WWW.IJRPR.COM

International Journal of Research Publication and Reviews

Journal homepage: www.ijrpr.com ISSN 2582-7421

ANALYSING LEGAL FRAMEWORK OF REGULATING DEEPFAKE TECHNOLOGY AND MISINFORMATION IN INDIA

PARIANSH GUPTA[1], MS. SRISHTI DIXIT[2]

[1] Pursuing B.A.LL.B. (H), 3rd Semester
Mangalayatan University Jabalpur
E-Mail: **gpariansh@gmail.com**
Mobile No. +91 9098573636
[2] Co-Author:
Assistant Professor
Mangalayatan University Jabalpur
E-Mail: **srishti.soni@mangalayatan.ac.in**
Mobile No. +91 8519001230

ABSTRACT :

In the realm of emerging technology where we are comfortably enjoying its creamy benefits, there exists a corner which is yet to be given due concern. This paper is referring to the Deepfake Technology and the Misinformation it spreads throughout the online persona of many unknown individuals, raising serious concerns about their privacy. With the enormous development of Artificial Intelligence, which we also refer to as A.I. and machine learning, this deepfake technology has taken a huge leap towards the advancement. This technology has found legitimate applications in areas such as film production, online education, and improving accessibility for people with disabilities, showcasing its potential to enhance various sectors. However, the double-edged nature has turned its beneficiary use to a potential misuse. The purpose of this paper is to comprehensively examine how deepfakes have merely become tools for exploitation, harassment, digital fraud, identity theft and most importantly non-consensual pornography. By not raising up the bar properly, this technology has eventually led to raise concerns about the advancements in this technology and its potential misconducts. This paper seeks to analyze these concerns in depth. Numerous studies and cases have revealed how the easily manipulative nature of deepfakes can be weaponized to facilitate crimes, leaving the victims with less or no means of recourse.

In response to these aforesaid challenges, this paper aims to explore the regulative amnesia towards this rapidly evolving technology and the very urgent need for countermeasures mainly pointing towards legal reforms or statutes that indispensably address the rising misuse of deepfakes. Public awareness and education stand as pillars to mitigate the threats posed by deepfake technology. It aims to completely acknowledge and dive deep into the juxtaposed concept of conduct and misconduct of this technology.

KEYWORDS- Deepfake Technology, Cybercrime, Lawful Regulation, Public Awareness, Legal Framework, Digital Media Ethics.

I. INTRODUCTION

With the advancements in technology around the globe, there is also a piece of technology that is more inclined with the modern dynamic world. We refer it to as Artificial Intelligence (AI). Amongst the AI there exists a technology which has made the most significant improvements and advancement in its core technological aspects, known as Deepfake Technology. Deepfake technology refers to AI-powered methods that are used to create or manipulate media, such as videos, images, or audio, to make them appear genuine but are fabricated. This technology utilizes "deep learning" to produce realistic, altered content, which can be used for various purposes, including entertainment and even malicious activities like spreading misinformation[1]. The goal of deepfakes is to create content that is difficult to distinguish from genuine, authentic media which makes it challenging to detect the manipulation.
While initially used for entertainment and creative expression, deepfakes have quickly become tools for misinformation, cyberbullying, and potential fraud[2]. Reports indicate that over a staggering 90% of deepfakes are pornographic in nature, majorly targeting women, highlighting the technology's potential for gendered violence and exploitation[3]. The misuse of this technology can cause severe mental trauma to the victims especially when the

[1] TechTarget, 'Deepfake Technology' https://www.techtarget.com/whatis/definition/deepfake
[2] Aditi Singh, 'Deep Fake Technology: Analysis of Legal Framework and the Way Forward' (2024) https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4868256
[3] The Hindu, 'Regulating Deepfakes and Generative AI in India Explained' (New Delhi, 08 January 2025) https://www.thehindu.com/news/national/regulating-deepfakes-generative-ai-in-indiaexplained/article67591640.ece

fabricated content is being spread without their consent, leading to harsh steps including ending their lives. Thus, it would be evident to state that deepfake technology needs to be highly regulated and for it, various guidelines or regulations must be introduced and compelled with. Currently, India lacks a dedicated deepfake law. While existing laws under the Information Technology Act, 2000 (ITA) and the Indian Penal Code 1860 (IPC), presently the Bhartiya Nyaya Sanhita (BNS) cover some aspects of digital crime, they do not address the unique challenges posed by AI-generated add it rules false media.[4] Lawmakers must adapt legal standards to safeguard societal safety and integrity without frustrating the technological innovations. To address these challenges, society must foster informed public discourse and implement comprehensive legal frameworks to ensure accountability and minimize harm, enabling a responsible use of this powerful technological advancement.[5]

II. DISCOVERING THE TECHNOLOGY BEHIND DEEPFAKES

Deepfake technology utilizes Artificial Intelligence to depict a person as if they are someone entirely different. It can involve manipulating an image, an audio track, a videotape, or any combination of those. Deepfake is a mixture of "deep literacy" and "fake." Tools for editing images, sounds, or vids are not inescapably new. What is new about deepfake is the use of machine learning techniques to make or modify media precisely enough that it is incredibly tough to distinguish from something legitimate. Central to this innovation are techniques such as deep learning and Generative Adversarial Networks (GANs), which enable creators to produce increasingly sophisticated and realistic outputs.[6]

a) Deep Learning

The compound word "deepfake" is formed by combining two English words "deep learning" and "fake." Deep Learning is used in the IT world to denote deep learning, which is a type of Machine Learning - one of the basic techniques that drives artificial intelligence. Deep learning is a key tool in the field of deepfake technology where, the algorithms are trained to identify subjects in videos and photographs. The first step to producing a deepfake is transforming the face images into smaller feature-based representations and dividing them into multiple layers[7]. These layers contain representations of features such as the nose shape, skin tone and eye color. The process starts by training algorithms on extensive datasets of labelled images and videos, allowing them to grasp the intricate details of human appearances and behaviors[8]. The quality and diversity of these directly influence the quality of the generated outputs. By analyzing millions of data points, deep learning algorithms develop a deeper understanding of human features, forming the foundation of deepfake creation.[9]

b) Generative Adversarial Networks (GANs)

GANs or Generative Adversarial Networks were first coined in the year 2014 by Ian Goodfellow. GANs operate with the help of two algorithm frameworks particularly known as a Generator and a Discriminator**.** The generator algorithm is trained using sample imagery, audio, or video to create a new idea or manipulate an existing one that collectively resembles the samples as closely as possible. The discriminator algorithm, meanwhile, is trained to recognize distinctive features in the samples, and point out where the generator misses them so it can go back and correct those inconsistencies. This adversarial process allows the generator to create such authentic deepfakes that neither artificial intelligence nor naked human eyes can point out the difference. GANs enable the creation of increasingly realistic fake media. Early deepfake models struggled with details such as natural eye movements and blinking. By incorporating more diverse and detailed datasets, GANs can now produce outputs that account for the aforesaid discrepancies, resulting in highly lifelike representations.[10]

III. Factors Contributing to the Rise of Deepfakes

Several key factors have contributed to the thunderous growth and accessibility of deepfake technology:

a) ***Data Availability*****:** The dynamism of technological world has given a massive boost to databases consisting of virtual datasets. These datasets are often made freely available to the public which is then used by the generators to retrieve sources that serve as a base for creation of any deepfake.[11]

b) ***Advancements in Cloud Computing*****:** Affordable and accessible cloud computing platforms, such as Amazon Web Services (AWS) have significantly lowered the predominant dependency on highly skilled professionals, enabling individuals with limited resources to create high-quality deepfakes. This has lowered the barrier for individuals to experiment with the technology.[12]

c) ***5G Connectivity:*** The additional bandwidth and reduced latency offered by 5G networks enable seamless streaming of high-quality video content. This connectivity supports real-time applications of deepfakes and enhances their integration into virtual and augmented reality systems.[13]

---

[4] SSRN, 'Deepfake Regulation in India' https://papers.ssrn.com/sol3/papers.cfm?abstract_id=5153296

[5] Blackberry, 'Deepfakes: The Growing Threat' https://www.blackberry.com/us/en/solutions/endpointsecurity/ransomware-protection/deepfakes

[6] Built In, 'What Is a Deepfake? (Definition, How to Spot One)' https://builtin.com/machinelearning/deepfake

[7] Research Gate, 'Deepfake Technology' https://www.researchgate.net/publication/384568279_Dark_sides_of_deepfake_technology

[8] Built In, 'What Is a Deepfake? (Definition, How to Spot One)' https://builtin.com/machinelearning/deepfake

[9] MIT Sloan, 'Deepfakes Explained' https://mitsloan.mit.edu/ideas-made-to-matter/deepfakesexplained

[10] TechTarget, 'What is Deepfake Technology?' https://www.techtarget.com/whatis/definition/deepfake

[11] Built In, 'What Is a Deepfake? (Definition, How to Spot One)' https://builtin.com/machinelearning/deepfake

[12] Infosys, 'Deepfake and It's Impact on Cybersecurity' https://www.infosys.com/services/cyber-security/documents/deepfake-impact-cybersecurity.pdf

[13] Proofpoint, 'What Is a Deepfake? Definition & Technology' https://www.proofpoint.com/us/threatreference/deepfake

d) ***Free Internet:*** Several internet providers are still giving out amenities such as Unlimited 5G network or free internet for some time mainly if the company is generally new in the market, for example – Vodafone & Idea (VI). This leads to users misusing the internet for creating bogus data by utilizing their free network, even for a typically smaller time duration.

IV. THE DARK SIDE OF AI & DEEPFAKE TECHNOLOGY

Deepfake technology, powered by AI, is increasingly misused, threatening personal privacy and societal trust. Originally created for creative purposes, it is now exploited for defamation, blackmail, impersonation, and financial scams.[14]

A. Social Media Trap

Social media platforms act as a fuel for deepfake creation by being a source for large amount of personal data. Any data posted online can be easily exploited and used maliciously. One such incident took place recently where a man created a fake Instagram page with the name of a famous social media influencer where he posted semi-pornographic videos and pictures in the form of reels and posts respectively. Soon enough, the profile got viral and netizens demanded to see the fabricated pornographic content which too, was created by the man as a form of causing harassment to the victim.[15] This led to humongous fan following not knowing the synthetic reality behind the account. Later when this news came in to limelight, there was a massive online outrage amongst the users and a sense of sympathy was flown for the influencer. The man behind this was arrested by the police for allegedly harassment and uploading of morphed photos. Such cases featuring public figures making inflammatory statements underscore the potential to spread misinformation, influence public opinion, and even destabilize societies.[16]

B. Deepfakes as Tools for Deception and Manipulation

The misuse of deepfake technology enables various crimes causing threat to internet persona of individuals, resulting in undermining the privacy, security, and trust in digital world. The deceptive nature of this globalized technology now poses a great threat to the society.

a) Impersonation

Impersonation refers to the act of pretending to be someone else, often with the intent to deceive or commit fraud. With the increasing usage of AI to create deepfakes, it has become quite evident to impersonate others. Criminals can use various AI models to create deepfakes that are highly realistic in audio and video content that can easily depict individuals face shape, voice, and other characteristics allowing them to seamlessly impersonate others.[17] For instance, in one high-profile case, criminals used deepfake videos to impersonate Elon Musk and tricked an 82-year-old retiree named Steve Beauchamp, into investing hefty amount of money into a scam led by the scammers in the name of investments. [18]

b) Defamation

The rise of Deepfake Technology has also given opportunity to defame any person digitally by misusing this technology. Criminals create deepfakes of known or reputed persons and in most of the cases, these deepfakes are made with *mala fide* intention. Deepfake technology facilitates the crime of defamation by enabling the creation of false or misleading media that damages an individual's reputation. Circulation of fabricated content leads to psychological trauma, destruction of professional standings, and even disruption in personal relationships. [19]

c) Non-Consensual Pornography

One of the most harmful uses of deepfake technology is creating non-consensual pornographic content. Such fabricated media causes severe emotional distress, reputational damage, and humiliation, and spreads rapidly online, making it difficult for victims to cope, sometimes leading to tragic consequences.[20]

d) Privacy Violations

Deepfakes has also given rise to privacy violations as they enable the creation of fabricated content by manipulating videos or audios that misrepresents someone's actions, videos, images wrongfully without consent. The most targeted people are mainly high-profile individuals or celebrities as deepfakes can be used to falsely portray their online imprints and their opinions or behaviors. Very relative incident is the deepfake of Shah Rukh Khan's Face into a funny image mainly created with the intention of mockery which is being spread at a massively high rate and causing privacy violations of the actor and infringing upon an individual's right to control how their images are used. [21]

---

[14] Europol, Facing Reality? Law Enforcement and the Challenge of Deepfakes (April 2022) https://www.europol.europa.eu/publications-events/publications/facing-reality-law-enforcement-andchallenge-of-deepfakes

[15] BBC, 'Woman's identity stolen for erotic AI content' https://www.bbc.com/news/articles/cn0znk47x9eo

[16] PECB, 'Biometric Data Protection: Safeguarding Your Digital Identity' (2024) https://pecb.com/article/biometric-data-protection-safeguarding-your-digital-identity

[17] BlinkOps, 'How Cybercriminals Exploit Deepfakes in Cybercrime' (1 November 2024) https://www.blinkops.com/blog/how-cybercriminals-exploit-deepfakes-in-cybercrime

[18] AI Incident Database, 'Deepfake Elon Musk Scam' (14 August 2024) https://incidentdatabase.ai/cite/795/

[19] Europol, Facing Reality? Law Enforcement and the Challenge of Deepfakes https://www.europol.europa.eu/cms/sites/default/files/documents/Europol_Innovation_Lab_Facing_Reality_Law_Enforcement_And_The_Challenge_Of_Deepfakes.pdf

[20] The Regulatory Review, 'Protection against Sexual Violence linked to Deepfake Technology' https://www.theregreview.org/2024/04/13/protecting-against-sexual-violence-linked-to-deepfake-technology/

[21] TOI, 'Hakla Meme of Shah Rukh Khan refuses to die' https://timesofindia.indiatimes.com/etimes/trending/hakla-shah-rukh-khan-meme-refuses-to-die-despite-takedown-attempts-goes-viral-again/articleshow/123113447.cms

V. EXISTING LEGAL FRAMEWORK REGULATING THE DEEPFAKE TECHNOLOGY IN INDIA

While India does not have specific legislation that is targeted for this technology, there exists legal frameworks that aids in reliefs or remedies against the misuse of deepfakes. Laws like the Information Technology (IT) Act, 2000, new provisions in the recently introduced Bharatiya Nyaya Sanhita (BNS), 2023, and the Digital Personal Data Protection Act (DPDP) 2023 offers mechanisms to address issues such as privacy breaches, reputational harm, and the generation & expansion of obscene or misleading content. These frameworks, while effective to an extent, fall short in addressing the complexities of generative AI technologies.

A. Information Technology (IT) Act, 2000

The IT Act is India's cornerstone legislation for cybercrime and online misconduct, with specific sections addressing issues arising from the misuse of deepfake technology.

a) ***Section 66C:*** This section states that whoever fraudulently or dishonestly uses another person's electronic signature, password, or unique identification feature shall be punished with imprisonment of up to three years and a fine of up to one lakh rupees.[22]

b) ***Section 66D:*** This section targets cheating through personation by electronic means. Whoever, by means of any communication device or computer resource cheats by personation, shall be punished with imprisonment of either description for a term which may extend to three years and shall also be liable to fine which may extend to one lakh rupees.[23]

c) ***Section 66E:*** This section penalizes breaches of privacy, such as capturing or transmitting private images without consent. The use of deepfake technology to exploit personal likenesses without permission can be covered under this provision.[24]

d) ***Section 67:*** This section prohibits the electronic transmission of obscene material. Deepfake pornography, a prudent misuse of this technology falls under the ambit of this section and its punishment.[25]

B. Bhartiya Nyaya Sanhita (BNS), 2023

The BNS act, introduced in December 2023, is simply a re-arranged and amended version of the India Penal Code (IPC) 1860. This act also contains provisions to regulate deepfakes, to some extent.

a) ***Section 77 (Voyeurism):*** This provision states that, whoever captures or disseminates the image of a woman engaging in a private act when she expects not to be observed by the perpetrator or by any other person at the behest of the perpetrator is punishable under this section. [26]

b) ***Section 318 (Cheating):*** This provision deals with the act of deceiving a person into taking actions or delivery of property, potentially causing damage or harm to that person in body, mind, reputation or property, is said to commit cheating. It can be invoked when individuals misuse deepfakes with the intention to deceive or harm to the person. [27]

c) ***Section 351 (Criminal Intimidation):*** This provision states that threatening a person with any injury to him/any person in whom he has any interest, intending to cause alarm or cause him to do/not do something, is an offence under Section 351.[28] This section provides remedy to a person to whom criminal intimidation has been made against with the malicious use of deepfakes, to threaten or blackmail him. [29]

d) ***Section 356 (Defamation):*** This section defines defamation as whoever makes or publishes any content, whether verbal, written, signs, or by any visible representations, with the intention of causing harm to the person or his reputation, is said to defame the person. As criminals uses deepfake technology to manipulate the data of an individual aimed at destroying the public image or professional standings, this section provides a legal framework to penalize all those wrongdoers.[30]

C. Digital Personal Data Protection Act (DPDP) 2023

The DPDP Act, 2023 emphasizes the protection of personal data and privacy in the digital age, making it a valuable tool against deepfake-related crimes. The following sections provide remedies for issues arising from the misuse of deepfake technology:

a) ***Section 4:*** This section states that personal data can only be processed with the explicit content of the data principal (the individual to whom the data belongs). This directly addresses the unauthorized use of personal data such as images, videos, and voice recordings frequently exploited in deepfake creation. By stating consent as mandatory, the provision enhances accountability among entities handling sensitive personal data and acts as a preventive measure against its misuse for deepfakes.[31]

---

[22] Information Technology Act 2000 (India), S. 66C

[23] Information Technology Act 2000 (India), S. 66D

[24] Information Technology Act 2000 (India), S. 66E

[25] Information Technology Act 2000 (India), S. 67

[26] Bhartiya Nyaya Sanhita 2023 (India), S. 77

[27] Bhartiya Nyaya Sanhita 2023 (India), S. 318

[28] VIF India, 'Bharatiya Laws Against Deepfake Cybercrime Opportunities and Challenges Meera Srikant' https://www.vifindia.org/article/2025/april/28/Bharatiya-Laws-Against-Deepfake-Cybercrime-Opportunities-and-Challenges

[29] Bhartiya Nyaya Sanhita 2023 (India), S. 351

[30] Bhartiya Nyaya Sanhita 2023 (India), S. 356

[31] Digital Personal Data Protection Act 2023 (India), S. 4

b) ***Section 9:*** This section specifically deals with the processing of personal data of children. It states that the Data Fiduciary shall obtain verifiable consent from the parent or the guardian of the child before processing personal data of the children. Since major victims of deepfakes are children, this section explicitly mandates to acquire consent from the parents before processing the data, which the criminals fail to do so. [32]

c) ***Section 12:*** This section grants individuals the right to correct, complete, update and erasure of misused data, and seek redressal for grievances. Victims of deepfakes can demand the removal of manipulated content, modify, or erase their data, ensuring enforcement and accountability for violations.[33]

VI. JUDICIAL PRECEDENTS AND DOCUMENTED MISUSE: LEGAL DIMENSIONS

There have been numerous examples of people misusing this technology and making a false attempt to gain unfair advantage over a situation. Some of them are listed below:

1. In 2020, a video of an MP went viral on messaging platforms ahead of legislative assembly elections. In the original video the MP was captured speaking in English, against his opponent and encouraging voters to vote for his party. The video was manipulated by his party with a political communication firm to create deepfakes to target voters using over 20 different languages in India. The voice over was done by a dubbing artist and later lip synced using a deepfake software. The content reached over 15 million people on WhatsApp groups.[34]

2. Similarly, In March 2022, amongst the Russia-Ukraine war, a deepfake video of the Ukrainian president Zelensky went viral on social media platforms and news channels, in which he deliberately asked his soldiers to lay down their weapons in the middle of the war. The video was quickly identified as a deepfake and taken down by the authorities.[35]

3. In a recent case of ***Abhishek Bachchan vs The Bollywood Tee Shop & Ors***, the former is the Plaintiff who found that several Defendants were using his long-built goodwill and reputation to produce, sell and were making commercial gains with the use of any technology including but not limited to Artificial Intelligence, Generative Artificial Intelligence, Machine Learning, Deepfakes, Face Morphing, without proper authorization from the Plaintiff. They were involved in selling unauthorized AI generated T-shirts, Ice Posters, Coffee Mugs, Wallpapers and even unauthorized signed posters with the Plaintiff's name and photographs. It also came to the knowledge of the Hon'ble Court that one of the Defendants had a YouTube Channel and was creating AI generated content using the Plaintiff's name, image, likeness, and other attributes of his personality in an unauthorized manner. The Court directed the Defendants to immediately take down, remove, disable, and block all the products URLs identified respective paragraphs.[36]

4. Likewise in the case of ***Jaikishan Kakubhai Saraf Alias Jackie vs The Peppy Store & Ors.*** The Plaintiff initiated a lawsuit seeking inter-alia protection of his own name, image, likeness, persona, voice, and various other distinctive attributes of his personality against unauthorized and misuse over the internet as one of the Defendant allegedly was creating content using artificial intelligence (Gen AI) tools exploiting the Plaintiff's image and persona, while the other Defendant created an unlicensed Artificial Intelligence Chatbots that would reply in a matching voice of the Plaintiff. Moreover, one of the Defendant was involved in the circulation of links which were pornographic in nature and used the Plaintiff's name in the said links. The Hon'ble Court held that the said material is prima-facie prejudicial to the Plaintiff's reputation and violates his personality rights, thus the Defendant's are required to restrain and immediately stop the circulation of any such products.[37]

5. By looking at the above cases it is very evident to say that the rise of Artificial Intelligence and Deepfake technology has programmed majority of the population to misuse it instead of using it for some beneficial purpose. We are still unaware of the bare minimum digital media ethics that would significantly lower the risks of falling into the trap of this technology laid by the perpetrators. If not duly regulated, this technology would abrupt a massive fire with little to no means of water left to extinguish it.

6. For instance, In ***Sadhguru Jagadish Vasudev & Anr vs Igor Isakov & Ors***, a very renowned globally revered spiritual leader/ yogi/ mystic/ public figure with millions of followers across the globe filed a lawsuit against the Defendants because they were allegedly involved in unlawful usage of the plaintiff's personality rights and were streaming online content by using modern technology and AI tools to unauthorizedly morph and doctored the Plaintiff No. 1's voice and discourses/ speeches/ interview(s) to, inter alia, create deep fakes, in the nature of false, misleading and unlawful images, audio-visual advertisements/ videos. Moreover, the Defendants were perpetuating a financial scam by initiating commercial transactions and/or promoting and selling purported services for gaining traction on social media through AI-generated motivational and inspirational talks/ speeches purported to be originating from Plaintiff No.1. The Hon'ble Court in this case granted

[32] Digital Personal Data Protection Act 2023 (India), S. 9

[33] Digital Personal Data Protection Act 2023 (India), S. 12

[34] 'MP caught using AI to create Deepfake' https://www.thehindubusinessline.com/news/national/bjp-leader-manoj-tiwari-used-deepfake-videos-to-reach-out-to-voters-in-delhi-report/article30857871.ece

[35] TheIndianExpress, 'Ukrainian President Deepfake' https://indianexpress.com/article/world/ukraine-deepfake-video-zelenskyy-7824017/

[36] Abhishek Bachchan V. The Bollywood Tee Shop & Ors [2025 SCC OnLine Del 5944]

[37] Jaikishan Kakubhai Saraf Alias Jackie V. The Peppy Store & Ors. [CS(COMM) 389/2024]

relief in favour of the Plaintiffs and directed the Defendants to suspend or takedown any URSs, links, fabricated content that was infringing the Plaintiffs exclusive rights.[38]

7. In mid-2024 arose a case of similar nucleus whereby the Defendants published deepfake videos on social media (Facebook / Instagram / WhatsApp / Telegram) that showed an AI-generated persona of the MD & CEO of National Stock Exchange of India Ltd. (NSE). These videos purportedly encouraged investors to join a WhatsApp group for stock-picking tips, claiming that "NSE recommends stocks weekly," and promised reimbursement for losses if the advice was followed with due diligence. These videos also displayed the NSE trademark logo & branding to give an impression of official sanction or endorsement. The Hon'ble Court in ***National Stock Exchange Of India vs Meta Platforms Inc*** held that the videos were false, misleading, and infringing, and that continuing circulation would cause irreparable damage and also emphasized that under the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021 (IT Rules), intermediaries have a duty to take prompt action on complaints about prohibited content, including false or misleading content.[39]

8. The entire suit arose because AI-generated deepfake videos used the likeness and voice of NSE's CEO to mislead investors. This shows how deepfakes can be weaponized for financial fraud, misrepresentation, and manipulation of public trust. The aforesaid case is one of the first Indian precedents where a High Court gave explicit directions against AI-generated deepfake content.

VII. RECOMMENDATIONS AND SUGGESTIONS FOR REGULATING DEEPFAKE

Despite the present legal frameworks in India, we still lack a dedicated regulatory framework that has been drafted with the sole purpose of addressing the misuse of deepfake technology and its applications. Existing laws act as reactive measures rather than preventive measures. To address the growing challenges derived from deepfakes, a set of regulative reforms are recommended:

a) ***General Preventive Measures:*** A direct approach to regulate deepfakes requires enacting specific laws targeting their misuse. These laws should clearly define what constitutes a deepfake, outline its potential harm, and set strict penalties for their creation, distribution, or misuse, ensuring that people who exploit this technology are held accountable. Additionally, regulatory bodies must collaborate with technology and ethics experts to monitor emerging threats and stay ahead of evolving risks.[40]

b) ***Intermediaries Obligation and Liability****:* Intermediaries such as social media platforms play a crucial role in managing deepfakes and preventing their misuse shall be a topmost priority. They should not only be held accountable for posted content but also for taking preventive steps to decrease the creation of deepfakes. A key aspect to achieve this would be enforcing strict guidelines for users taking advantage of GenAI and to require platforms to label AI-generated content identification for the benefit of users. [41]

c) ***Enhanced Reporting Structure:*** A robust and easy-to-use reporting structure must be established, empowering citizens to easily report suspicious deepfakes and social media platforms must actively monitor and manage deepfake content through these systems, ensuring prompt review and removal of reported content. India's ability to identify and remove fabricated content has always been relatively moderate, thus it requires sharp focus on implementing such easy-to-use reporting mechanism before the content goes viral all over the internet.

d) ***Situational Public Awareness:*** The most effective and comprehensive step that should be taken to mitigate the effects of deepfake should be addressing at the grassroot levels. Public awareness campaigns and educating individuals about the uses and misuses of deepfake technology, how to identify them, and what steps to take if they encounter harmful content or even if they are the victims of this technology. Through widespread awareness programs, individuals will be better equipped to identify deepfakes and resist the influence of misinformation.

VIII. CONCLUSION

Deepfake technology is one of the most pressing challenges in the digital era, merging remarkable innovation with potential harm. While its underlying AI-powered mechanisms can create beneficial applications, the same capabilities are highly misused to spread misinformation, initiate fraud, and cause irreparable harm to individual's dignity and privacy. The absence of a dedicated legal framework in India leaves an open gap, forcing reliance on provisions given under the IT Act, BNS, and DPDP Act, which are largely reactive rather than preventive. Effective regulation must go beyond reactive measures, it requires an approach combining legislative clarity, technological safeguards, platform accountability, and public awareness. By establishing differentiating factors, strict penalties, and robust reporting systems, along with educating citizens to critically identify the fabricated content, society can foster the benefits of AI while minimizing its misuse. In this way, India can strike the crucial balance between fostering innovation and safeguarding the rights, security, and trust of its people in the face of this evolving digital threat.

---

[38] Sadhguru Jagadish Vasudev & Anr V. Igor Isakov & Ors [CS(COMM) 578/2025]

[39] National Stock Exchange Of India V. Meta Platforms Inc [Interim Application (L) No. 21456 of 2024 in Com IPR Suit (L) No. 21111 of 2024, Bombay High Court]

[40] IndiaAI, 'New Laws and Penalties for Creators and Platforms to Address Deepfakes' https://indiaai.gov.in/news/new-laws-and-penalties-for-creators-and-platforms-to-addressdeepfakes

[41] Bar and Bench, 'Intermediary Liability' https://www.barandbench.com/view-point/generative-ai-and-intermediary-liability-under-the-information-technology-act

IX. REFERENCES

1. Abhishek Bachchan V. The Bollywood Tee Shop & Ors [2025 SCC OnLine Del 5944]
2. AI Incident Database, 'Deepfake Elon Musk Scam' (14 August 2024) https://incidentdatabase.ai/cite/795/
3. Bar and Bench, 'Intermediary Liability' https://www.barandbench.com/view-point/generative-ai-and-intermediary-liability-under-the-information-technology-act
4. BlinkOps, 'How Cybercriminals Exploit Deepfakes in Cybercrime' (1 November 2024) https://www.blinkops.com/blog/how-cybercriminals-exploit-deepfakes-in-cybercrime
5. Built In, 'What Is a Deepfake? (Definition, How to Spot One)' https://builtin.com/machinelearning/deepfake
6. Europol, Facing Reality? Law Enforcement and the Challenge of Deepfakes https://www.europol.europa.eu/cms/sites/default/files/documents/Europol_Innovation_Lab_Facing_Reality_Law_Enforcement_And_The_Challenge_Of_Deepfakes.pdf
7. Hindustan Times, 'Fake AI Generated Profile' https://www.hindustantimes.com/india-news/assam-man-arrested-for-creating-fake-profile-ai-generated-images-of-influencer-archita-phukan-101752383365208.html
8. Infosys, 'Deepfake and It's Impact on Cybersecurity' https://www.infosys.com/services/cyber-security/documents/deepfake-impact-cybersecurity.pdf
9. Jaikishan Kakubhai Saraf Alias Jackie V. The Peppy Store & Ors. [CS(COMM) 389/2024]
10. MIT Sloan, 'Deepfakes Explained' https://mitsloan.mit.edu/ideas-made-to-matter/deepfakesexplained
11. MP caught using AI to create Deepfake https://www.thehindubusinessline.com/news/national/bjp-leader-manoj-tiwari-used-deepfake-videos-to-reach-out-to-voters-in-delhi-report/article30857871.ece
12. National Stock Exchange Of India V. Meta Platforms Inc [Interim Application (L) No. 21456 of 2024 in Com IPR Suit (L) No. 21111 of 2024, Bombay High Court]
13. PECB, 'Biometric Data Protection: Safeguarding Your Digital Identity' (2024) https://pecb.com/article/biometric-data-protection-safeguarding-your-digital-identity
14. Proofpoint, 'What Is a Deepfake? Definition & Technology' https://www.proofpoint.com/us/threatreference/deepfake
15. ResearchGate, 'Dark Sides of Deepfake Technology' https://www.researchgate.net/publication/384568279_Dark_sides_of_deepfake_technology
16. Sadhguru Jagadish Vasudev & Anr V. Igor Isakov & Ors [CS(COMM) 578/2025]
17. TechTarget, 'Deepfake' https://www.techtarget.com/whatis/definition/deepfake
18. The Regulatory Review, 'Protection against Sexual Violence linked to Deepfake Technology' https://www.theregreview.org/2024/04/13/protecting-against-sexual-violence-linked-to-deepfake-technology/
19. TheIndianExpress, 'Ukrainian President Deepfake' 7 https://indianexpress.com/article/world/ukraine-deepfake-video-zelenskyy-7824017/
20. VIF India, 'Bharatiya Laws Against Deepfake Cybercrime Opportunities and Challenges Meera Srikant' https://www.vifindia.org/article/2025/april/28/Bharatiya-Laws-Against-Deepfake-Cybercrime-Opportunities-and-Challenges