11] This posits as a problematic application of deepfakes. Nonconsensual pornography or NCP can be linked to Deepfake Nonconsensual Pornography (DNCP).[12] NCP in the era of artificial intelligence is DNCP. Similar to NCP, DNCP entails the sharing of a sexually explicit image without permission.[13] Deepfake pornography is not magic and it is no longer "rocket science".[14] The app DeepNude can generate a naked image of a woman, by allowing users to upload photos of any woman.[15] Scarlett Johansson's face-swapping in AI-generated videos that circulate online despite her lack of participation is an example of this.[16]

Financial Fraud: Apart from pornography, the Hong Kong deepfake scam in 2023, where the fraudsters used deepfake technology to impersonate a company executive on a video call and ending up stealing $25 million from employees,[17] highlights deepfakes' role in financial aspects as well. Similarly, for a limited time, stock markets were impacted by a phony image

<https://www.researchgate.net/publication/351300442_Deep_Insights_of_Deepfake_Technology_A_Review> accessed September 8 2025.

[8] Rana Ayyub, 'I Was The Victim Of A Deepfake Porn Plot Intended To Silence Me' (HuffPost, 21 November2018) <https://www.huffingtonpost.co.uk/entry/deepfakeporn_uk_5bf2c126e4b0f32bd58ba316> accessed 8 September 2025.

[9] *Ibid.*

[10] *Ibid.*

[11] Karen Hao, 'Deepfake porn is ruining women's lives. Now the law may finally ban it' (MIT Technology Review, 12 February 2021) <https://tinyurl.com/52c8pmp8> accessed 8 September 2025.

[12] Moncarol Y Wang, 'Don't Believe Your Eyes: Fighting Deepfaked Nonconsensual Pornography With Tort Law' (2023) 2022 University of Chicago Legal Forum. <https://chicagounbound.uchicago.edu/uclf/vol2022/iss1/16/> accessed September 8 2025.

[13] Rebecca A Delfino, 'Pornographic Deepfakes: The Case for Federal Criminalization of Revenge Porn's Next Tragic Act' (2019) 88 Fordham L Rev, 889-91 <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3341593> accessed September 8 2025.

[14] Samantha Cole, (n 6).

[15] Samantha Cole, 'This Horrifying App Undresses a Photo of Any Woman With a Single Click' (Vice, 26 June 2019) <https://www.vice.com/en/article/deepnude-app-creates-fake-nudes-of-any-woman/> accessed 8 September 2025.

[16] US Department of Homeland Security, Increasing Threat of Deepfake Identities (Report) <https://tinyurl.com/3r6h6m7j> accessed 8 September 2025.

[17] Shannon Murphy, 'A Deepfake Scammed a Bank out of $25M — Now What?' (Trend Micro, 7 February 2024) <https://www.trendmicro.com/en_sg/research/24/b/deepfake-video-calls.html> accessed 8 September 2025.

ISSN: 2582-6433

of an explosion close to the Pentagon.[18]

Misinformation: We use our mobile devices, especially social media platforms, to access the news and obtain a quick overview of events. Deepfakes have the potential to propagate false information, perplex consumers or exert influence.[19] Social media platforms are the main channels through which deepfakes are disseminated to a wide audience.[20] Since social media has made virality a top priority, numerous studies have previously demonstrated that bogus news spreads more quickly online.[21] In one study, MIT researchers looked at 126,000 rumours that were shared by three million people. They discovered that more people were exposed to erroneous information than to true information.[22] This is a huge advantage for the widespread dissemination of deepfakes. There are reliable and technical ways to identify deepfakes. However, the public, especially those with low levels of AI literacy, find it difficult to discern deepfakes and original videos.[23] A study shows, users only 50% of the time properly identify deepfake videos.[24]

Politics: Deepfakes could also be used to instigate aggressive threats to politics. One of the main issues during the 2024 U.S. presidential election was misinformation produced by artificial intelligence.[25]

Thus, deepfakes have significantly transformed the misleading scene, from trivial matters like celebrity gossips to influencing public opinion, impacting choices, and harming reputations. As AI-generated content becomes harder to distinguish between fact and fiction, it becomes increasingly challenging to distinguish between the two.

[18] Shannon Bond, 'Fake viral images of an explosion at the Pentagon were probably created by AI' (*NPR*, 22 May 2023) <https://www.npr.org/2023/05/22/1177590231/fake-viral-images-of-an-explosion-at-the-pentagon-were-probably-created-by-ai> accessed 8 September 2025.
[19] Robert P Griffin, 'The National Security Implications of Deepfake Technology' in *Proceedings of the 17th International Conference on Cyber Warfare and Security* (Academic Conferences International Ltd 2022).
[20] *Ibid* 345.
[21] Peter Dizikes, 'Study: On Twitter, false news travels faster than true stories' (*MIT News*, 8 March 2018) <https://news.mit.edu/2018/study-twitter-false-news-travels-faster-true-stories-0308> accessed 8 September 2025.
[22] *Ibid*.
[23] *Ibid*.
[24] Andreas Rössler and others, 'FaceForensics: A Large-Scale Video Dataset for Forgery Detection in Human Faces' (2018) arXiv preprint <https://doi.org/10.48550/arXiv.1803.09179> accessed 8 September 2025.
[25] Sayash Kapoor and Arvind Narayanan, 'We Looked at 78 Election Deepfakes. Political Misinformation Is Not an AI Problem' (*Knight Columbia*, 13 December 2024) <https://knightcolumbia.org/blog/we-looked-at-78-election-deepfakes-political-misinformation-is-not-an-ai-problem> accessed 8 September 2025.

ISSN: 2582-6433

C. The Deepfake Threat in India

The first ever usage of a deepfake video in India, happened in 2020 relating to an election campaign. Two videos of Bharatiya Janata Party (BJP) President Manoj Tiwari attacking the Arvind Kejriwal-led Delhi government went popular on WhatsApp one day before the Legislative Assembly elections in Delhi. In one video, Tiwari spoke in English, but in the other, he spoke in Haryanvi. Initially it was perceived as a typical political outreach, but it was later realized that these videos were not authentic.[26]

Since then, concerns over the possible abuse of artificial intelligence (AI) have been highlighted by the usage of deepfake films to deceive social media users. Following the release of pictures and videos of him, Narayana Murthy, the founder of Infosys, issued a public warning in 2023. He asked everyone to be on guard and notify the police of any such occurrences.[27]

Since 2019, the number of deepfake instances in India has increased by 55%, and losses are expected to exceed Rs 70,000 crore in 2024 alone. According to Pi-Labs' 2024 research, deepfake fraud is becoming more and more of a problem in India. The likelihood of cybercrime, financial fraud, and privacy invasion has increased due to the quick development of generative artificial intelligence (GenAI) technologies, especially in the production of realistic audio, video, and image content.[28] Along with additional risks like cybercrime automation and AI-enhanced privacy invasion, deepfake fraud currently accounts for 40% of all AI-related cybercrimes worldwide. The accessibility of these tools is demonstrated by the fact that over 50 apps are available for producing deepfake content, and over a million deepfake videos were reported worldwide in 2024.[29]

The Data Security Council of India's *India Cyber Threat Report 2025* had identified deepfake exploitation as a critical cybersecurity threat in 2024. Predictions indicate deepfakes will be

[26] Nilesh Christopher, 'We've Just Seen the First Use of Deepfakes in an Indian Election Campaign', (*Vice*, 18 February, 2020) <https://www.vice.com/en/article/the-first-use-of-deepfakes-in-indian-election-by-bjp/>, accessed 8 September 2025.
[27] Darshan Devaiah, 'Karnataka reports 12 deepfake-related cybercrime cases in two years' *The Hindu* (India, 19 March 2025) <https://www.thehindu.com/news/national/karnataka/karnataka-reports-12-deepfake-related-cybercrime-cases-in-two-years/article69333474.ece> accessed 8 September 2025.
[28] BW Online Bureau, India's Deepfake Cases Up 550% Losses May Hit Rs 70,000 Cr By 2024: Report, *BW Business World* (India, 5 December 2024) <https://www.businessworld.in/article/indias-deepfake-cases-up-550-losses-may-hit-rs-70000-cr-by-2024-report-541202> accessed 8 September 2025.
[29] Ibid.

ISSN: 2582-6433

increasingly used in advanced deception campaigns, malware distribution, and highly sophisticated phishing attacks in 2025. A 2023 McAfee study further revealed that 47% of Indians—the highest rate globally—have either been victims of or know someone affected by deepfake voice scams. High-profile individuals, including celebrities, religious leaders, and government officials, have already been targeted.[30]

Indian public figures have already become prominent targets of deepfake technology, highlighting its use for political manipulation and personal harm. In a politically motivated case, BJP politician Manoj Tiwari used deepfake technology to adapt a prior speech on the Citizenship Amendment Act into a new message for the Delhi Elections. The original Hindi speech was artificially dubbed into Haryanvi to target voters in that region.[31]

Prime Minister Narendra Modi was the victim of a satirical video that the Indian National Congress, the nation's primary opposition party, uploaded to Instagram in February, shortly before the country's national elections. In the video, Modi's face was superimposed using artificial intelligence over the body of a well-known musician whose song "Chor," which translates to "Thief," had just gone viral. Modi's Bharatiya Janata Party (BJP) responded with its own AI-generated content, not to be outdone. In order to give the impression that Rahul Gandhi, the leader of the Congress, was disparaging a former ally who had recently left the opposition coalition, they produced a film in which his face was superimposed on another opposition politician. This was an obvious attempt to draw attention to the differences among the opposition. A new, AI-powered era in Indian political campaigns began with this back-and-forth. To draw in voters and more successfully attack opponents than ever before, parties started utilizing a variety of cutting-edge digital technologies, such as voice cloning, AI chatbots, bespoke video messaging, deepfakes, QR codes, and even holograms.[32]

Actor Ranveer Singh was the victim of a deepfake where the audio of a genuine interview was

[30] Anand & Anand, 'Real or Fake? Dealing with Deepfakes Dilemma in Digital Society' (4 February 2025) <https://www.anandandanand.com/news-insights/real-or-fake-dealing-with-deepfakes-dilemma-in-digital-society/> accessed 8 September 2025.
[31] Biranchi Naryan P Panda and Isha Sharma, 'Deepfake Technology in India and World: Foreboding and Forbidding' (*Asian Institute of Research*, 16 July 2025) <https://www.asianinstituteofresearch.org/lhqrarchives/deepfake-technology-in-india-and-world%3A-foreboding-and-forbidding> accessed 8 September 2025.
[32] Samriddhi Sakunia, 'AI and Deepfakes Played a Big Role in India's Elections', New Lines Magazine (India, 12 July 2024) <https://newlinesmag.com/spotlight/ai-and-deepfakes-played-a-big-role-in-indias-elections/> accessed 8 September 2025.

ISSN: 2582-6433

replaced with AI-generated dialogue. The manipulated video falsely showed him criticizing the Prime Minister and endorsing an opposition party. An FIR was filed, and Singh publicly warned his followers about the dangers of deepfakes. In a widely circulated instance of non-consensual imagery, a deepfake video of actor Rashmika Mandanna amassed over 2.4 million views. This case, which involved AI-powered face-swapping, sparked a national debate on the inadequacy of existing legal protections against such digital harassment and cyberbullying.[33]

One can assume that those who produce such deepfake content target influential people in an attempt to seriously harm their reputations and potentially profit from their actions. However, deepfakes are used as a weapon to prey on the general public as well. A woman's deepfake video became viral on Instagram in a matter of days, and the phony account gained 1.4 million followers. The video featured a woman wearing a red saree dancing sensuously to the Romanian song "Dame Un Grr," which was a recent trend across social media. The accused was a self-taught AI enthusiast and mechanical engineer, who made a decoy profile using the victim's private images.[34]

These incidents collectively underscore the urgent need for robust legal frameworks to address the threats deepfakes pose to electoral integrity, individual privacy, and public safety.

II. LAWS ADDRESSING DEEPFAKES AND THE VISIBLE VOID

A. Existing Cyber Crime Laws in India – A Closer Reach to Deepfakes

The Information Technology Act, 2000 serves as India's core cyber legislation. Several of its provisions are relevant to addressing deepfake-related offenses:

- *Section 66D*: It has been construed to include identity fraud and penalizes cheating by personation employing a computer resource.
- *Section 67*: Prohibits the electronic publication or transmission of pornographic material, including sexual content.
- *Section 66E*: Prevents invasions of privacy by capturing or sending private photos without permission.

[33] Panda and Sharma, n 31.
[34] Geeta Pandey, Deepfake deception: Indian woman's identity stolen for erotic AI content, *BBC News* (India, 23 July 2025) <https://www.bbc.com/news/articles/cn0znk47x9eo> accessed 8 September 2025.

ISSN: 2582-6433

- *Section 69A*: Gives the government the authority to restrict public access to internet content that poses a risk to public safety or order.[35]

The Bharatiya Nyaya Sanhita (BNS) 2023 somewhat strengthens India's response to cybercrimes with updated provisions:

- *Section 294*: Criminalizes electronic transmission of obscene content.
- *Section 77*: Penalizes non-consensual capture/sharing of private images.

While more modern than the IT Act, the BNS still lacks specific provisions criminalizing the unique creation and harmful use of deepfakes.

The Digital Personal Data Protection Act 2023, intends to handle issues with the gathering and use of personal information, especially when there has been a major infringement on someone's right to privacy.[36]

The use of false and misleading material in election campaigns to sway public opinion is strictly prohibited by Indian electoral laws and regulations, such as the Representation of the People Act, 1951, and Election Commission guidelines.[37]

B. Possible Reforms Against Deepfakes

Defamation: As per Section 356 of BNS, it means publishing any statement, either spoken or written, which intends to harm the reputation of the person it is directed towards. Courts have noted that where there is intent or knowledge of potential harm, visual representations meant to damage reputation—including digitally altered photos or videos—can be sued as defamation.[38] Here is the take. If the origin of a deepfake is unknown or foreign, it could be challenging to prove the creator's intention to damage reputation. Although the BNS clause is extensive, technically complex deepfakes (AI-generated, hard to track) might evade prosecution because there might not be enough reliable digital proof or attribution.

Copyright Law: The copyright owner has the exclusive right to make copies of his work

[35] Ayushman Kumar, 'Illusion of Identity: Legislative Challenges Revolving around Deepfake Technology' (*Lawctopus Academike*, 6 August 2025) <https://www.lawctopus.com/academike/illusions-of-identity-legislative-challenges-revolving-around-deepfake-technology/> accessed 9 September 2025.
[36] The Digital Personal Data Protection Act 2023 (IN).
[37] Kuldeep Singh Panwar and Nilutpal Deb Roy, 'Rising Menace of Deepfakes with the Help of AI: Legal Implications in India' (2024) 4(3), 100 <chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/https://ijirl.com/wp-content/uploads/2024/05/RISING-MENACE-OF-DEEPFAKES-WITH-THE-HELP-OF-AI-LEGAL-IMPLICATIONS-IN-INDIA.pdf>, Indian Journal of Integrated Research in Law.
[38] Aditya Mehrotra, 'Dissecting the Framework of Deep Fakes in India – A Glaring Lacuna', *NLIU Cell for Law and Technology* (5 December 2024) <https://clt.nliu.ac.in/?p=887> accessed 8 September 2025.

ISSN: 2582-6433

according to *Section 14 of the Copyright Act, 1957*. Indian courts have granted injunctions in cases where AI-generated manipulations of celebrities' images or videos amounted to unauthorized uses of their personality and likeness, essential elements of copyright and related "personality rights" in India.[39]

The interim orders in Abhishek Bachchan and Aishwarya Rai Bachchan reaffirm the judiciary's commitment to protecting individual dignity in the face of evolving technological threats. They establish that personality rights are not only a matter of economic interest but are also fundamental to the right to live with dignity. By insisting on swift take-downs, accountability from platforms, and even government involvement.[40]

However, a comprehensive list of exceptions (fair dealing) for purposes including news reporting, criticism, commentary, and review is provided under *Section 52 of the Copyright Act*. Because of the content being transformational, deepfakes made for this purpose would be considered "fair dealing" and not actionable. Furthermore, unless their original creative work is involved, copyright law provides little protection for the majority of regular people, including women whose photos or videos are utilized in deepfakes.

It is challenging to apply copyright law to eliminate deepfakes because most persons do not possess copyright over generic images, videos, or likenesses of themselves unless they produced them as artistic works or can demonstrate ownership. Copyright law may not be enough for women affected by non-consensual deepfake pornography or harassment since it ignores fundamental abuses of privacy, consent, and dignity.

Right to Privacy: According to the Supreme Court's ruling in *Justice K.S. Puttaswamy (Retd.) v. Union of India* (2017), the right to privacy is a fundamental right guaranteed by Article 21 of the Constitution.[41] Any interference with an individual's dignity, autonomy, or identity control may be considered a violation. However, deepfakes are not explicitly defined, prohibited, or regulated by Indian law as a distinct category, which makes it challenging to

[39] Divy Lotia, 'Deepfakes, AI and the Law: Protecting Celebrity Personality Rights in India', *IndiaLaw* (15 September 2025) <https://www.indialaw.in/blog/intellectual-property-rights/deepfakes-ai-law-protecting-celebrity-rights-india/> accessed 8 September 2025.
[40] *Ibid*.
[41] Justice K.S. Puttaswamy (Retd.) v. Union of India, (2017) 10 SCC 1.

ISSN: 2582-6433

implement privacy laws until blatant harm or unlawful use is proven.[42] Because of antiquated laws and inadequate technology, enforcement is usually uneven. Celebrities and prominent people have stronger rights and remedies because courts have more explicitly identified their commercial, publicity, and dignity interests; regular persons' protection is less clear and occasionally difficult to enforce.[43]

Pornography Laws: The BNS's *Sections 294 and 295* are essential for controlling pornographic publications and content. According to these sections, everything that is "lascivious or appeals to the prurient interest" or corrupts people is considered obscenity. It is illegal to sell, rent, distribute, or display such pornographic items in public. The penalties include jail time and fines. In particular, Section 295 makes it illegal to sell pornographic materials to children, highlighting the need to shield young people from such content. The protection of children against pornographic exploitation is emphasized in *Section 14 of the Protection of Children from Sexual Offences (POCSO) Act, 2012*. The IT Act also imposes strict regulations on the digital environment. Online transmission of pornographic and sexually explicit content is covered by Sections 67, 67A, and 67B.[44] Therefore, it is well established that Indian law has a strict position on pornography and has a number of measures designed to limit the creation, dissemination, and use of pornographic content.

None of these laws specifically mention or describe "deepfake," "synthetic media," or "artificially generated content," but they all make it illegal to create, publish, and distribute pornographic, sexually explicit, or child pornographic content. Authorities would frequently be reluctant to prosecute deepfake cases as a result of this disparity and inconsistent enforcement. Because deepfakes are notoriously hard to track down and platforms can spread them quickly, there are gaps in determining the genuine intent of their creators. Additionally, victims face slow and inefficient enforcement of these rules.These provisions, however, remain fragmented and insufficient to address the full scope of technological and societal harm caused by deepfakes.

[42] Meera Srikant, 'Bharatiya Laws Against Deepfake Cybercrime Opportunities and Challenges', *Vivekananda International Foundation* (28 April 2025), <https://www.vifindia.org/article/2025/april/28/Bharatiya-Laws-Against-Deepfake-Cybercrime-Opportunities-and-Challenges> accessed 8 September 2025.
[43] Tanya Pandey, Court Ruling boosts acceptance of personality rights in deepfake cases, *Economic Times* (India, 15 September 2025), <https://economictimes.indiatimes.com/tech/technology/court-ruling-boosts-acceptance-of-personality-rights-in-deepfake-cases/articleshow/123886025.cms> accessed 8 September 2025
[44] Srishti Ojha, 'Explained: What Indian laws say about pornography and sex toys' *India Today* (India, 22 August 2024) <https://www.indiatoday.in/law/story/indian-law-on-pornography-sex-toys-bnc-pocso-act-it-act-2585977-2024-08-21> accessed 8 September 2025.

ISSN: 2582-6433

C. Challenges in Applying Existing Laws

While laws exist to combat cybercrimes, imposing criminal liability for deepfakes faces significant practical and legal hurdles.

Attribution and Jurisdictional Hurdles: A primary challenge is the anonymity of perpetrators, who often operate under pseudonyms using VPNs or other masking technologies. The content has the risk of being widely reposted, obscuring its origin.

Furthermore, the global nature of the internet means creators can target Indian victims from abroad. Although Indian law claims extraterritorial jurisdiction for cybercrimes impacting the country, practical enforcement is extremely difficult. It requires cooperation through mutual legal assistance treaties (MLATs), a process that is often slow, cumbersome, and uncertain, especially if the perpetrator is in a non-cooperative jurisdiction.

Evidentiary and Forensic Obstacles: Prosecuting a deepfake case requires prosecutors to conclusively prove the content is fake and link it to the accused. This demands advanced digital forensics to analyse the media, a technically complex and expensive process. As technology improves, distinguishing deepfakes from real content becomes even harder for experts.

There is also a dual risk - sophisticated fakes may deceive investigators, or defendants may falsely claim authentic evidence is a deepfake. Indian law enforcement is still developing the specialized forensic capacity needed to handle AI-manipulated content effectively.[45]

The Role and Liability of Intermediaries: Online platforms (intermediaries) like Facebook and YouTube are critical distribution points for deepfakes. They are generally protected from liability for user-generated content under Section 79 of the IT Act, provided they follow due diligence guidelines.

However, this “safe harbour” immunity is not absolute. The IT Rules, 2021 mandate that platforms must remove reported content, especially morphed or intimate images, within 24 hours. For other deepfakes and misinformation, the required action time is 36 hours. Failure to comply can lead to the platform losing its legal protection and facing liability for abetting the offense.[46]

Crucially, as established in the Shreya Singhal case, platforms are not required to proactively monitor content but must act on official court or government orders.

The Pervasive Risk of Harm The core danger of deepfakes lies in their hyper-realism. They are not simple edits but AI-generated fabrications that can seamlessly replace a person’s likeness and voice. This technology moves beyond harmless parody into the realm of serious

[45] Ayushman Kumar (n 35).
[46] Ibid.

ISSN: 2582-6433

crime, enabling:

- Political misinformation and election interference.
- Reputational damage and defamation (e.g., the Rashmika Mandanna case).
- Financial fraud through impersonation.
- Psychological harm and privacy violations via non-consensual intimate imagery.

The laws in place in India only provide sporadic defence against deepfakes. There are no laws that specifically make the deliberate production of deepfakes illegal. Because of this disparity, the technology is mainly uncontrolled and emphasizes punishment over prevention.

In a November 7, 2023 advisory, the Ministry of Electronics and Information Technology directed major social media platforms to:

- Proactively identify and remove deepfakes and misinformation violating Indian laws or platform terms.
- Act on reports within 36 hours, per IT Rules 2021.
- Warn users against uploading prohibited or synthetic content.
- Ensure prompt compliance with takedown obligations.[47]

I place an argument here that an advisory is not a law. It serves as a recommendation rather than a legally enforceable mandate. Without binding laws, compliance remains voluntary and vague. Terms like "proactively identify", "ensure prompt compliance" and so on, are open to interpretation. The advisory does not define what constitutes them. Thus, the advisory acknowledged the problem but fails to provide legal backing.

While the Government of India has promptly highlighted the threats posed by deepfakes in a report recently,[48] the approach I would say, is predominantly reactive – focusing on punishment rather than prevention. None of the laws – including the IT Act, the Bharatiya Nyaya Sanhita or the Digital Personal Data Protection Act – explicitly criminalize the act of "generating deepfakes". This creates a legal vacuum where creators can operate with impunity until a specific harm is demonstrated already. Simply widening the scope of existing provisions to include deepfakes, still leaves gaps unsealed.

The real problem is that, India currently has no AI-specific regulations, allowing largely unrestricted use of tools like ChatGPT and Midjourney. Though initiatives like the 2018 National AI Strategy and the 2023 Digital Personal Data Protection Act provide high-level

[47] Government of India, Ministry of Electronics & IT, 'Union Government issues advisory to social media intermediaries to identify misinformation and deepfakes' (Press Release, 2023).
[48] Government of India, Ministry of Electronics & IT, 'India well-equipped to tackle evolving online harms and cybercrimes; Government to Parliament' (Press Release, 2025).

ISSN: 2582-6433

frameworks, they lack concrete rules against consumer-level AI misuse—such as exploiting voices, images, or videos without consent. This regulatory gap leaves individuals vulnerable to AI-facilitated harm.[49]

This potential for widespread harm underscores the urgent need for legal and technological solutions that can keep pace with the threat.

III. A BLUEPRINT FOR CRIMINALIZING AND ELUDING DEEPFAKE THREAT

As part of this article, I advocate for introducing a multi-pronged approach to not only punish but to prevent even the creation and dissemination of deepfakes. This approach integrates legislative innovation, technological empowerment and institutional capacity building and public awareness to create a resilient ecosystem against deepfakes.

India's legal system needs to be strengthened immediately in order to fight deepfakes in three different ways. First, passing a specific Deepfake Regulation Act that defines synthetic media precisely and penalizes those who create and distribute it maliciously, is paramount. Secondly, making AI-enabled impersonation and unapproved synthetic content clearly illegal by amending the IT Act of 2000, specifically Sections 66C, 66E, and 67A removes doubts regarding interpretation. Thirdly, as a necessary extension of the constitutional right to privacy under Article 21, explicitly establish digital personality rights in law, safeguarding people's voice, likeness, and visual identify from AI abuse. These actions would empower victims, narrow legal loopholes, and establish clear prohibitions.[50]

The implementation of the Deepfake Prevention Bill 2023, which creates a thorough legal framework to combat fraudulent AI-generated content, deserves recognition for the strong effort made in the fight against deepfakes. The bill is almost ready for full implementation as of July 2025. Important clauses include case-based fines or criminal penalties of up to five years in jail for producing or disseminating deepfakes without permission, particularly when sexual content, fraud, or identity theft are involved. In line with international legislative trends,

[49] Panda and Sharma (n 31).
[50] Asim Mustafa Khan, 'Regulating Deepfakes in India: A Legal and Ethical Analysis of Misinformation in The Age of AI' [2025] 7(3), 7673, <https://www.ijllr.com/post/regulating-deepfakes-in-india-a-legal-and-ethical-analysis-of-misinformation-in-the-age-of-ai>, Indian Journal of Law and Legal Research, accessed 10 September 2025.

ISSN: 2582-6433

the measure places a strong emphasis on consent and harm reduction.[51]

I place an argument that platforms should be held accountable for failing to remove harmful content, such as deepfakes and misinformation, within the notice period specified under the IT Rules. This balances the perspectives of the internet platform and the deepfake victim, but also highlights the need for clarity on what constitutes "proactively identify" under the Act. By this way, I believe that platforms must demonstrate reasonable efforts to remove harmful content, including deepfakes, to ensure a balanced approach to addressing the issue. But there also exists a void in what such “reasonable efforts” would constitute under the Act or Rules. Clarity on the meanings and definitions and what fails to constitute as “reasonable efforts” is required as well.

AI watermarking can also be a helpful step in the process of redressing deepfake harm, even though it is not a novel idea. Although this technique cannot stop the production of deepfakes, it may be able to alert users when what they are viewing or encountering is artificial intelligence (AI)-generated, fabricated, or even a deepfake.

I believe that watermarking in deepfake apps could help identify the original video developer, as there is no current regulation and visible watermarks can be easily erased, which could be beneficial in for deepfake creators.

However, I also disagree that they do not address the original issue of deepfakes going viral on social media. Since the public who are exposed to the content are unlikely to notice the watermarks, unless the platform they are viewing it through, specifically highlights them, watermarks would only have an impact during the enforcement or liability stage and not during the actual harm.

Instagram's update, which asks users if they are using artificial intelligence (AI) in the content they wish to upload, might be useful in tagging content as AI,[52] but not for those who want to

[51] VarIndia, ‘India Enacts DeepFake Law Under AI TRA Bill 2024’ < <https://varindia.com/news/india-enacts-deepfake-law-under-ai-tra-bill-2024#:~:text=India's%20DeepFake%20Prevention%20Bill%202023,effect%20or%20nearing%20full%20implementation> accessed 8 September 2025.

[52] ‘Label AI content on Instagram’ (*Instagram Help Center*) <https://help.instagram.com/761121959519495> accessed 10 September 2025.

ISSN: 2582-6433

post malicious deepfake content, because it is just an option which can be switched on or off. There is a certain window between a person clicking the upload button and the content being posted online. If Instagram, or any other platform, during that window, could make efforts to analyse if the content has used AI or even completely created by using AI and tagging it accordingly, would try to solve the problem at its root.

Deepfake technology's complexity necessitates a forensic system for content tracking, liability determination, and mandatory metadata inclusion for media origins, source of extraction and their modifications.

Gender harassment refers to unwelcome verbal and visual insults directed at individuals based on their gender, using cues to elicit negative feelings, such as making chauvinistic jokes, publishing sexual images, and making demeaning comments about gender.[53] So, inappropriate sexual behaviour can occur anywhere on the internet, particularly on social networking sites where users are electronically connected. Additionally, it is now easier to obtain a specific person's photo or video, anywhere from the internet.

Deepfakes are no different from other types of sexually inappropriate behaviour or information on the internet. Deepfakes frequently have sexual overtones and cause victims a great deal of emotional distress. It may be helpful, in my opinion, to categorize these deepfakes under the heading of online sexual harassment in order to hold the material producers criminally liable.
The establishment of accredited digital forensics labs under institutional auspices requires government funding. Creating standardized procedures for media authentication, certifying evidence for admissibility in court, and assisting law enforcement would be the responsibility of these labs. At the same time, encouraging the use of technological protections, including cryptographic watermarking at the point of creation and secure digital content provenance standards, can aid in identifying fake media and authenticating real ones.

Even though these measures might be implemented, I believe that harmful deepfake issues are unlikely to be resolved until clear-cut regulations that specifically target deepfakes while also taking free speech concerns into account are introduced. A straightforward examination of

[53] Azy Barak, 'Sexual Harassment on the Internet' (2005) 23(1), 78 <https://www.researchgate.net/publication/249794676_Sexual_Harassment_on_the_Internet> Social Science Computer Review, accessed September 10, 2025.

ISSN: 2582-6433

whether a specific deepfake content stays within the bounds of harm or totally surpasses its intent and causes the victim any kind of harm should also be taken into account. I am also of the opinion that, trying to stretch the scope of existing laws cannot really solve technological issues and harms at its root. Advanced technology requires tech-specific laws, which can help address issues completely, without leaving much gaps or loopholes.

IV. CONCLUSION

In conclusion, the escalating threat posed by deepfake technology—to individual privacy, personal reputation, and democratic integrity—exposes critical gaps in India's legal framework. Current laws, including the IT Act, 2000 the Bharatiya Nyaya Sanhita, etc., are largely reactive and fragmented. They address downstream harms such as defamation, fraud, or obscenity only after damage has occurred, but fail to explicitly criminalize the malicious creation or non-consensual dissemination of synthetic media itself. This legislative void is compounded by practical challenges in attribution, jurisdictional reach, and intermediary accountability.

To effectively counter this evolving risk, India must transition from a reactive to a proactive regulatory posture. This necessitates a multi-faceted strategy: enacting a dedicated Deepfake Regulation Act to define and penalize AI-generated misuse, amending existing cyber laws to cover synthetic impersonation and harm, and formally recognizing digital personality rights to protect against identity theft. Strengthening forensic capabilities, ensuring stringent platform accountability, and raising public awareness are equally vital. Without such comprehensive and modernized legal safeguards, citizens remain vulnerable to digital exploitation, and trust in the integrity of information and institutions stands imperilled.