Research article

Maharaja Surajmal Institute Law Journal
Year 2024, Volume-1, Issue-2 (July - December)

www.acspublisher.com

Deepfakes and the Law: Addressing the Regulatory Gap and Mitigating the Risks of AI-Generated Content

Rashi Makhija[1], Anuradha Jha[2]

[1]Research Scholar, University School of Law and Legal Studies Guru Gobind Singh Indraprastha University, Delhi
[2]Professor, Guru Gobind Singh Indraprastha University, Delhi

ARTICLE INFO

Keywords: phenomenon, pornography, non-consensual, impersonate, deepfake technology

Doi: 10.48165/msilj.2024.1.2.1

ABSTRACT

The creation of fake pictures, videos, and voices made possible with the help of Artificial Intelligence is rapidly gaining traction as an emerging threat. Initially meant for artistic and educational use, deepfake technology can be and is misused to suit one's needs. Disguising oneself, spreading untrue information, fabricating videos of an individual without their permission, and even changing the perceived view of a society are all deepfake possibilities that can be done easily with this technology.

As with everything, deepfakes come with their own set of problems and risks. Their core weakness comes in the hand of fraud; criminals are now able to use AI to impersonate an individual's voice and trick employees into unknowingly performing money transfers. This has caused business and people to lose large sums of money. Without a doubt, another blatant issue are non-consensual deepfake videos where an individual's likeness is placed over obscene content. Research indicates that the majority of deepfake pornography involving women is done making the whole phenomenon an internet issue on stalking and mistreatment.

Even with all their expansion issues, the current laws set in place are not sufficient for deepfake crimes. Europe's *General Data Protection Regulation (GDPR)*, as well as India's *Digital Personal Data Protection Act of 2023*, was supposed to protect personal data, but does not sovle the issue of deepfakes. Therefore, victims have little aid legally to take action, while numerous criminals remain unchecked.

This article analyzes the failure of current laws and tries to find a solution for the same. It suggests that aggressive legal measures, advanced deepfake detection technology, and increasing artificial intelligence awareness abuse would be needed to curb deepfake misuse.

*Corresponding author.
E-mail address: rashimakhija369@gmail.com (Rashi Makhija)

INTRODUCTION

Resulting from the advancements in use of AI, creating deepfakes poses considerable risk; these videos and audio recordings, while being incredibly lifelike and convincing, are actually fabricated. This technology enables computers to produce deceptively realistic audio-visual content including videos, photographs, and voice recordings. Numerous other ethical issues arise from the technology's unfortunate propensity to be used for identity theft, fraudulent appropriation, and manipulation without consent. Such issues call for creation of a comprehensive legal framework to control as well as to prevent deepfakes.[1]

The ability of generating fake statement videos enables the spread of irrelevant news concerning the politician in question, thus having an impact on elections, deteriorating the respect towards governmental and media bodies, and spreading skepticism. Given that deepfakes appear to be highly replicated, differentiating between real and fake is getting more difficult.

The exploitation of deep fake technology has caused a stir over startling incidents of financial fraud. This includes the newest episode where scammers created a fake impersonation video of a famous financial analyst, Michael Hewson, using advanced AI.[2] The impersonation made use of deep fake audio and video technology which reproduced video footage of Hewson's face and voice perfectly. In this fake video, "Hewson" claimed to endorse a certain investment quote unquote opportunity that convinced unsuspecting victims to fund it like it was a genuine ponzi scheme. The funds were lost in the scheme and people later realized it was all fabricated.[3] Michael Hewson, the victim of the impersonation, was left with the blame as the fraudsters vanished into thin air with the cash.[4] This demonstrates the considerable risks associated with deep fakes when used for fraudulent schemes. The advent of advanced AI makes it trivial for scammers to impersonate reputable professionals, placing victims into a predicament of discerning reality from deception. It demonstrates a clear gap in the law relating to this level of fraud.

The advance of deepfake technology has made it effortless for a person to create fake inappropriate images and videos of others without their consent. Such technology is often maliciously used against women and girls who, in many cases, become the primary victims of this misuse.

Recently, the internet was treated to images of teenage girls which had in reality never been photographed.[5] However, thanks to the ever-improving deepfake technology, such images were transformed into a completely unbelievable version of reality. In turn, this has led these girls to tremendous psychological suffering and rising worries about the famed "technology" that can be brandished in such a manner. Victims of such incidents often find it difficult to remove content from the internet and merely try to ignore it. There is also the added difficulty of finding those responsible for the act as deepfakes can be created with complete anonymity.

Deepfake technology is being used for malicious purposes, including the spreading of false information about well-known public figures. An outrageous example is the multiplied circulation of lascivious forgeries of images of a singer, Taylor Swift.[6] Photos created by AIs surfaced on social networking sites and went viral, fooling countless people and getting them enraged in public. Though Taylor Swift did nothing to these photos, the blends amazed numerous individuals and illustrated how easily one's reputation could be shredded apart with deepfake technology.[7]

Such events emphasize the risks put forth by the deepfakes, and shows the requirement for regulating the use of such technologies. With the ever-growing sophistication and availability of this technology, it is more important than ever to be proactive about establishing robust legal safeguards and education in order to protect targets, particularly women and public figures, from harmful AI- fabricated material.

Technological advancement is becoming unbearably fast, creating a gap between its development and the extent

[1]A. Shaji George, "Deepfakes: The Evolution of Hyper-realistic Media Manipulation," *Research Gate* (Dec. 25, 2023), available at: https://doi.org/10.5281/zenodo.10148558.

[2]Michael Bow, "City Analyst Michael Hewson Cloned in AI Deepfake Scam," The *Times*, Mar. 23, 2025, available at: https://www.thetimes.com/uk/technology-uk/article/city-analyst-michael-hewson-cloned-ai-deepfake-scam-fn5wkxt09 (last visited on Mar. 23, 2025).

[3]*Supra*

[4]I*d.*

[5]CBS News, "AI Photos of Naked Students Circulated at Pennsylvania School," *CBS News Pittsburgh*, Dec. 2023, available at: https://www.cbsnews.com/pittsburgh/news/ai-photos-naked-students-pennsylvania-school/ (last visited on Mar. 23, 2025).

[6]Mackenzie Ferguson, "Deepfake Technology in 2025: From Creative Tools to Ethical Challenges," *OpenTools AI News*, 2025, available at: https://opentools.ai/news/deepfake-technology-in-2025-from-creative-tools-to-ethical-challenges (last visited on Mar. 23, 2025).

[7]Imran Rahman-Jones, "Taylor Swift Deepfakes Spark Calls in Congress for New Legislation," *BBC News,* Jan. 27, 2024, available at: https://www.bbc.com/news/technology-68110476 (last visited on Mar. 23, 2025).

to which governments and laws can keep up. The ability to construct believable fake videos, images, and voices makes deepfakes highly troubling. Unique threats to privacy, security, and trust are introduced by deepfakes. The most challenging legal issues revolve around proving the authenticity of things, assigning blame for the wrongful use of deepfakes, and protecting the victims from potential damage. Unfortunately, many of the existing laws were crafted at a time before the very notion of deepfakes were purported, which put forward various issues.

No single federal law in the United States regulates deepfake technology directly. Circuited instead are the various states, each devising their own laws to tackle deepfake-crimes. While some states, California and Texas for instance, made illegal the creation and sharing of deepfake aided pornography as well as using deepfakes to interfere in elections without consent, the enforcement of the decree remains inconsistent across the country due to how different it varies from state to state.[8]

The United Kingdom is developing a policy called the Online Harms Act criminalize the distribution of deepfake pornography without consent. This law seeks to punish people for abusing AI content in inappropriate ways. It is considered some of the most strident legal action in the world against the most inappropriate use of deepfakes.[9]

Specialists in Australia have grave fears concerning the uncontrolled rise of deepfake pornography, coupled with the absence of solid legislation to contain it. Some attempts have been made to dismantle the non-consensual, AI generated content. However, sith the speed of innovation in the AI industry, those attempts seem futile. Many say that legal measures are not sufficient. There is the need for public awareness of the issues revolving around the misuse of deepfakes and a willingness to change the underlying attitudes that make this abuse possible.

THE GROWING THREAT OF DEEPFAKES

The advancement of deepfake technology poses a threat to our world, as its misuse has been reported in cases of harassment, misinformation, and audio-visual fraud. Deepfake videos and audio recordings can be deceptively authentic, making it easy for people to fall into a web of lies or worse, be victims of elaborate financial schemes.

One of the most sophisticated cases deepfake fraud happened with a bank in United Arab Emirates where $35 Million were lost due to AI-generated voice scam.[10] AI was used to duplicate the voice of the Executive so the scammers Simulated themselves as the Executive of the bank, called in and instructed the employees to transfer the funds to a secured account. Owing to the convincing voice, bank employees fully believed and facilitated in executing the transaction. Sadly, once the employees had discovered the fraud, it was too late, the money was gone.

The case proves that deepfake technology is dangerous and unregulated as it enhances the risk level associated with scamming.The deepfake is now sophisticated enough to tip the scales in favor of the scammers.

The advancements in deepfake technology are also being exploited in politics like in the case of elections. In India, misleading and deceptive videos of politicians are circulated to confuse voters.[11] As an example, a few deepfake videos depict politicians making statements they did not actually make. These videos are easily spreadable on social media and led people to form inaccurate opinions on different matters. Political parties and the citizens tend to be used as pawns which is detrimental to democracy.

Once deepfakes are created, the damage is already done since they are too realistic and fact-checks would make them too late. They can sway public sentiment, alter election patterns, and instill animosity towards the political domain.

Deepfakes can disrupt elections by deceiving voters with phony speeches and manipulated campaign videos, and they can destabilize financial markets by disseminating false information about companies or economic policies, according to the World Economic Forum, 2022. Additionally, it undermines public confidence in the media

[8]Kaleigh Rogers, "States Cracking Down on Deepfakes Ahead of 2024 Election—But They Might Be Missing the Most Concerning Threats," *ABC News,* Mar. 27, 2024, available at: https://abcnews.go.com/538/states-cracking-deepfakes-ahead-2024-election/story?id=108517821 (last visited on Mar. 23, 2025).

[9]UK Government, "Online Safety Act Explainer," *Gov.uk,* 2024, available at: https://www.gov.uk/government/publications/online-safety-act-explainer/online-safety-act-explainer (last visited on Mar. 23, 2025).

[10]Thomas Brewster, "Huge Bank Fraud Uses Deepfake Voice Tech to Steal Millions," *Forbes*, Oct. 14, 2021, available at: https://www.forbes.com/sites/thomasbrewster/2021/10/14/huge-bank-fraud-uses-deep-fake-voice-tech-to-steal-millions/ (last visited on Mar. 23, 2025).

[11]M. Momeni, "Artificial Intelligence and Political Deepfakes: Shaping Citizen Perceptions Through Misinformation," *Journal of Creative Communications* 20(1), 41-56 (2024), available at: https://doi.org/10.1177/09732586241277335.

by leading people to doubt everything they read and hear online.[12]

A study from 2023 revealed that more than 80% of individuals who suffered from deepfakes did not know that their faces, voices, or other personal information was being utilized in fake audio and video files.[13] This is because deepfakes could be constructed with or without a person's consent which makes it harder for patients to defend themselves. In today's world, voiceless and faceless scamming which is impersonating others via the internet, is being increased through the use of AI. This has the potential to cause frauds, blackmails, and other financial scams to happen.[14]

Deepfakes allows for things to be altered and claimed to have happened when in reality there is no proof for it, be it words said or actions undertaken. Such capabilities obliterate reputations and sway individuals into forming illogical opinions. One of the exceedingly shocking cases of deepfakes' misuse involves the creation of deep fake pornographic images and videos of real people without their permission, or even worst- their knowledge.

According to a report, released in 2023, 96% of deepfake pornography is made without the consent of the participants, and the majority of victims are women.[15] This suggests that nearly all available explicit deepfake content online is intended for the voyeuristic harassment, humiliation, and exploitation of women. Some examples of the worst situations are fake bare body pictures of women and girls being circulated via the Internet, which causes emotional pain and harms their personal and professional lives. Deepfake videos blackmailing, where fake explicit content is produced, and criminals threaten to release them unless their monetary or other demands are met. Teenage girls being the primary victims, as AI-created indecent photographs are shared on social networking sites, leading to adverse effects on their psychology.[16] Deepfake technology isn't just an innocuous internet fad – it's a significant problem impacting the lives of real people. Considering the majority of potential victims are unaware that their digital persona is being compromised and women are chiefly the targets, there is a dire need of more stringent legislation alongside effective implementation accompanied by public education and awareness to mitigate deepfake crimes before they do more damage.

INDIAN PERSPECTIVE ON DEEPFAKES

India does not have a specific law pertaining to deepfakes, however, different aspects of the problem can be targeted through diverse provisions under the cyber laws, data protection laws, and even the criminal laws.[17] This is in part the result of inadequate education and enforcement over the emergence of this new technology.

The *Digital Personal Data Protection Act of 2023 (DPDPA)* is the latest Indian law regarding privacy and the handling of personal information. This particular Act is aimed at regulating the manner in which organizations and individuals collect, process, store, and use data. This specific policy attempts to protect the exploitation of personal information, but does not delineate provisions for deepfake harms, and hence allows for offensive behaviour to continue without restrain.[18]

Deepfake technology infringes upon an individual's right to both their image and sound, and therefore falls under the scope of personal data protection under the DPDPA. Still, manipulation of media through AI has not been addressed which means deepfakes continue to operate in the legal gray area under this law. The legal experts argue that deepfake-related offenses ought to be included

[12]Nathan Hamiel "Deepfakes: A Different Threat Than Expected," *World Economic Forum*, Jan. 2025, available at: https://www.weforum.org/stories/2025/01/deepfakes-different-threat-than-expected/ (last visited on Mar. 23, 2025).

[13]Brooke Seipel, "Data Shows You'll Encounter a Deepfake Today—Here's How to Recognize It," *McAfee Blog,* 2024, available at: https://www.mcafee.com/blogs/internet-security/data-shows-youll-encounter-a-deepfake-today-heres-how-to-recognize-it/ (last visited on Mar. 23, 2025).

[14]Tom Williams, "Experts Say AI Scams Are on the Rise as Criminals Use Voice Cloning, Phishing, and Technologies Like ChatGPT to Trick People," *ABC News Australia,* Apr. 11, 2023, available at: https://www.abc.net.au/news/2023-04-12/artificial-intelligence-ai-scams-voice-cloning-phishing-chatgpt/102064086 (last visited on Mar. 23, 2025).

[15]Kristin Houser, "Porn Deepfakes Now Make Up 96 Percent of All Deepfakes Online," *Futurism*, 2024, available at: https://futurism.com/the-byte/porn-deepfakes-96-percent-online (last visited on Mar. 23, 2025).

[16]Internet Crime Complaint Center (IC3), "Public Service Announcement: Malicious Actors Creating Synthetic Content to Exploit Victims," *IC3*, June 5, 2023, available at: https://www.ic3.gov/PSA/2023/PSA230605 (last visited on Mar. 23, 2025).

[17]Aaratrika Bhaumik, "Regulating Deepfakes and Generative AI in India: Explained," *The Hindu,* Dec. 4, 2023, available at: https://www.thehindu.com/news/national/regulating-deepfakes-generative-ai-in-india-explained/article67591640.ece (last visited on Mar. 23, 2025).

[18]The Digital Personal Data Protection Act, 2023 (Act No. 29 of 2023), s. 4.

in the upcoming revisions of the DPDPA to guard against identity theft and misinformation involving AI to a greater degree.

The IT Act is the principal legislation dealing with cybercrimes in India. Deepfakes are not mentioned explicitly, but some provisions can also be relevant in cases of deepfake abuse where it provides for the punishment of prying into people's private lives, including capturing, publishing, or broadcasting private photographs of a person without their permission.[19] This act prohibits the publication or transmission in any form of obscene materials and can be used against deepfake pornography[20] and also pertains to sexually explicit materials and refers to the areas of law which can be enforced where deepfakes are used for the production of non-consensual pornography.[21] It further empowers the government to block any online material that purportedly compromises national security and may be invoked to erase any hostile deepfake videos.[22]

Some deepfake crimes also fall under the provisions of the IPC, the enactment which includes defamation where in case a deepfake video resulting into a person being defamed is made.[23] Furthermore, Section 509, which deals with the offence of outraging a woman's modesty, pertains to the ways women are caricatured by deepfake videos with intent to ridicule or insult.[24] Section 419 of *Indian Penal Code, 1860* talks about impersonation fraud where the deepfakes are used for committing fraudulent acts of assuming someone's identity.

The copyright Act, 1957, also provides for infringement of copyright where the deepfakes utilize copyrighted works without permission.[25]

In the Delhi High Court, Bollywood actor Anil Kapoor successfully sued individuals for using AI to impersonate his voice, name, and image in videos. The court ruled that his likeness was not to be used without consent, which is a first of its kind in Indian deepfake cases. [26]

Public Interest Litigation (PIL) by journalist Rajat Sharma filed a PIL at Delhi High Court in May 2024. Sharma mentioned the rapid growth of unmonitored deepfake technology of AI as a problem that needed immediate attention. The purpose of the filing was to stop the violation of an individual's privacy, as well as the peace within society by attempting to use deepfakes.[27]

GLOBAL LEGAL PERSPECTIVES ON DEEPFAKES

Countries have created various methods to regulate deepfake technologies, but gaps still exist within the blanket law for deepfakes.

United States

The federal law does not legislate deepfakes, however some states have laws that deal with certain aspects. California and Texas have made laws against deepfake pornography and interference for elections without consent.[28]As of now at least 23 states in America have laws addressing deepfake content that is created without consent. These laws enable the victims to sue the producers or distributors of such content and get restraining orders against them.[29]

The Take It Down Act[30] looks to make it a federal offense to publish or give the danger of publishing certain documents or images that are intimate in nature either of real people and of AI produced personalities.[31] This law is meant to protect all states uniformly. In the National Defense Authorization Act, 2021 deepfakes are listed as a

[19]The Information Technology Act, 2000 (Act 21 of 2000), s. 66E.

[20]The Information Technology Act, 2000 (Act 21 of 2000), s. 67.

[21] The Information Technology Act, 2000 (Act 21 of 2000), s. 67A.

[22]The Information Technology Act, 2000 (Act 21 of 2000), s. 69A.

[23] The Indian Penal Code, 1860 (Act 45 of 1860), s. 500.

[24] The Indian Penal Code, 1860 (Act 45 of 1860), s. 509.

[25]The Copyright Act, 1957 (Act 14 of 1957), s. 51.

[26]TOI Tech Desk, "How This Court Case Resulted in Anil Kapoor Making It to TIME's List of Most Influential People in AI," The *Times of India*, Mar. 2024, available at: https://timesofindia.indiatimes.com/technology/tech-news/how-this-court-case-resulted-in-anil-kapoor-making-it-to-times-list-of-most-influential-people-in-ai/articleshow/113154447.cms (last visited on Mar. 23, 2025).

[27]Prashant Jha, "Journalist Rajat Sharma Files PIL in Delhi High Court to Block Apps and Platforms on Deepfakes," *Bar & Bench,* May 8, 2024, available at: https://www.barandbench.com/news/journalist-rajat-sharma-pil-delhi-high-court-block-apps-platforms-deepfakes (last visited on Mar. 23, 2025).

[28] *Id.*

[29]Elliott Davis Jr., "These States Have Banned the Type of Deepfake Porn That Targeted Taylor Swift," *U.S. News & World Report*, Jan. 30, 2024, available at: https://www.usnews.com/news/best-states/articles/2024-01-30/these-states-have-banned-the-type-of-deepfake-porn-that-targeted-taylor-swift (last visited on Mar. 23, 2025).

[30]Daniel Miller, "What is the Take It Down Act?" *FOX 13 Seattle,* Mar. 3, 2025, available at: https://www.fox13seattle.com/news/take-down-act-what-to-know (last visited on Mar. 23, 2025).

[31]*Supra*

risky issue for national security. [32]A proposal called The Deepfakes Accountability Act seeks to place AI generated videos and images under watermarking rules. Some states, such as Texas and California, have enacted laws against deepfake pornography and deepfake misinformation concerning elections.[33]

European Union

The *General Data Protection Regulation (GDPR)* has limitations for use of personal data which restrains the creation of deepfakes. Nevertheless, AI generated content is not covered. In the case of harmful deepfakes, platforms are required to identify and eliminate them in accordance to The Digital Services Act, 2022.[34]

The Artificial Intelligence Act (AIA) 2024 for the EU has provisions to regulate deepfakes and other AI generated content. It seeks to prevent abuse, but the impact on the freedom of AI creators and consumers could be devastating.[35]

United Kingdom

The *Online Safety Act, 2023* makes the issuance of non-consensual pornography through deep fakes illegal.[36] Even the House of Lords Report on AI Ethics, 2023 suggests that social network services should be liable for the failure to delete deepfakes.[37]

Spain imposed new rules that require deepfake content to be labeled as AI-generated. The penalties for noncompliance are exceedingly harsh for protecting the minors.[38] Spain's plans for 2025 include creating new laws aimed at preventing deepfake crimes against minors. The planned changes to the Penal Code would do the following like prohibiting using deepfakes to impersonate and annoy children. And to apply greater punishment for creating non-consensual deepfakes.[39]

This legislation arose from multiple incidents where AI-infused explicit deepfake images of teenagers were created using real minor's images, which was shocking and scandalous.[40]

In the middle of 2024, Rafał Brzoska, a Polish billionaire, appealed for help from renowned Polish personalities in order to sue Meta due to the widespread deepfake impersonation scams of fake-AI Meta's account that operated on its platforms. This was done with the hope that Meta would stop the deceitful deepfake impersonation scams without any expectation of compensatory damages.[41]

In 2024, a landmark case in Texas resulted in a woman winning 1.2 billion dollars from a lawsuit for showing intimate pictures without her consent. This case has exacerbated the fight for the federal act that would make distribution of non-consensual explicit content and deepfake images a crime.[42]

---

[32]Press Release, "NSA, U.S. Federal Agencies Advise on Deepfake Threats," *National Security Agency,* Sept. 12, 2023, available at: https://www.nsa.gov/Press-Room/Press-Releases-Statements/Press-Release-View/Article/3523329/nsa-us-federal-agencies-advise-on-deepfake-threats/ (last visited on Mar. 23, 2025).

[33]*Id*.

[34]Regulation (EU) 2016/679 of the European Parliament and of the Council, Official Journal of the European Union, L 119, 1-88 (Apr. 27, 2016), available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=LEGISSUM%3A310401_2 (last visited on Mar. 23, 2025).

[35]Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024, Official Journal of the European Union, L 277, 12 July 2024, pp. 1–157, available at: https://eur-lex.europa.eu/eli/reg/2024/1689/oj/eng (last visited on Mar. 23, 2025).

[36] *Id.*

[37]"UK Can Lead the Way on Ethical AI, Says Lords Committee," Artificial Intelligence Committee News, Apr. 16, 2018, available at: https://committees.parliament.uk/committee/376/artificial-intelligence-committee/news/94648/uk-can-lead-the-way-on-ethical-ai-says-lords-committee/ (last visited on Mar. 23, 2025).

[38]David Latona, "Spain to Impose Massive Fines for Not Labelling AI-Generated Content," *Reuters*, Mar. 11, 2025, available at: https://www.reuters.com/technology/artificial-intelligence/spain-impose-massive-fines-not-labelling-ai-generated-content-2025-03-11/ (last visited on Mar. 23, 2025).

[39]"Deceptive Audio or Visual Media ('Deepfakes') 2024 Legislation," *National Conference of State Legislatures*, Nov. 22, 2024, available at: https://www.ncsl.org/technology-and-communication/deceptive-audio-or-visual-media-deepfakes-2024-legislation (last visited on Mar. 23, 2025).

[40]Lauren Feiner, "The Senate Passed a Bill Cracking Down on Sexually Explicit Deepfakes," *The Verge*, Jul. 24, 2024, available at: https://www.theverge.com/2024/7/24/24205275/senate-passes-defiance-act-non-consensual-intimate-ai-deepfakes (last visited on Mar. 23, 2025).

[41] *Id*.

[42]Julianne McShane, "Texas Woman Awarded $1.2 Billion in 'Revenge Porn' Lawsuit," *NBC News,* Aug. 14, 2023, available at: https://www.nbcnews.com/news/crime-courts/texas-woman-awarded-12-billion-revenge-porn-lawsuit-rcna100159 (last visited on Mar. 23, 2025).

In the landmark case,[43] a plaintiff filed suit against Reddit because it hosted deepfake images of her without her consent. This case raised issues about the responsibility of platforms because Section 230 of the Communications Decency Act poses a restriction on liability.

Another case where the accused was arrested for allegedly creating deepfake photographs of women and distributing them on the internet. This case underlined the gap of legal measures in India to resolve offenses involving deepfakes.[44]

Furthermore, the UK case[45], where the British Broadcasting Corporation (BBC) sued some websites for publishing deepfake clips of its presenters. This case highlighted the lack of adequate measures to address the problem of nameless makers of deepfakes and to tackle this barrier, there is an acute demand for reinforced legislation.

NEED FOR STRONGER LEGAL PROTECTION

Deepfake technology has been used to create non-consensual pornographic materials - particularly aimed at women. Such misuse cause extreme distress and damage to one's reputation. A prime example would be of Cally Jane Beech, an ex-Love Island contestant, who found an AI-generated nude image of her on the internet.[46] This problem isn't limited to famous people; it subsumes countless unfortunate people who become stakeholders of non-consensual image manipulation.

This problem is not limited to facial modification, it also extends to emulating a person's voice as well, and the implications are far reaching. Distress of this nature is difficult to express and appreciate. On a macro scale, 98 percent of deepfake (videos) are pornographic. Further, 99 percent of the victimized demographic are women, including politicians, activists, and journalists.[47] Emotional and reputational damage stemming from this abuse is negative and debilitating in its own right.

The usage of deepfakes makes it easy to spread misinformation, which can damage the public's trust in media organizations and other institutions. A case in point, AI-generated deepfakes have been utilized in investment scam frauds, like what happened with Michael Hewson, a well-known analyst in the City. His image was altered in a video that advertised a scam WhatsApp group that claimed to offer astonishing returns.[48]

As an illustration, a McAfee survey reported that 75 percent of Indians admitted having seen deepfake content within the past year, especially the political deepfakes.[49] The advanced techniques used in deepfakes allow cybercriminals to execute impersonating deepfakes, which can aid them in financial fraud and identity theft. Because deepfake technology is so advanced, telling the difference between real content and false content is very hard.[50]

In Bengaluru, con artists made use of deepfake videos of well-known business personalities like N.R. Narayana Murthy, and Mukesh Ambani to defraud people with almost 1 crore rupees.[51] Also, the number of deepfake fraud cases in India have become over six-fold since 2019, with estimated loss of 700 billion rupees in 2024 alone.[52]

[43]Jane Doe et al. v. Reddit, Inc., Case No. SACV 21-00768 JVS (KESx), United States District Court, Central District of California, Oct. 7, 2021.

[44]State v. Vishal Sudhirkumar Jha, FIR No. 01/22, PS Special Cell, U/s 153A, 153B, 354A, 509 IPC & 66, 67 IT Act, Jan. 21, 2022.

[45]Suniti Singh, "Covid: France to Ease UK Travel Ban, Allowing EU Citizens to Return Home," *BBC News*, Dec. 22, 2020, available at: https://www.bbc.com/news/world-55348574 (last visited on Mar. 23, 2025).

[46]LAURA PARKIN FOR MAILONLINE, "Love Island's Cally Jane Beech Shook to Tears Over AI-Generated Nude Photos," *Daily Mail*, Aug. 15, 2023, available at: https://www.dailymail.co.uk/tvshowbiz/article-13029437/Love-Island-Cally-Jane-Beech-shook-tears-AI-pictures-nude.html (last visited on Mar. 23, 2025).

[47]Luke Hurst, "Generative AI Fueling Spread of Deepfake Pornography Across the Internet," *Euronews*, Oct. 20, 2023, available at: https://www.euronews.com/next/2023/10/20/generative-ai-fueling-spread-of-deepfake-pornography-across-the-internet (last visited on Mar. 23, 2025).

[48]*Id.*

[49]ETtech, "75% Indians Have Viewed Some Deepfake Content in Last 12 Months, Says McAfee Survey," *The Economic Times*, Apr. 25, 2024, available at: https://economictimes.indiatimes.com/tech/technology/75-indians-have-viewed-some-deepfake-content-in-last-12-months-says-mcafee-survey/articleshow/109599811.cm (last visited on Mar. 23, 2025).

[50]*Id.*

[51]Express News Service, "Deepfake Videos of Narayana Murthy, Mukesh Ambani: Bengaluru Residents Lose Rs 87 Lakh in Trading Scam," *The Indian Express,* Nov. 5, 2024, available at: https://indianexpress.com/article/cities/bangalore/deepfake-videos-narayana-murthy-mukesh-ambani-bengaluru-trading-scam-9654607/ (last visited on Mar. 23, 2025).

[52]BW Online, "India's Deepfake Cases Up 550%, Losses May Hit Rs 70,000 Cr By 2024: Report," *Business World*, Dec. 19, 2024, available at: https://www.businessworld.in/article/indias-deepfake-cases-up-550-losses-may-hit-rs-70000-cr-by-2024-report-541202 (last visited on Mar. 23, 2025).

CURRENT RELEVANT LAWS AND THEIR SCOPE

The current legal framework struggle to cater to the prevalent issues posed by deepfakes, and relevant legislation in India is non-existent. The outdated legal frameworks exist for digitally created content, making it next to impossible to impose sanctions against offenders. Pre-existing privacy regulations may fail to address the scope of digital impersonation or remedial action.

There exists no singular law in India which adequately addresses such issues of deepfakes and the term deepfake is absent in Indian legislative text. There are established laws like the *Information Technology Act of 2000*, and some portions of *Indian Penal Code* that deal with peripheral issues such as slander, identity theft, and cybercrime, but none focus on the fabrication and dissemination of deepfakes.

Because the internet is global, it becomes very easy for deepfakes that were made in one country to impact people in an entirely different country, making enforcement much more difficult because of differing legal norms. This cross-jurisdictional complexity was recently witnessed when a British soldier was sentenced to jail for posting sexually suggestive deepfake videos of women superimposed onto pornographic platforms.

The intricate nature of free speech poses a legal issue when one tries to regulate dangerous deepfakes. Content moderation policies might also be counterproductive and more radical than needed, making one wonder how far the policy can go.

The Indian courts have recognized the issues with deepfakes. In a recent case, Bollywood Actor Anil Kapoor won an identity theft lawsuit where AI technology was improperly using his image, which established principles for personality rights within the digital domain.[53]

To respond to the dangers posed by deepfakes, specialists and government officials put forward the proposal of advancing more protective measures, which include creating laws meant for the processes that involve the production and dissemination of harmful deepfake images. An example would be the proposed *Disrupt Explicitly Forged Images and Non-consensual Edits (DEFIANCE) Act of 2024* that seeks to identify and punish the perpetrators of non-consensual explicit deepfake images and video production.[54]

[53] *Id.*

[54] "Durbin, Graham, Klobuchar, Hawley Introduce DEFIANCE Act to Hold Accountable Those Responsible for the Proliferation of Non-consensual, Sexually-Explicit 'Deepfake' Images and Videos," *United States Senate Committee on the Judiciary*, Jan. 30, 2024, available at: https://www.judiciary.senate.gov/press/releases/durbin-graham-klobuchar-hawley-introduce-defiance-act-to-hold-accountable-those-responsible-for-the-proliferation-of-nonconsensual-sexually-explicit-deepfake-images-and-videos (last visited on Mar. 23, 2025).

RECENT DEVELOPMENTS HIGHLIGHTING THE NEED FOR ACTION

The legal cases in court have revolved around the use of deepfakes which shows a person in a light which is not true. An example is a Norwegian gentleman who made a complaint against ChatGPT because the system said her father murdered his children leading to the accusation of AI damaging their generated misinformation.[55] This has highlighted flaws within legal systems.

The British teachers have expressed the concern that their coworkers and pupils would be the objects of harassment and mudslinging, caused by the viral use of deepfakes leading to even tighter control of social media sites.[56] The UK government proposed severe restrictions on deepfake pornography hoping to shield victims of fake, non-consent pornography by introducing terms of imprisonment for producers and sellers of these materials.[57]

Some jurisdictions have attempted to pass legislation against creators of deepfakes, or 'impersonation' videos. The lack of proper technology and the existence of gaping holes in the law makes implementation doubtful. Take for example, the state of California where new legislations directed at restraining AI generated election misrepresentation video fakes face opposition, revealing the struggle of attempting to govern an advancing intelligence organic technology.[58]

The combination of deepfakes and other advanced technologies pose a major threat which can result in severe damage. The Ministry of Finance highlighted that cases of

[55] Hanan Dervisevic, "Norwegian Man Files Complaint Against ChatGPT for Falsely Saying He Killed His Sons," *ABC News*, Mar. 21, 2025, available at: https://www.abc.net.au/news/2025-03-21/norwegian-man-files-complaint-chatgpt-false-claims-killed-sons/105080604 (last visited on Mar. 23, 2025).

[56] Anjum Peerbacos, "Teacher Felt 'Worthless' After Facing Discrimination – As Report Warns Racism Is Harming Profession," *Sky News,* Oct. 27, 2024, available at: https://news.sky.com/story/teacher-felt-worthless-after-facing-discrimination-as-report-warns-racism-is-harming-profession-13241003 (last visited on Mar. 23, 2025).

[57] *Id.*

[58] *Id.*

sophisticated cyber fraud are increasing leading to a loss of millions at an alarming rate.[59]

Deepfake-related digital crimes have surged and resulted in major losses. CERT-In's advisory states that there is a heightened risk of deepfake manipulation which leads to misinformation, fraud, and damage to reputation.[60]

A PIL was recently placed before the Delhi High Court, calling for regulation of AI and deepfake technologies. The Delhi High Court's legislation AI along with deepfake technologies has a crucial need for these issues to be addressed and tackled. The court illustrated the astounding danger that deepfake technology poses to societies, including disinformation and the violation of the public sphere as well as the cover of democracy.[61]

FINAL THOUGHTS

The advancement of deepfake technology is of grave concern with its ability to be misused predominantly for creating dubious news, fraudulent activities, and other malicious content, although it does have some positive functions. In India, deepfake strangled elections, faked explicit videos to defame others, and financially scammed many people. The situation keeps worsening with each passing day and the power of the current laws are impotent to alleviate it.

As of now India does not have a law that directly addresses deepfakes. The *Information Technology Act* and the *Indian Penal Code* do cater to some peripheral crimes such as cyber infringement and slander, but their inception predated the existence of deepfake technology. Meaning, the fact that criminals can use deepfakes to inflict harm to a person and get away with it. Even when the cases are

[59]Hritam Mukherjee, "India Says Cyber Fraud Cases Jumped Over Four-Fold in FY2024, Caused $20 Million Losses," *Reuters*, Mar. 11, 2025, available at: https://www.reuters.com/world/india/india-says-cyber-fraud-cases-jumped-over-four-fold-fy2024-caused-20-mln-losses-2025-03-11/ (last visited on Mar. 23, 2025).

[60]Ken Kadet, "Deepfake Attacks Strike Every Five Minutes Amid 244% Surge in Digital Document Forgeries," *Business Wire*, Nov. 18, 2024, available at: https://www.businesswire.com/news/home/20241118521944/en/Deepfake-Attacks-Strike-Every-Five-Minutes-Amid-244-Surge-in-Digital-Document-Forgeries (last visited on Mar. 23, 2025).

[61]Bhavna Sharma v. Union of India (W.P.(C) 1762/2025); Nihit Dalmia, "Delhi HC Issues Notice on PIL Seeking Restrictions on DeepSeek," *The Law Advice*, Feb. 13, 2025, available at: https://www.thelawadvice.com/news/delhi-hc-issues-notice-on-pil-seeking-restrictions-on-deepseek (last visited on Mar. 23, 2025).