DEEPFAKE TECHNOLOGY: ANALYSING THE LEGAL CHALLENGES AND THE INDIAN FRAMEWORK

Paridhi Kurre, Hidayatullah National Law University

Taniya Khusbu Kujur, Hidayatullah National Law University

I. INTRODUCTION

Deepfake, a term that attained popularity in 2017, is another phenomenon in the world of synthetic media. Deepfake technology is an artificial intelligence mechanism produced using machine learning techniques to create synthetic and hyper-realistic media, such as audio, video, images, etc. Deepfake is a portmanteau of "deep learning" and "fake"[1]. It arose in 2017 when a Reddit user with a similar moniker posted edited videos. A face-swap video is made in a few steps. The two people's hundreds of facial images are first put through an encoder, an AI algorithm. The encoder identifies and remembers similarities among the two faces, reducing them to their shared characteristic and compressing the images. Such features are then trained to be recovered first from compressed photos by a second AI system known as a decoder.[2]

The worldwide recognition of deepfake media has become prominent these days. Today, youth and even the younger generation constantly interact with deepfake videos and images, morphed and altered in a certain manner on different social media platforms, namely Instagram, Facebook, YouTube, Reddit, etc. According to a news article, "More than 75% of Indians present online and surveyed by cybersecurity company McAfee have seen some form of deepfake content over the last 12 months, while at least 38% of the respondents surveyed have encountered a deepfake scam during this time[3]. The deepfake technology is mainly being influenced by a massive number of people unknowingly forwarding the deepfake content on social platforms such as WhatsApp and Telegram groups, which leads to the exponential spread of misinformation. The deepfake issue is well recognised, yet many people are unfamiliar with

[1] 'Deepfake' (Wikipedia) <https://en.wikipedia.org/wiki/Deepfake> accessed 13 January 2025
[2] Aranya Nath & Sreelakshmi B, 'Deepfakes on Copyright Law- Inadequacy of Present Laws in Determining the Real Issues' (2004) 15(1), Indian Journal of Law and Justice 287
[3] '75% Indians have viewed Some deepfake content in last 12 months says McAfee survey' (The Economic Times) <https://economictimes.indiatimes.com/tech/technology/75-indians-have-viewed-some-deepfake-content-in-last-12-months-says-mcafee-survey/articleshow/109599811.cms?from=mdr> accessed 13 January 2025

distinguishing such media and information, and public awareness is limited.

The Indian legal framework cannot help the people victimised by deepfake scams enough, as it lacks specific regulations targeting deepfakes. Although certain provisions under the Information Technology Act exist, there is no comprehensive legislation addressing the unique challenges of technology. In short, India is still in the early stages of developing such targeted legislation. Certain legislation, such as the *Bhartiya Nyaya Sanhita, 2023* and the *Information Technology Act 2000*, safeguards individuals from privacy breaches, defamation and such misuse of technology. These regulations identify the gaps present in the Indian framework and protect the victims from cyber harms. For this reason, India has an increasing number of deepfake frauds. According to a report, "Deepfake cases in India have surged by 550 per cent since 2019, with losses projected to reach Rs70,000 crore in 2024 alone. Deepfake fraud now constitutes 40 per cent of all AI-related cybercrimes globally, alongside other threats such as cybercrime automation and AI-enhanced privacy invasion."[4] Such cases exemplify that deepfake frauds are frequently detected only after harm has taken place, thereby demonstrating the limitation of the Indian legal framework.

This article will analyse the interconnection of deepfake technology with divergent laws and the requirement of deepfake legislation in the Indian framework.

II. ANALYSING THE CONNECTION BETWEEN DEEPFAKE TECHNOLOGY: COMMUNICATION, ENTERTAINMENT AND MEDIA LAW

1. DEEPFAKE TECHNOLOGY AND COMMUNICATION

Deepfake technology has been used by the majority of people to exploit communication. Communication through deepfakes leads to several major issues, such as hate speech, misinformation, harassment, elections and political ethics. People fabricate deepfake images, videos, and audio through social media, which can lead to misinformation. It can take many forms, such as memes, misattributed content, fabricated or cloned websites and news.[5] Deepfake memes can inappropriately represent any individual, and they may also lead to

[4] 'India's Deepfake Cases Up 550%, Losses May Hit Rs 70,000 Cr By 2024: Report' (BW Businessworld) <https://www.businessworld.in/article/indias-deepfake-cases-up-550-losses-may-hit-rs-70000-cr-by-2024-report-541202> accessed 13 January 2025

[5] 'Misinformation and Disinformation and Deep Fakes' (University of Essex) <https://www.essex.ac.uk/research-projects/human-rights-big-data-and-technology/misinformation-and-disinformation-and-deep-fakes> accessed 13 January 2025

societal variations. Misinformation generated through deepfake video, audio and images provides fake content to a group of people, and this fake news leads to misinformation, which can also defame and mislead people. For example, Deepfakes blur the line between reality and fabrication by creating highly convincing fake media. This erodes trust in visual evidence and challenges the authenticity of digital content. Misinformation can easily gain credibility when it is disguised as a genuine video or image, making it more likely to be shared and believed by unsuspecting individuals.[6] The study, conducted by the "Indian School of Business (ISB)" and "Cyberspace", showed that with social media emerging as the primary vector of misinformation, fake news and deepfakes concerns are rising in the country. Social media platforms are the dominant source of misinformation, responsible for 77.4% of cases compared to just 23 per cent originating from mainstream media. Twitter (61 per cent) and Facebook (34 per cent) were identified as the leading platforms for spreading fake news.[7]

Political deepfake misinformation has also been escalating these days. The study analysed a substantial number of fake news stories, revealing that political fake news accounts for the most significant share (46 %), followed by general issues (33.6 %) and religion (16.8 %).[8] There have been numerous occurrences worldwide where deepfakes have been employed to advance political interests by exploiting the likeness and image of renowned political figures.[9] In 2020, India witnessed its first-ever use of AI-generated deepfake technology in political campaigning when several deepfake videos of politician Manoj Tiwari were circulated on WhatsApp groups. These videos depicted Tiwari making accusations towards his political rival Arvind Kejriwal in both English and Haryanvi languages, preceding the elections in Delhi, the Indian capital state.[10]

The excessive use of deepfakes in political communications highlights serious weaknesses in India's legal system for regulating digital content and administering elections. Deepfakes often spread widely even before authorities become aware, as the content can be created and circulated rapidly. There are currently no clear and specific laws that address or punish the creation and spread of such deepfake content. The country also lacks an effective system for

[6] Hassan Hadi Saleh and others, 'Impact of Deepfake Technology on Social Media: Detection, Misinformation and Societal Implications' (2023) 23 The International Society for Research in Education and Science 431
[7] 'Nearly Half of The Fake News Stories in India Are Political: Study' (NDTV) <https://www.ndtv.com/india-news/nearly-half-of-the-fake-news-stories-in-india-are-political-study-7291481> accessed 13 January 2025
[8] Ibid
[9] Shinu Vig, 'Regulating Deepfakes: An Indian perspective' (2024) 17(3) Journal of Strategic Security 74
[10] Ibid

real-time monitoring and has no immediate mechanism to compensate for the damages caused. Such content also shapes the voters' thinking and opinion. Hence, deepfake technology through communication from social media and political campaigns influences people's interests, which can lead to severe misinformation and the dissemination of false news.

2. DEEPFAKE TECHNOLOGY AND ENTERTAINMENT

Deepfake holds significant potential for positive applications across a variety of fields, from entertainment to humanitarian efforts and education. Notably, it's making quite an impact on the entertainment industry. The entertainment industry seems as a major beneficiary of deepfake technology, utilising it to produce top-notch content. Deepfakes have played a pivotal role in generating lifelike characters in movies, TV shows and video games.

While deepfake technology offers such advantages to the entertainment industry, it simultaneously poses risks and challenges, as deepfakes enable creators to manipulate anyone's image into hyper-realistic video, audio, or image without their consent, thus posing an equal risk. "Deepfakes can be used to manipulate and cheat people by making it appear as if someone is saying or doing something that they never did. This might include creating fake videos of persons engaged in illegal or immoral activities, making false statements, or engaging in inappropriate conduct."[11] Youtuber Jimmy Donaldson, popularly recognised as Mr. Beast, recently became the victim of a misleading AI-generated deepfake advertisement.[12] "Celebrity and revenge pornography were among the early malicious uses of a deepfake."[13] In 2017, when the deepfake technology was first used to generate pornographic content by an anonymous Reddit user, the video was created using the images of Hollywood actors Gal Gadot, Emma Watson, Katy Perry, Taylor Swift, and Scarlett Johansson.

Another prominent incident in India involved a well-known Indian actress, Rashmika Mandanna, superimposed onto the body of a British Indian influencer. This use of deepfake violates the "Right to Publicity" under entertainment law. The "Right to Publicity" aims to protect celebrities' interests by controlling the use of their images and identities. This safeguards the rights of celebrities to prevent or seek compensation for commercial uses or

[11] Vig, 'Regulating Deepfakes' 75
[12] Tom Gerken, 'Mr Beast and BBC stars used in deepfake scam videos' (BBC News) <https://www.bbc.com/news/technology-66993651> accessed 14 January 2025
[13] Ashish Jaiman, 'Debating the ethics of deepfakes' (Orfonline, 27 August 2020) < https://www.orfonline.org/expert-speak/debating-the-ethics-of-deepfakes > accessed 14 January 2025

limitations of their facial features, vocal characteristics, unique expressions, signature poses, and other distinguishing attributes. India does recognise the right to publicity, yet it has no such exclusive law. Nevertheless, the Right to publicity is legally enforceable in Indian courts. For instance, in **ICC Development (International) Ltd v Arvee Enterprises,**[14] the Delhi High Court has passed a judgment stating the right of publicity is exclusive to a person or any manifestations of his/her persona, such as their name, personal attributes, autograph, or vocal characteristics. Nonetheless, the unauthorised use of a celebrity's persona, image, or information constitutes a violation of their right to publicity and can be legally challenged. Therefore, if a deepfake uses the image or voice of a well-known individual, it breaches their right to privacy.

Although the right to publicity has been recognised by the Indian courts, it means people have jurisdiction over the commercial and public use of their identity. India lacks a comprehensive law that specifically deals with digital content or AI-generated content like deepfakes. An unclear statutory framework creates uncertainty about how such cases should be enforced in practice. Judicial remedies are generally slow, and victims often depend heavily on courts to get relief. The issue of deepfakes is also case-specific, which makes them ineffective against their massive scale. Deepfakes are also produced and circulated expeditiously in the digital entertainment and media ecosystem.

3. DEEPFAKE AND MEDIA

Deepfakes have been used extensively by numerous people throughout digital media. Information shared across social media through deepfake images, audio and videos contributes substantially to misinformation and forged news. The growing popularity of deepfake content on social media challenges the authenticity of media; as a consequence, the circulation of replicated images, texts and audio on social media platforms growingly appears original. False resemblances of women and their voices are reproduced through deepfakes and circulated in the media, which can lead to matters of sexual harassment and defamation. According to social media analytics firm Twicsy, 84 per cent of social media influencers have fallen victim to deepfake pornography.[15]

[14] ICC Development (International) Ltd v Arvee Enterprises (2023) 26 PTC 245 (Del) [14]
[15] Ankita Deshkar, 'your photos aren't safe: How deepfake tech is being weaponised, and how to fight back' (The Indian Express, 2 May 2025) <https://indianexpress.com/article/technology/tech-news-technology/how-deepfake-tech-is-weaponised-and-how-to-fight-back-9771402/> accessed 14 January 2025

Deepfake content has also gained popularity through YouTube videos, where the clips posted seem so original, making it challenging for viewers to differentiate them from exploited content. For example, a YouTube channel named BuzzFeed Video uploaded a deepfake video of Barack Obama, in which he conveyed how the nation is entering an era in which rivals can make it seem like someone makes a statement, even if they would never say those statements, the video also displayed Barack Obama saying "Dipshit" to Donald Trump. The clip made the entire video extremely original, and it appeared as if he was expressing those certain things. With the growing number of deepfakes on social media, people's judgement can be impacted by events or moments that rarely happened. Even if the deepfake is eventually (or quickly) revealed, the initial impact on the audience can be difficult to recover.[16]

Hence, deepfake technologies are getting recognized these days, and directions has been provided for individuals on how to detect deepfake images, videos and many more on several media platforms, due to rising cases of deepfakes in digital media, several indicators can help you identify a deepfake on your own, such as inconsistent lighting, blurriness around the face or hair, mismatched audio, or something off about the eyes, such as too much or too little blinking. [17]

III. THE VIOLATION OF PRIVACY RIGHTS

In the given case, **"K.S. Puttaswamy vs Union of India"**[18] The court declared the right to privacy as a fundamental right under Article 21 of the Constitution. With the widespread use of deepfake technology, this technology has been used on social media through different AI platforms to generate deepfake photos and videos of an individual without their consent, leading to the violation of privacy rights. For instance, in the case of **Anil Kapoor vs Simply Life India & Ors**,[19] Actor Anil Kapoor sought protection against the unauthorised use of his persona through deepfake technology, and the Delhi High Court issued an order to prevent Kapoor's name, likeness, voice, and other distinctive features from being misused online; thus, this case establishes legal recognition of deepfake technology and the urgency of protecting

[16] Kate Coleman, 'How Deepfakes are Impacting Culture, Privacy, and Reputation' (Status lab) <https://statuslabs.com/blog/what-is-a-deepfake> accessed 14 January 2025
[17] Ibid
[18] K.S. Puttaswamy vs Union of India AIR 2017 SC 4161
[19] Anil Kapoor vs Simply Life India & Ors CS (COMM) 652/2023 (Delhi High Court)

people's privacy rights.[20]

However, the development of deepfake technology has critically affected the reputation of women across the world through deepfake pornography. Deepfake technology uses women's audio and images to generate non-consensual content, leading to the violation of privacy rights. The *2023 State of Deepfakes report* estimates that at least 98 per cent of all deepfakes are porn and 99 per cent of the victims are women.[21] The creation of Deepfake porn was used to exploit individuals to receive money through blackmail. For instance, in Ghaziabad, an elderly man was allegedly cheated of Rs 74,000 using an altered video of the former cop. The deepfake video that went viral online purportedly showed Prem Prakash as a retired Additional Director General of Police, on a video call with an elderly man's daughter. On November 4th, Arvind Sharma, 74, received two video calls from the accused. He disconnected the first call after a naked woman appeared on the screen, and the second call appeared as a male police officer who threatened him with jail if he didn't pay up. Out of fear, he transferred Rs 74,000.[22] These cases demonstrate how women's privacy has been breached by using their photos without consent to generate non-consensual deepfake pornography, leading to severe damage to their reputation.

Deepfake technology has also been widely used against high-profile celebrities and social media influencers to ruin their persona or for entertainment purposes, resulting in the violation of their privacy rights. This misuse occurs because deepfake technology exploits celebrities' and influencers' images and audio to create content without their consent, often resulting in unethical or non-consensual content. According to social media analytics firm Twiscy, 84 per cent of social media influencers have fallen victim to deepfake pornography, and among this group 90% are female.[23] Influencer-based deepfake pornography has approximately 400 million views, showing an alarming interest in exploitative content.[24] This issue is not limited

[20] Nupur Thapliyal, 'Delhi High Court Protects Actor Anil Kapoor's Personality Rights, Restrains Misuse of His Name, Image or Voice Without Consent' (Live Law, 20 September 2023) <https://www.livelaw.in/top-stories/delhi-high-court-anil-kapoor-voice-image-misuse-personality-rights-238217> accessed 15 January 2025
[21] Subham Tiwari, 'Inside thriving deepfake porn bazaar' (India Today, 5 December 2023) <https://www.indiatoday.in/india/story/deepfake-porn-artificial-intelligence-women-fake-photos-2471855-2023-12-04> accessed 15 January 2025
[22] Chandrajit Mitra, 'Retired Top Cop Latest Victim of Deepfake, Video Used to Con Ghaziabad Man' (NDTV, 30 November 2023) <https://www.ndtv.com/ghaziabad-news/retired-top-cop-latest-victim-of-deepfake-video-used-to-con-ghaziabad-man-4621233> accessed 15 January 2025
[23] Deshkar, 'Your photos aren't safe'
[24] 'Over 90% female Instagram influencers fall victim to deepfake pornography, finds study' (The Hindu) <https://www.thehindu.com/sci-tech/technology/over-90-female-instagram-influencers-fall-victim-to-deepfake-pornography-finds-study/article68196062.ece> accessed 16 January 2025

to influencers; even legendary actors have been targeted due to the deepfake technology. In the case of **Amitabh Bachchan Vs. Rajat Negi and Ors.,**[25] the court granted ad interim in rem injunctions against the unauthorised use of his personality rights and personal attributes such as voice, image, and likeness for commercial use. [26]

Deepfake technology also contributes to breaches of data privacy. A data privacy breach occurs when a third party accesses the data submitted to a trusted website without authorisation.[27] Over the years, various companies have observed data breaches in which names, phone numbers, bank details, and social security numbers have been accessed and leaked.[28] Such data breach led to violation of privacy rights, as the individuals were unaware of how their numbers and bank details were being used to carry out fraud. Bhumi Pednekar, an Indian actress, recently addressed the issue of such videos, emphasising their impact on safety. She told *India Today* that not only is it a privacy violation, but it also infringes upon fundamental rights and safety, particularly for women. Imagining the emotional toll of encountering such inappropriate use of personal imagery is challenging. The act transcends mere privacy invasion, becoming a profound violation of personal boundaries.[29]

IV. EVOLUTION OF DEEPFAKE TECHNOLOGY FRAUD IN PREVALENT TIMES

Deepfake technology, like many other innovations, was initially created for positive and other beneficial purposes. Unfortunately, we have embarked on an irresponsible journey by misusing deepfake technology, which has led to several significant scandals. It opens unprecedented possibilities of fraud and misrepresentation. The technology is capable of face swapping, voice cloning, and body manipulation, often used to create fake identities, audio-visual deepfakes, and to impersonate individuals. These factors lead to a significant number of digital and financial frauds. By using this technology, scammers make audio and video calls to

[25] Amitabh Bachchan Vs. Rajat Negi and Ors CS(COMM) 819/2022 (Delhi High Court)
[26] Vikrant Rana, Anuradha Gandhi and Rachita Thakur, 'Deepfakes and Breach of Personal Data – A Bigger Picture' (Live Law, 24 November 2023) <https://www.livelaw.in/law-firms/law-firm-articles-/deepfakes-personal-data-artificial-intelligence-machine-learning-ministry-of-electronics-and-information-technology-information-technology-act-242916?fromIpLogin=31023.340622574393> accessed 16 January 2025
[27]'Ethical Concerns in Generative AI: Tackling Bias, Deepfakes, and Data Privacy'(Hyqoo) <https://hyqoo.com/artificial-intelligence/ethical-concerns-in-generative-ai-tackling-bias-deepfakes-and-data-privacy/> accessed 16 January 2025
[28] Ibid
[29] 'Bhumi Pandekar Speaks Out Against Deepfake Technology, Labelling It A 'Breach of One's Privacy' (Time of India) <https://www.msn.com/en-in/entertainment/bollywood/bhumi-pednekar-speaks-out-against-deepfake-technology-labelling-it-a-breach-of-ones-privacy/ar-BB1hHCwv?ocid=BingNewsVerp> accessed 16 January 2025
[29] Ibid

demand a hefty amount of money. The scammer usually pretends to be a higher-up, such as a police officer, or impersonates a boss or CEO of the employee, asking them to send money. For instance, an accounts manager received a WhatsApp message from a fraudster impersonating the company's managing director. Using the company logo as the profile picture, the scammer requested Rs 1.15 crore, claiming it was an advance for a new project. The manager transferred the funds without verification.[30]

The kinds of ongoing deepfake frauds are as follows:

1) DEEPFAKE CALLS

Deepfake calls are pointed out as phone scams that use voice cloning to create false audio clips impersonating the voices of relatives and victims, such as friends and family, asking for financial help. Deepfake calls violate *Section 66D of the Information Technology Act*,[31] which specifies cheating by personation by means of any communication device or computer resources, and *Section 319 of the Bhartiya Nyaya Sanhita*,[32] which refers to "Cheating by Personation". Calls are extremely compelling as they sound like a genuine individual. This has made it easier for criminals to create these fake calls and exploit people's trust.

In one case, a 73-year-old man in India fell victim to a deepfake scam after receiving a call, impersonating his former colleague, requesting for money. The scammer used deepfake technology to create a video call in which the impersonator's face and voice matched the victim's former colleague. The victim transferred money before realising he had been tricked.[33] In another case, a man from Kanpur was scammed out of Rs. One lakh by using deepfake technology. The scammer called him, impersonating his nephew and claiming he was arrested on serious charges. Believing the call was genuine, the man transferred the money but later realised he had been duped when he contacted his real nephew.[34] Scamsters strategically put victims under intense mental pressure, accusing them of knowingly or unknowingly engaging

[30] Surbhi Gloria Singh, 'Fake CEOs swindle Rs 7 crore from Delhi firms: Modus operandi explained' (Business Standard, 4 December 2024) <https://www.business-standard.com/finance/personal-finance/fake-ceos-swindle-rs-7-crore-from-delhi-firms-modus-operandi-explained-124120400763_1.html accessed 17 January 2025
[31] Information Technology Act 2000, s 66D
[32] Bhartiya Nyaya Sanhita 2023, s 319
[33] Alison Grace Johansen, 'What are deepfakes and how to spot them' (The Guardian,13 January 2020) <https://in.norton.com/blog/emerging-threats/what-are-deepfakes> accessed 18 January 2025
[34] 'Man Duped Of ₹1 Lakh in Ai Deepfake Scam' (The Times of India) <https://timesofindia.indiatimes.com/city/kanpur/man-duped-of-1-lakh-in-ai-deepfake-scam/articleshow/109208459.cms> accessed 18 January 2025

in serious crimes. They leverage modern technology, and with the rise of deepfake technology, it has been increasingly used to fabricate evidence and coerce individuals, revealing significant gaps in India's legal framework.

2) DIGITAL ARREST

Amidst the ongoing digital scams, there has been a surprising rise in a new form of digital crime called digital arrest scams. Such a scam involves scammers imitating law enforcement officials by using body manipulation, voice cloning, and face-swap technology to persuade victims that they are under a digital or virtual arrest. The scammers share the victims' details, relatives' names, and their relationships with the victims to make the victims believe the scammers are real officers and that the victims are under arrest. To get out of such digital arrest, the scammer, disguised as a police officer, demands a large sum.

The following are some digital arrest incidents in recent times.

An elderly woman in South Mumbai was scammed out of Rs. 1.5 crore by fraudsters posing as Special Investigation Team (SIT) officers. They claimed she was under investigation for money laundering and drug-related offences. The scammers used video calls and forged documents to convince her, and she ended up transferring the money to multiple accounts provided by the criminals. She realised the scam after discussing it with a family member and reported it to the police.[35]

Another incident involves retired professor Kamta Prasad, from Bihar, India, who fell victim to such a digital arrest scam within five hours. The fraudsters impersonated the police and the Telecom Regulatory Authority, convincing him that his Aadhaar ID was being misused for illegal payments. Terrified by the threats of arrest, Prasad transferred Rs 13 lakhs to prove his control over his bank account.[36]

However, with the development of deepfake technology, there has been a rise in such scams, and vulnerable sections of society that are not aware of digital fraud are easily targeted. The

[35] 'Mumbai: Elderly woman loses ₹1.5 crores in 'digital arrest, scammers pose as SIT officers' (Hindustan Times, 2 January 2025) <https://www.hindustantimes.com/india-news/mumbai-elderly-woman-loses-rs-1-5-crore-in-digital-arrest-scammers-pose-as-sit-officers-101735820771904.html> accessed 18 January 2025

[36] 'I'm Ruined: Digital Arrest' Scammers Stealing People's Savings in India' (NDTV, 20 January 2025) <https://www.ndtv.com/india-news/digital-arrest-scammers-stealing-peoples-savings-in-india-im-ruined-7514718> accessed 18 January 2025

Indian legal framework does not comprehensively address these issues, thus making victims more vulnerable to financial fraud.

3) ROMANCE SCAM

A romance scam is a confidence trick where a scammer pretends to have romantic intentions towards a victim, gains their affection and trust, and then uses that trust to manipulate them into sending money or providing personal information. Romance scammers often indulge in identity theft to create fake identities on dating sites or social media platforms. These scams involve criminals gathering information from various sources to create convincing counterfeit identities across different online platforms. They chat with the victim, share stories, and build an emotional connection. Then they use deepfake technology to generate highly realistic video calls. Once the trust is established, the scammers come up with urgent situations, such as medical emergencies or requiring money for travel or any other kind of financial urgency. The scammers often request money through untraceable methods like gift cards, wire transfers, or cryptocurrency. Such scammers usually come up with excuses to avoid meeting the victim, claiming they are travelling or working abroad.

For instance, the Yahoo boy scam, one of the most prominent romance scams, included the cyber fraudsters based in Nigeria who utilized face-swapping apps and software to conduct real-time video calls with unsuspecting victims. The FBI reported that over USD 650 million has been lost to such romance scams.[37] Another such incident is from Vizag, where a 25-year-old fraudster scammed an engineer using fake profiles and emotional manipulation to extract a sum of Rs 28 lakhs on a dating app.[38] These incidents demonstrate how such scams are not generally recognised among citizens, thereby exposing them to financial fraud and coercion.

4) QR CODE SCAMS

QR code scams involve fraudsters using fake QR codes to steal personal information or money from unsuspecting victims. The fraudsters either replace legitimate QR codes with false ones or send them via text or email, claiming there's an issue with your account. When victims scan

[37] 'The Real-Time Deepfake Romance Scams Have Arrived'(Wired) <https://www.wired.com/story/yahoo-boys-real-time-deepfake-scams/>accessed 19 January 2025

[38] 'Engineer from Vizag loses Rs 28 lakh after falling for a new romance scam' (India Today, 29 July 2024) <https://www.indiatoday.in/technology/news/story/engineer-from-vizag-loses-rs-28-lakh-after-falling-for-a-new-romance-scam-2573169-2024-07-29> accessed 19 January 2025

these codes, they are redirected to malicious websites where scammers can steal personal data, install malware, or prompt them to enter sensitive details. This scam violates the provisions of section *66C of the Information Technology Act,*[39] which provides for punishment for identity theft. For instance, a police constable from Pune lost Rs 2.3 lakhs in a QR code scam when he attempted to pay at a bakery. Soon after, an unauthorised debit of Rs. 18,755 was made from his savings account. A further unauthorised transaction of Rs 12,250 was deducted from his salary account, leaving him with only Rs. 50 in his account. Later, circumstances escalated when he received an OTP transaction of Rs 1.9 lakh from his gold loan account, despite not sharing an OTP, followed by two transactions worth Rs 14,000 from his credit card. Fortunately, the constable acted quickly and froze his account and card.[40]

However, there has been increasing awareness of such QR Code scams, such as by the Reserve Bank of India, with Radio Chitkara airing an informative program to promote secure use of safe digital payment practices and combat financial fraud. The broadcast, aimed at empowering citizens with the knowledge to navigate the digital financial landscape, highlights key issues such as QR Code Scams.[41]

5) CELEBRITY SCAMS

Celebrity scams involve fraudsters using face-swapping, voice cloning, and body manipulation to impersonate celebrities and endorse products, services, or investment opportunities that they have not actually approved. Such scams are often used to promote fake investment schemes, fraudulent products, or non-existent giveaways. The scale of the threat is substantial, with millions of dollars being lost to deepfake scams. In one instance, a 54-year-old French interior designer fell prey to scammers from Nigeria who posed as Brad Pitt, fabricated a romantic relationship with the victim, and later requested financial support for medical treatment related to his divorce. The victim lost USD 850,000 (approximately Rs.7.36 crore).[42] The rise of deepfake technology scams depicts the limitations within the Indian legal

[39] Information Technology Act 2000, s 66C
[40] 'Police officer from Pune loses Rs 2.3 lakh after scanning QR code to pay at local bakery' *(*India Today, 16 December 2024) <https://www.indiatoday.in/technology/news/story/police-officer-from-pune-loses-rs-23-lakh-after-scanning-qr-code-to-pay-at-local-bakery-2650360-2024-12-16> accessed 19 January 2025
[41] 'RBI's public awareness campaign on money transaction through QR codes' (Chitkara University) <https://sustainable.chitkara.edu.in/pdfs/RBI-public-awareness-campaign-on-money-transaction-through-QR-codes.pdf> accessed 19 January 2025
[42] 'Rs 7.36 crore AI scam involving Brad Pitt addressed by actor. 'It's awful that…' (Economic Times) <https://economictimes.indiatimes.com/magazines/panache/rs-7-36-crore-ai-scam-involving-brad-pitt-addressed-by-actor-its-awful-that-/articleshow/117302234.cms?from=mdr>accessed 20 January 2025

framework in safeguarding against such scams, making it crucial to strengthen the regulation of such cybercrimes.

6) INVESTMENT AND STOCK TRADING SCAMS

Investment and stock trading scams are deceptive schemes wherein fraudsters guarantee high returns with minimal risk to solicit victims. Common scams include Ponzi schemes, fake investment groups, and pump-and-dump tactics. In these scams, scammers repeatedly misrepresent investment products, provide forged stock tips, or pose as unregistered brokers, and often use phishing to steal personal information. In India, individuals are usually targeted through frequently used platforms such as WhatsApp and Telegram.

For instance, in one case, Sasidharan Nambiar, a 73-year-old retired Kerala High Court judge, joined a WhatsApp group named *"Aditya Birla Equity Learning"* in December 2024 and lost Rs 90 lakh.[43] The easy access to technology available through various websites and applications largely drives the rise in deepfake scams. Scammers strategically place victims under intense mental pressure by accusing them of knowingly or unknowingly engaging in serious crimes. They leverage modern technology, and with the rise of deepfake technology, such methods have been aggressively used to fabricate evidence and coerce individuals, thereby revealing significant gaps in India's legal framework. The lack of technological awareness is another influential basis for the growth of deepfake scams, highlighting the urgency of educating the public to curb the growing number of scams.

Whereas cheating, impersonation, and identity theft are already criminalised under existing laws, deepfakes offer a fundamentally different legal limitation. They can convincingly impersonate real individuals without direct human imitation, as they are created using automated AI tools, which makes it difficult to fit deepfake-related offences properly into traditional legal definitions of fraud. The technology permits anonymous or cross-border actors to generate and circulate content, although identifying the creator is often complex and challenging.

[43] 'He lost Rs 90 lakh after joining a WhatsApp group: Investment scams are raging, here's how to stay' (The Indian Times) <https://indianexpress.com/article/technology/tech-news-technology/investments-scams-how-to-spot-protect-safe-side-9796966/> accessed 20 January 2025

V. DEEPFAKE TECHNOLOGY'S IMPACT ON MEDIA RELIABILITY

Deepfake technology, driven by artificial intelligence, has transformed the field of synthetic media by enabling the creation of hyper-realistic content. While this innovation has attracted considerable attention for its technological advancements, it has also raised serious concerns about media reliability and public trust. The major impact of the technology on media reliability are as follows:

1) NO TRANSPARENCY BETWEEN REAL AND FABRICATED MEDIA

Deepfakes blur the line between reality and fabrication by creating highly compelling false media. This erodes trust in visual evidence and challenges the authenticity of digital content. Misinformation can easily gain credibility when it is disguised as a genuine video or image, making it more likely to be shared and believed by unsuspecting individuals.[44] The deceptive power of deepfakes lies in their ability to convincingly replicate voices, faces, and entire conversations. In one instance, an exposed deepfake video of Ukrainian President Volodymyr Zelenskyy was posted on various Ukrainian websites and social media platforms, encouraging Ukrainians to surrender to Russian forces during the Russia-Ukraine war.[45] This fuels conspiracy theories and the spread of misinformation, as deepfakes can quickly go viral due to their sensational nature, captivating audiences and generating significant attention. In the fast-paced world of social media, the speed at which deepfakes spread makes it challenging to contain the dissemination of false information. Even after debunking, the deepfake may have already reached a wide audience, making it difficult to rectify the damage done.[46] It also causes a threat to journalists' integrity and ethics as they face unprecedented challenges in verifying and sourcing information.

2) COPYRIGHT INFRINGEMENT

Copyright refers to the legal rights granted to creators over their literary and artistic works. This includes a wide variety of creations such as books, music, paintings, films, computer

[44] Alexander Godulla and others, 'Dealing with deepfakes – An interdisciplinary examination of the state of research and implications for communication studies' (2021) 10(1) SCM Studies in Communication and Media 77
[45] 'Incident 198: Deepfake Video of Ukrainian President Yielding to Russia Posted on Ukrainian Websites and Social Media' (AI Incident Database) <https://incidentdatabase.ai/cite/198/> accessed 20 January 2025
[46] Renee Hobbs, 'Mind Over Media: Propaganda Education for a Digital Age' (Media Education Lab) <https://mediaeducationlab.com/pub/mind-over-media-propaganda-education-digital-age> accessed 20 January 2025

games, and architecture. Copyright is provided to creators for a limited duration to protect their work from theft or misuse and grant them exclusive rights to reproduce, distribute, display, perform, and modify their creations. Only original creators and those duly authorised hold the exclusive right to reproduce their work.

Deepfakes and internet-forged content may infringe the copyright of original creators. The use of deepfake technology to create manipulated versions of existing works infringes the copyright owner's exclusive rights, specifically the authority to reproduce, distribute, and publicly display their works.[47] Additional concerns have been raised as to the ownership of such generated media. In **Camlin (P) Ltd v National Pencil Industries**[48], the Delhi High Court held that copyright belongs to individuals who create original works resulting from their skill and effort. Hence, pursuant to existing laws and judicial pronouncements, only a human can be regarded as an author, as originality is involved in the formation of content with innovative ideas and unique methods of expression.

VI. LEGAL FRAMEWORKS

Deepfake technology has gained global recognition due to its spread of misleading information, breaches of privacy rights, and fostering of fraud. The Indian judiciary was initially not responsive to the difficulties caused by deepfake technology. However, due to the extensive use of technology in recent years, the judiciary has begun to address the threats posed by deepfakes. Despite this growth, there are no specific decisions or prevailing judgments that directly address the threat caused by deepfake technology. The existing judiciary primarily debates on defining the features of deepfake technology. For instance, the Delhi High Court, a Division Bench of *Chief Justice Manmohan* and *Justice Tushar Rao Gedela*, noted that deepfakes (digitally manipulated videos that impersonate people, which may be used to spread false information) are on the rise.[49] In another instance, Supreme Court *Justice Hima Kohli* emphasised the various threats linked with deepfakes. She highlighted concerns regarding the possibility of invasion of privacy, the dissemination of false information, and the emergence of security threats. She further emphasised that deepfakes are created with such realism that

[47] Didier Ching and others, 'Face/Off: Changing the face of movies with deepfakes' (2023) 18(7) PLOS ONE e0287503

[48] Camlin (P) Ltd v National Pencil Industries (1989) 2 SCC 349

[49] Bhavini Srivastava, 'Deepfakes on the rise, what steps taken to curb it? Delhi High Court asks Centre' (Bar and Bench, 24 October 2024) <https://www.barandbench.com/news/deepfakes-on-the-rise-what-steps-taken-delhi-high-court> accessed 21 January 2025

they often appear to come from reliable sources, which is especially concerning, as it increases the potential harm caused by misleading information.[50] Hence, while several Judges have spoken about deepfake technology, no landmark or authoritative judgements have yet been provided on this technology on which the public can rely for future perspectives.

However, Indian laws do not recognise any crimes associated with deepfakes. There are certain provisions linked with deepfake technology that may help to address the issues.

1. **Information Technology Act, 2000:** The IT Act contributes a major part to the protection of individual rights and security in cyber frameworks, such as *Section 67A of the IT Act*, [51] which refers to the transmission of sexually explicit content. When someone, without the individual's consent, generates their photos, videos, and audio to create sexually explicit content, this section imposes heavy penalties on the offender. *Section 66E of the IT Act,*[52] refers to whoever, intentionally or knowingly, captures, publishes or transmits the image of a private area of any person without his or her consent, under circumstances violating the privacy of that person. Such an act is punishable with imprisonment which may extend to three years or a fine not exceeding two lakhs, or with both. [53] *The Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021,*[54] provide an important mechanism that is accountable for removing individuals' non-consensual photos or videos shared on different media platforms, including content that portrays misinformation/disinformation, promotes sexually explicit videos or triggers outbreaks of violence, and is detrimental to individuals who consume such content.

2. Bhartiya Nyaya Sanhita, 2023

Section 353 of the BNS,[55] aims to restrain the spread of misinformation and disinformation by penalizing the act of making false or misleading statements, rumours, or reports that can cause

[50] Isha Sharma, 'Indian Judiciary's Stance on Deepfakes' (Cyber Peace Foundation, 16 December 2023) <https://www.cyberpeace.org/resources/blogs/indian-judiciarys-stance-on-deepfakes> accessed 21 January 2025
[51] Information Technology Act 2000, s 67A
[52] Information Technology Act 2000, s 66E
[53] 'Punishment for violation of privacy'(Lawgist) <https://lawgist.in/information-technology-act/66E> accessed 21 January 2025
[54] Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules 2021, rr 3(1)(d) and 3(2)(b)
[55] Bhartiya Nyaya Sanhita 2023, s 353

public mischief or fear.[56] *Section 111 of the BNS,* [57] states that organised cybercrimes, including cybercrimes involving deepfake content, can be prosecuted. [58] Furthermore, *Section 356 of the BNS*, [59] states that whoever, by words either spoken, or intended to be read, or signs or by visible representations, makes or publishes in any manner, any imputation concerning any person, intending to harm, is said to defame the person.[60] *Section 319 of the BNS,* [61] describes the "cheat by personation", if he cheats by pretending to be some other person, or by knowingly substituting one person for another.[62]

3. Constitution of India

Article 21 of the Constitution,[63] protects individual rights, including the Right to Privacy. It safeguards people when their photos are used without their consent, which amounts to a violation of their privacy. The Constitution provides the Right to Freedom of Speech and Expression under *Article 19(1)(a)*,[64] there are several "reasonable restrictions" on it for reasons including security, public order, defamation, or morality.[65]

4. The Copyright Act, 1957.

According to *Section 51 of the Act,*[66] copyright in a work is infringed when any person, without the license from the owner or registrar of copyrights, does anything for which only the owner has the exclusive rights. [67] According to *Section 63 of the Act*,[68] any individual who intentionally violates or assists in the violation of copyright in a work or any other right granted

[56] 'India well-equipped to tackle evolving online harms and cyber crimes; Government to Parliament'(pib.gov.in) <https://www.pib.gov.in/PressReleasePage.aspx?PRID=2154268&reg=3&lang=2#:~:text=Digital%20Personal%20Data%20Protection%20Act,be%20prosecuted%20under%20section%20111> accessed 21 January 2025
[57] Bhartiya Nyaya Sanhita 2023, s 111
[58] 'AI and deepfakes: Navigating the digital revolution and its dark side' (Bar and Bench) <https://www.barandbench.com/view-point/ai-and-deepfakes-navigating-the-digital-revolution-and-its-dark-side> accessed 22 January 2025
[59] Bhartiya Nyaya Sanhita 2023, s 356
[60]'BNS Section 356- Defamation'(Devgan) <https://devgan.in/bns/section/356/> accessed 22 January 2025
[61] Bhartiya Nyaya Sanhita 2023, s 319.
[62] 'BNS Section 319- Cheating by Personation' (Devgan) <https://devgan.in/bns/section/319/> accessed 22 January 2025
[63] Constitution of India 1950, art 21.
[64] Constitution of India 1950, art 19(1)(a)
[65]'Legal Dimension of Deepfake Technology: Privacy, Consent, and Criminal Liability' (Juris Centre, 27 July 2025) <https://juriscentre.com/2025/07/27/legal-dimensions-of-deepfake-technology-privacy-consent-and-criminal-liability/#:~:text=Legal%20Framework%20in%20India,revenge%20pornography%20deepfakes%5B7%5D> accessed 22 January 2025
[66] Copyright Act 1957, s 51
[67] 'Copyright Misuse and infringement' (SSRANA) < https://ssrana.in/ip-laws/copyright-law-india/copyright-misuse-and-infringement-india/> accessed 22 January 2025
[68] Copyright Act 1957, s 63

by the Act faces a maximum sentence of three years in jail and a maximum fine of two lakh rupees.[69]

3. Indecent Representation of Women (Prohibition) Act, 1986,[70] prohibits the indecent representation of women through advertisements, publications, and other media. Amendments have extended its scope to cover digital content, making it applicable to deepfakes that depict women in derogatory or sexualized manners without their consent. The Act broadly defines 'indecent representation' under section 2(c) as any depiction likely to deprave, corrupt, or injure public morality.[71]

5. Digital Personal Data Protection Act, 2023 [72] the Act emphasises the right of individuals over their data and imposes obligations on entities that process such data. Entities must obtain explicit consent from individuals before processing their data. In the context of deepfakes, using someone's image or likeness without consent violates these provisions. Individuals can access, correct, and erase personal data. Victims of deepfake misuse can exercise these rights to request the removal of unauthorised content involving data. The act imposes substantial fines for breaches, which can deter entities from misusing personal data to create deepfakes.[73]

Hence, these are the legal provisions that can be used to tackle deepfake technology; however, several aspects are not covered directly to address such challenges, such as fraud, which is growing rapidly. Laws in India do not provide exclusive security against the exploitation of deepfake technology, and lack strengthened legal provisions to regulate it.

VII. LIMITATIONS OF THE EXISTING LEGAL FRAMEWORK IN INDIA

Deepfakes are a rapidly growing form of technology driven by artificial intelligence that allows individuals to create realistic videos, images and audio recordings that closely resemble real

[69] Parth Sarthi Garg, 'Implications of Copyright Law on Deepfakes' (Satyaki Legal) <https://satyakilegal.com/implications-of-copyright-law-on-deepfakes/> accessed 22 January 2025
[70] Indecent Representation of Women (Prohibition) Act 1986, s 2(c)
[71] 'The Impact of Deepfake Technology: Legal Risks and Regulatory Solutions New Technology – Worldwide' (Mondaq, 28 November 2024) <https://www.mondaq.com/india/new-technology/1550822/the-impact-of-deepfake-technology-legal-risks-and-regulatory-solutions> accessed 22 January 2025
[72] Digital Personal Data Protection Act 2023, ss 8,12 and 19
[73] Pranav Dabas, 'The Impact of Deepfake Technology: Legal Risks and Regulatory Solutions' (Metalegal, 26 November 2024) <https://www.metalegal.in/post/the-impact-of-deepfake-technology-legal-risks-and-regulatory-solutions?utm_source=mondaq&utm_medium=syndication&utm_content=articleoriginal&utm_campaign=article> accessed 22 January 2025

people. Deepfakes appear as a major digital threat because such creations often occur as genuine. In India, they pose major consequential challenges to law enforcement agencies, regulatory authorities, digital platforms, and society at large. Indian laws and Judicial precedents were framed at a time when such advanced technological threats did not exist, and are therefore not fully equipped to deal with these challenges. As a consequence, the country continues to struggle in effectively dealing with deepfakes due to technical difficulties, enforcement issues, legal loopholes and ethical concerns.

Applicability of Deepfakes under the Indian Evidence Act

In accordance with the Indian Evidence Act 1872, the admissibility of electronic records is recognised under *Section 65A*,[74] which directs the court to follow the procedure laid down in *Section 65B of the Act*.[75] *Section 65B* prescribes the conditions under which electronic records, such as emails, audio recordings, videos or digital files, are admissible in courts. It involves a certificate confirming that the electronic record was produced and has not been altered.

In **Anvar P.V v. P.K. Basheer**[76], the Supreme Court held that secondary electronic evidence, such as CDs, DVDs, or printouts, must be accompanied by a certificate under Section 65B to be admissible. This judgement overruled the earlier decision in **State (NCT of Delhi) v. Navjot Sandhu**,[77] which granted courts the power to admit electronic evidence under Sections 63 and 65 without compliance with Section 65B. The court in Anwar P.V. expounded that the mere production of an electronic record is inadequate; it must be strictly in compliance with Section 65B. Later, in **Arjun Panditrao Khotkar v. Kailash Kushanrao Gorantyal**,[78] the Supreme Court further clarified that under *Section 65B (4)*, the certificate is mandatory unless the original record is unavailable. In such exceptional cases, courts may exercise discretion under *Section 65B (1)*. In proper authentication, the courts must underscore that the electronic evidence has not been tampered with in any manner.

Deepfakes are created using artificial intelligence to manipulate media in a process that looks completely genuine, even though it may be forged. As a consequence, the genuineness of an electronic record becomes difficult to trust, even when all the legal requirements under Section

[74] Indian Evidence Act 1872, s 65A
[75] Indian Evidence Act 1872, s 65B
[76] Anvar P.V v P.K. Basheer (2014) 10 SCC 473 [24]
[77] State (NCT of Delhi) v Navjot Sandhu (2005) 11 SCC 600 [150]
[78] Arjun Panditrao Khotkar v Kailash Kushanrao Gorantyal (2020) 7 SCC 1 [52]-[54],[58]

65B of the Indian Evidence Act are explicitly followed. It is again challenging to determine who actually created such content or whether it has been altered. The idea behind Section 65B of the Indian Evidence Act is to establish that electronic evidence, such as videos, audio recordings, or digital files, has not been altered and comes from a known source. The law assumes that if the original identity and integrity of the electronic record can be confirmed through the required procedure, then the evidence can be treated as reliable. However, deepfake technology challenges these basic assumptions. The admissibility and reliability of AI-manipulated media created through deepfakes raise serious concerns as to whether they can be used as evidence in court.

However, neither of these landmark judgments conveys the issue of AI-generated or deepfakes. Traditional methods of verifying the source or issuing the certificate under 65B may not be suitable, effective or even be achievable in comparable circumstances. For instance, a deepfake video may originate from an authenticated source, but the content itself can be fabricated using Generative Adversarial Networks (GANs). The acceptance of such a video as evidence could mislead the court and endanger the administration of justice.

Can current laws handle deepfakes?

At present, India's legal system is not fully prepared to handle the challenges caused by deepfakes in judicial proceedings. *Section 65B* necessitates a certificate which assumes digital content is created or stored on identifiable devices or platforms whose integrity can be verified. However, deepfakes can be generated anonymously, using open-source tools and rapidly shared across social media platforms without leaving a clear trail of origin. Furthermore, the Indian framework lacks sufficient digital forensic tools to detect deepfakes. Unlike jurisdictions such as the European Union, which has introduced the AI Act, or certain U.S. states like California that have enacted laws targeting deepfakes in the election scenario, India currently does not have a separate statute addressing such issue of synthetic media. Judges often rely on expert opinions and forensic reports because trial courts lack the technical capacity and expertise to identify manipulated content, which may not be sufficient when dealing with highly sophisticated GAN-generated media. However, judgements like Anvar P.V. and Arjun Panditrao have made significant advancements in regulating electronic evidence; they don’t address the complexities introduced by deepfakes. The Challenges of detection and attribution of deepfakes are created through advanced levels of technology that

can evade traditional forensic tools and are so sophisticated that they make it difficult for trained experts to detect manipulation.

One of the most serious questions in combating deepfakes undertakes the responsibility for creating or circulating deepfake content. Tracing the original creator is exceptionally challenging, as deepfakes can be produced anonymously using easily accessible tools and can be shared rapidly across the internet and social media platforms.

Spread of Deepfake Misinformation in Politics and Media

The misuse of deepfakes has serious consequences because in a democratic country like India, where elections and public discourse play a crucial role. Deepfake technology can be used to alter speeches of political leaders, damage reputations, and mislead citizens, particularly during election periods. It has a vigorous potential to manipulate political narratives and change public opinion.

Deepfake propaganda becomes especially dangerous during times of elections or communal tension. For instance, in 2020, a deepfake video of a political leader delivering a speech was circulated online that had been altered to influence voter sentiment. Such incidents create confusion and distrust among the public and highlight how deepfakes can undermine democratic processes.[79]

Role and Responsibility of Social Media Platforms

Social media platforms play a major role in the circulation of deepfakes, as content on these platforms can go viral within minutes; thus, regulating such material becomes extremely challenging. Under the current legal framework, a complaint is mandatory, as social media platforms are generally not required to proactively remove deepfake content. Although certain obligations on intermediaries are imposed by the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021,[80] most platforms are unable to detect deepfakes due to a lack of effective and consistent mechanisms. This allows manipulated content to remain online for long periods, causing widespread harm before any action is taken.

[79] Aditya Pratap Singh, 'Legal Implications of Deepfake Technology in Criminal Law' (2025) 8 (1) International Journal of Law Management & Humanities 1655

[80] Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules 2021, r 3(1)(b)

Content on social media often remains online until a formal complaint is filed. Under the existing rules, intermediary liability does not require social media platforms to pre-emptively remove harmful content or to actively identify deepfakes on their own. Consequently, the effectiveness of content moderation is delayed and weakened. As deepfake material spreads widely, it causes serious harm before any corrective or remedial action is taken.

Privacy and Consent Issues

Deepfakes have increasingly been misused against women and celebrities, who often become victims of revenge pornography, harassment, and identity fraud. Typically, victims are unaware that their images or videos have been altered until the content has already fallen into the public domain and spread widely. Several cases have emerged in India where individuals' faces were morphed into pornographic videos and circulated online, leading to severe mental distress, reputational damage, and cyber harassment. Existing laws do not adequately deal with such issues; hence, this results in a failure to provide timely and effective remedies to victims.

Some laws and provisions under the Information Technology Act, 2000, acknowledge protection against cyberattacks, privacy violations, and the circulation of explicit content concerning women; however, the IT Act does not provide specific security for the content generated through artificial intelligence tools. This reflects the loopholes under the Indian legal framework, where content is circulated without consent, placing an undue burden on victims by limiting their accessible legal recourse to address the harm.

Lack of Awareness and Digital Illiteracy

A significant challenge associated with deepfake technology is that the public is frequently unaware of deepfakes, and vulnerable people usually lack knowledge of digital content. Several individuals are unable to distinguish between genuine content and manipulated media, which makes them more vulnerable to deepfake scams and fraud. Individuals mostly trust what they see or hear without questioning its authenticity.

For instance, in 2023, a deepfake-recorded audio that convincingly imitated the voice of the company's CEO was used to manipulate an employee, which led him to approve a large financial transaction.[81] Such incidents show that a lack of awareness can be exploited by

[81] Singh, 'Legal Implications of Deepfake Technology' 1655

cybercriminals, which further worsens the deepfake problem in India.

VIII. CONCLUSION

Deepfake technology presents a paradox. On one hand, it brings significant advancements in entertainment, education, and the arts. On the other hand, it poses serious risks by creating realistic yet misleading digital content.

India's current legal framework is not adequately equipped to tackle these challenges, being largely reactive, fragmented, and lacking in both technical deterrence and victim-centric redressal mechanisms. There is a pressing need for specific and nuanced legislation that defines and criminalises harmful deepfakes. By identifying malicious deepfakes and making their creation and dissemination illegal, the law can provide a strong foundation for addressing this issue. Additionally, it is crucial to protect victims through the establishment of swift mechanisms for removing harmful content and providing legal assistance to those affected. Enhancing law enforcement capabilities is also vital; police and agencies require the necessary tools and training to effectively investigate and address deepfake crimes. Other nations have recognised the urgency of the deepfake issue and have begun developing specific laws. India can learn from these examples to create its own legislation that addresses these technological challenges while respecting individual rights. Encouraging the use of watermarks or labels can help the public identify synthetic content without stifling creativity.

By thoughtfully addressing these issues through a collaborative approach involving lawmakers, technology platforms, and civil society, India can protect its citizens from the dangers posed by deepfakes while promoting innovation and freedom of expression.

VIII. RECOMMENDATION

1. The need for stronger detection tools to detect deepfake videos, audio, and photos will help individuals detect this technology, this detection tool will also help to diminish the misinformation it spreads. Labelling of AI-generated synthetic media may reduce misinformation. Labelling of deepfake content would help people bifurcate the synthetic media from reality, preventing various mishaps and scams.

2. Cases of fraud prevail in today’s era, and the need for more effective and stringent legal and policy frameworks is required since there are no exclusive provisions for deepfake

fraud. Introduction of an act which defines, prohibit and penalise harmful deepfakes, with a clear distinction for parody, satire and legitimate use is the need of the hour.

3. Deepfake technology can ruin someone's life. Individuals of all ages are glued to their devices. In such a case, where everyone is indulged in the digital world, it is essential to raise awareness about such scams and the potential risks of deepfakes. The government should roll out nationwide digital literacy programs focusing on deepfake risks, detection tips, and reporting mechanisms via schools, media and government portals.

4. Surveys can be conducted related to this technology, about how people perceive this technology, through surveys, suggestions could be added on how an individual can tackle deepfake content.

5. Social media platforms must create and enforce stricter rules to stop the spread of deepfakes. They should set up ways for users to report and remove deepfake content, ensure their content moderation practices are clear, and hold users responsible for harmful actions.