DECIPHERING THE LEGAL REGIMES GOVERNING DEEP-FAKES

Anisha Bhattacharjee, Research Scholar, Tezpur University

Kamal Lochan Das, Independent Researcher

ABSTRACT

Whereas global innovations and revolutionary advancements in the field of artificial intelligence have significantly modified our life and work styles, the threats these developments have put towards the mankind is truly undeniable. Deepfake technology, as such, are not inherently illegal, however its legal standing is complex and dynamic. It is true that the concept can be used for good in various ways such as creating subtitles and translations for videos, training simulations, healthcare, educational purposes or even public training campaigns etc. But added malicious intent makes the use of such advanced artificial intelligence (AI) features a potential threat for the mankind. As a result, incidence of false narratives, defamation, misinformation, non-consensual contents etc. are on a significant rise.

In modern India, the rising trend in the misuse of AI has become a potential threat. There are numerous instances where misinformation generated through deepfakes have influenced public opinion, exaggerated communal tensions and also challenged the frameworks of cybersecurity. This is to say that not only the common people, but also ministers, popular actors, noted signers etc. have been a victim of such perils. Thus, substantial efforts have become a requisite to develop counter measures and raise awareness on the issue. This paper shall explore the rising threat of deepfakes and misuse of technology especially within the Indian context, highlighting noted incidents and examining the broader social and ethical implications. Further, it shall also assess the present legal and regulatory responses within the nation. The paper also calls for a concerted effort among technology companies, policy makers, civil society to address such challenges, while ensuring the positive role for deep-fakes and mitigating its capacity for harm.

Keywords: Artificial Intelligence, Cybersecurity, Deepfake Technology, Dynamic, India

Introduction

The rapid growth in the field of artificial intelligence has undoubtedly reshaped economies, performed revolutions in industries and transformed daily lives. However, the deepfake technology has turned to be one of the most sophisticated tools of the AI era. In general, deepfakes are images, videos or even audio clips which are not from the original source but are made to look real. Technically, deepfakes are a part of synthetic media or generative media, which is a media term used to make or modify contents using artificial intelligence, mostly through automated means. It is created through 'deep learning', which is a method of AI to teach computers the way of processing data, which is inspired by the human brain. These models can even recognize complex data patterns in order to produce accurate results or even predictions. Distinguishing such generated contents from the original ones seems to be a highly challenging task in the present context, as detection tools are limited and the scope for cybercriminals in manipulating the original are many. However, the term 'deepfake' is not illegal in itself. If used judiciously, it can be immensely helpful in various fields such as healthcare, education, training programs etc.

The evolution of artificial intelligence can be traced back to the substantial works of the British mathematician in the mid-20th century named Alan Mathison Turing. In the year 1935, he described the concept of a computing machine which would consist infinite memory and also a scanner which could move in such a way through the memory that it can adapt the ability to read what it finds and write further symbols[1]. However, the groundwork for AI was laid by him in 1950 when he introduced the concept of machines which could simulate the intelligence of humans in his paper "Computing Machinery and Intelligence", through which he introduced a test to measure computer intelligence named 'Turing Test'[2]. In 1952, an American computer scientist Arthur Samuel designed a program which could play checkers, which happened to be one of the first to learn the game independently. Earlier efforts were made to train computers to play chess. However, the term 'Artificial Intelligence' was for the first time coined by an American computer scientist John McCarthy at the Dartmouth Conference in 1956, who is also known as the father of AI. During the 1950s - 1970s, AI researches were basically concentrated on symbolic reasoning and rule-based systems, which used logical steps to mimic human

[1] B.J. Copeland, *History of Artificial Intelligence | Dates, Advances, Alan Turing, ELIZA, & Facts | Britannica*, https://www.britannica.com/science/history-of-artificial-intelligence (last visited Nov 24, 2024).
[2] A. M. Turing, *I.—Computing Machinery and Intelligence*, LIX Mind 433 (1950).

problem-solving. The next decade i.e. 1970s - 1980s, lack of tangible results and over expectations led to reduced funding and interests, causing this field to face stagnation. It was in the 1980s which saw the introduction of neural networks, which revived AI researches once again. This period witnessed advances in algorithms, applications like handwriting recognition and chess playing programs etc.[3] Thereafter such researches flourished with the 'deep learning' revolution in 2010s, the advances in image recognition, development of Generative Adversarial Networks (GANs) by Ian Goodfellow in 2014, through which realistic synthetic images, videos or even audios could be generated – paving the way for deepfake technology[4]. Presently, voice assistant applications such as Siri, Alexa, transformer-based models such as GPT series Google's BERT etc. have made AI deeply integrated in our daily lives.

However, as AI continues to evolve, some of its features including deepfake technology has posed potential threats of various kinds. From generating copied music contents using artist's original work to blackmailing and reputational harm, manipulation of evidences, misinformation, manipulation in politics or even such manipulation in a company's stock price etc., these technological developments have also evolved challenges for cyber warriors.

In many countries, including India, the regulatory bodies have not yet provided any precise definition of 'Deepfakes'. Nor does they have any specific laws to address deepfakes and crimes related to AI. However, the laws are applied through existing penal provisions and other Acts and Rules such as the Information Technology Act 2000, Copyright Act 1957, The Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules 2021 etc.

The Deepfake Mechanism

The deepfake technology basically uses two kinds of algorithms (set of instructions through which computer understands how to learn and perform a task on their own) – a generator and a discriminator. While the generator produces the initial fake digital content by building a training data set which is based on the desired output, the discriminator mainly examines or evaluates how realistic or phony the original output of the digital material is. This process is further repeated so as to enable the discriminator to gain more accuracy in identifying any

[3] Neural Networks - History, https://cs.stanford.edu/people/eroberts/courses/soco/projects/neural-networks/History/history2.html (last visited Nov 26, 2024).
[4] Ian Goodfellow et al., *Generative Adversarial Networks*, 63 Commun. ACM 139 (2020).

errors in the outputs given by the generator, causing the generator to fix those errors while producing better results and more enhanced realistic content[5].

Later, the blend of the generator and discriminator algorithm together builds a generative adversarial network (GAN). The GAN then employs deep learning to identify the patterns of the original photos and thereafter makes use of those patterns to generate fake contents. While creating a deepfake, the system of GAN scans the photos from a variety of perspectives to collect as many information. In case of deepfake video, multiple perspectives such as the patterns of movement and speech, behavioural patterns are taken into account. The data is then subsequently passed through the discriminator for a several times to improve the final output of the image or video, to make it look as realistic to the real content[6].

Such deepfake contents are made in either of the two ways. They may use the targeted person's original video source in which the subject is made to say or do things they never did, or they may attach/swap a targeted person's face over another individual. Regardless, there are several ways to detect such attacks. Signs like body movements or facial positioning in unnatural ways, unnatural colouring, unnatural skin ageing. Moreover, there are several organizations which offer protection against deepfakes through software/websites in different ways –

Adobe - This software offers a system where producers/creators can attach their signatures to images and videos with information pertaining to their work.

Intel FakeCatcher – It is a tool that analyses authentic clues in original videos and examine pixels of videos to determine its originality. It mainly uses two methods – (a) Photoplethysmography (PPG) - which detects movements in blood flow, which is normally not replicated by deepfakes; (b) Eye movements. Intel claims that their detector can provide results with an accuracy of 96% in milliseconds.[7]

Operation Minerva – The technology makes use of digital fingerprints to identify revenge porn or deepfake videos, which is being shared on various popular adult video sharing

[5] Kinza Yasar, Nick Barney & Ivy Wigmore, *What Is Deepfake Technology? | Definition from TechTarget*, WhatIs, https://www.techtarget.com/whatis/definition/deepfake (last visited Nov 26, 2024).
[6] *Ibid.*
[7] David Salazar, *How Intel Is Putting Its AI-Optimized Processors to Work Detecting Deepfakes*, FAST COMPANY (2023), https://www.fastcompany.com/90957928/intel-fakecatcher-deepfake-detector (last visited Nov 24, 2024).

sites.

Sentinel – It is a cloud-based solution which uses a number of technologies such as face landmark analysis, flicker detection, temporal consistency checks to detect any manipulation in the media.[8]

Sensity.ai – Founded in the year 2018, this company is one of the first intelligence company, run by a team of machine learning researchers to defend other organizations against deepfake threats and suspicious visual contents.[9]

Presently, technology giants like Microsoft are constantly upgrading and offering AI-enabled softwares for deepfake detection such as Microsoft Video Authenticator. Few other examples of such application/websites are DuckDuckGoose, Resemble, HyperVerge's Deepfake detection, WeVerify, Paravision Reviews etc.

Notable Cases

Existing literature claims that the term 'deepfake' was first coined in the year 2017. A Reddit (social news and discussion sharing website) user with same username created a subreddit where netizens could share deepfake pornography which they had created using face-swapping software and celebrity photographs. Although the shady forum has since been removed, 'deepfake' has persisted to be used as new type of AI generated content.[10]

In the year 2019, the founder of Facebook Mark Zuckerberg became a victim of deepfake. A video was posted to the Facebook-owned Instagram which showed him bragging on how Facebook "owns" its users. The fake video was made with the intent to demonstrate how netizens may deceive the public, using such social media tools like Facebook.[11]

The former U.S. President Joe Biden has also been targeted with several deepfake incidents. In

[8] Sam Romain, *Sentinel AI: The New Frontier in Deepfake Detection*, https://www.romainberg.com/blog/artificial-intelligence/sentinel-ai-your-ultimate-deepfake-detection-solution/ (last visited Nov 24, 2024).
[9] Sensity.ai | World Economic Forum, https://www.weforum.org/organizations/sensity-ai/ (last visited Nov 24, 2024).
[10] Gabe Regan, *A Brief History of Deepfakes — Reality Defender*, https://realitydefender.com (last visited Nov 24, 2024).
[11] Rachel Metz & Donie O'Sullivan, *A Deepfake Video of Mark Zuckerberg Presents a New Challenge for Facebook | CNN Business*, https://edition.cnn.com/2019/06/11/tech/zuckerberg-deepfake/index.html (last visited Nov 24, 2024).

one of the recent cases, a political consultant from the U.S. Democratic Party was held with steep federal fines and criminal charges for creating a robocall to mimic the then president, urging citizens to avoid voting ahead of the state's presidential elections. Later, the Federal Communications Commission straightaway ruled AI-generated robocall as illegal.[12]

In 2022, amid the Russia-Ukraine war scenario, a video of the Ukrainian President Volodymyr Zelenskyy made rounds all over which showed that he had asked his people to put down arms and surrender before Russia and that the efforts of his army have failed. However, it turned out to be a deepfake video as it was identified that the size of his head was bigger to his body and that it was digitally attached. Again, in the same year, fake morphed videos of Russian President Vladimir Putin surfaced where he was spoke of giving up the war and declare peace, whereas in reality he never did so.[13]

Yet in another case, videos of the famous international actor and producer Tom Cruise went immensely viral on TikTok (a video sharing application) where he performed unusual activities like biting lollipop, showing tricks with coin etc. It was later identified that those activities were not real and were AI generated deepfakes.

There are uncountable cases of such kind even taking place in real time which have put immense mental harm to famous personalities, including the general public. Eliminating such indecent activities has become quite a challenge for technology companies in the realm of the present-day situation.

The Indian Scenario

The first ever case of deepfake in political campaigns in India can be traced to an incident in the year 2020, where numerous videos of Manoj Tiwari, a political leader were surfaced and widely spread in numerous WhatsApp groups, where he made allegations against his political rival Arvind Kejriwal before the Delhi elections in both Haryanvi and English. It was found that the video contents were morphed and made using AI. Again, a doctored video of a political

[12] Shannon Bond, *Criminal Charges and FCC Fines Issued for Deepfake Biden Robocalls: NPR*, https://www.npr.org/2024/05/23/nx-s1-4977582/fcc-ai-deepfake-robocall-biden-new-hampshire-political-operative (last visited Nov 24, 2024).

[13] Jane Wakefield, *Deepfake Presidents Used in Russia-Ukraine War*, Mar. 18, 2022, https://www.bbc.com/news/technology-60780142 (last visited Nov 25, 2024).

leader in Madhya Pradesh, Kamal Nath was circulated where he was shown to create confusions on the sustainability of the State Government's Laadli Behna Scheme.[14]

Even our Hon'ble Prime Minister has been a subject to such deepfake videos. In a widely circulated fake video, he was seen doing Garba (a festive dance of Gujarat). He later clarified that he has not done any Garba dance since school. He subsequently warned the citizens to be aware of such deepfake videos and has also asked concerned authorities to ban deepfakes and put warnings on such content being shared.[15] Advisories were issued by the government to all internet and social media intermediaries to have a control on its spread and ensure stricter standards.

Recently a case has been registered in Maharashtra against Maharashtra Youth Congress's social media handle along with sixteen others for reportedly circulating morphed videos of the Union Home Minister Amit Shah. In the video, he announced to curtail the reservation rights of SCs, STs and OBCs. The video was widely propagated with a malafide intent in order to harm the reputation of the Union Minister.

However not only politicians, even actors and normal public are in threat of such morphed contents. In 2023, the Delhi Police have arrested a main accused for sharing a deepfake video of Rashmika Mandanna, an Indian actress. In the video she was in a black outfit and entering a lift. On investigation it was found that the video was of a different woman and that her faced was similarly swapped on that woman.

In a recent survey conducted by a popular antivirus company named McAfee, it was found that over 75% of Indians have seen deepfakes in the past year and that at least 38% of them have been a victim. During a period of 12 months, every fourth Indian have come across political contents which were morphed.[16]

---

[14] Aaratrika Bhaumik, *Regulating Deepfakes and Generative AI in India | Explained*, THE HINDU, Dec. 4, 2023, https://www.thehindu.com/news/national/regulating-deepfakes-generative-ai-in-india-explained/article67591640.ece (last visited Nov 25, 2024).

[15] Marya Shakil, *"Recently Saw a Video...": PM Raises Concern Over Deepfakes*, NDTV.COM, https://www.ndtv.com/india-news/pm-narendra-modi-says-deepfake-a-big-concern-asked-chatgpt-team-to-give-deepfake-warning-in-content-4581834 (last visited Nov 25, 2024).

[16] 75% Indians have viewed some deepfake content in last 12 months, says McAfee survey, THE ECONOMIC TIMES, Apr. 25, 2024, 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 (last visited Nov 25, 2024).

A 73-year-old man Radhakrishnan has been scammed with deepfake voice call, where one of his former colleagues named Venu Kumar's voice was perfectly mimicked. He asked a loan of Rs. 40,000 from him saying that it was urgently needed for a cause. Without any hesitation Radhakrishnan transferred the money. On investigation it was found that it was a fraud deepfake call generated with AI software.[17]

Despite its good uses, deepfakes in any form has thus posed a serious threat. Numerous other examples of morphed images of people/actors in pornography films, morphed statements of public figures, fake voice calls etc. are some emerging challenges for concerned authorities to tackle in the present and especially in the time to come.

International Responses

The more we delve into the study of the deepfake technology, the more we understand that this technology is developing as a double-edged sword- where on one hand, it proves to be extremely helpful in ever evolving world of globalisation, where on the other hand its misuse give rise to critical legal, ethical and security concerns. Even though, countries around the world are constantly coming up with policies and strategies to tackle the menace of deepfakes, but the authorities are unable to do much due to the quick evolving nature of the technology. The deepfake softwares are undergoing rapid technological advancements, becoming more realistic, sophisticated and easy to use. Again, the global nature of the technology has led to the creation and distribution of deepfakes across borders, which further complicates the jurisdictional capacity of the authorities.

United States

Although the US have still not come up with any comprehensive law to regulate deepfakes, however some of the States have enacted some initiatives to either ban or restrict deepfakes and other misleading online content. The National Artificial Intelligence Initiative Act, 2000 was adopted to regulate the use of AI in various sectors such as education, research, development etc, but the legislation is silent on the regulation of deepfakes.[18] The US President

[17] Case Study: Kerala's First Deepfake Fraud, INDIAN CYBER SQUAD (2023), https://www.indiancybersquad.org/post/case-study-kerala-s-first-deepfake-fraud (last visited Nov 23, 2024).
[18] Eddie Bernice [D-TX-30 Rep. Johnson, *H.R.6216 - 116th Congress (2019-2020): National Artificial Intelligence Initiative Act of 2020*, (2020), https://www.congress.gov/bill/116th-congress/house-bill/6216 (last visited Nov 24, 2024).

Joe Biden in 2023 signed an executive order, which lists down a set of guidelines that the American companies and federal agencies must follow when it comes to designing, implementing and acquiring advanced artificial intelligence, maintaining security at its forefront before making it available for the public.[19] The Department of Commerce has been instructed to create basis for labelling contents generated by AI for easy detection, which is also termed as watermarking. States like Texas and California have enacted laws that criminalise the distribution and publishing of videos created by deepfake technology, which aims to impact the process of political elections. The State of Virginia has also enacted a law that penalises people, found guilty of distributing non-consensual deepfake pornography content.

The Congress in 2023 also came up with the DEEP FAKES Accountability Bill which aims "to protect the national security against the threats posed by deepfake technology and provide legal recourse to victims of harmful deepfakes."[20] The bill obliges creators to notify users when a content is altered and mark deepfakes on online platforms. The Congress also passed the DEFIANCE Act in 2024 which aims to "improve rights to relief for individuals affected by non-consensual activities involving intimate digital forgeries and for other purposes".[21] Some other legislations, like the Deepfake Report Act, 2019 mandates the Directorate of Science and Technology in the Department of Homeland Security, U.S to report the status of technology related to digital content forgery at definite intervals. Again, the Protecting Consumers from Deceptive AI Act, 2024 mandates the National Institute of Standards and Technology to create task forces for facilitating and informing the technical standards development and guidelines pertaining to the recognition of content produced by generative artificial intelligence (GenAI).

Further, the Colorado Artificial Intelligence Act, 2024, which shall come into effect in February 2026, will deliver more responsibilities on those who create and implement high-risk Artificial Intelligence systems.[22] Some other states like Florida and Louisiana have taken steps

[19] The White House, *FACT SHEET: President Biden Issues Executive Order on Safe, Secure, and Trustworthy Artificial Intelligence*, The White House (2023), https://www.whitehouse.gov/briefing-room/statements-releases/2023/10/30/fact-sheet-president-biden-issues-executive-order-on-safe-secure-and-trustworthy-artificial-intelligence/ (last visited Nov 24, 2024).
[20] Yvette D. [D-NY-9 Rep. Clarke, *Text - H.R.5586 - 118th Congress (2023-2024): DEEPFAKES Accountability Act*, (2023), https://www.congress.gov/bill/118th-congress/house-bill/5586/text (last visited Nov 26, 2024).
[21] Richard J. [D-IL Sen. Durbin, *Text - S.3696 - 118th Congress (2023-2024): DEFIANCE Act of 2024*, (2024), https://www.congress.gov/bill/118th-congress/senate-bill/3696/text (last visited Nov 24, 2024).
[22] Newly passed Colorado AI Act will impose obligations on developers and deployers of high-risk AI systems | White & Case LLP, (2024), https://www.whitecase.com/insight-alert/newly-passed-colorado-ai-act-will-impose-obligations-developers-and-deployers-high (last visited Nov 24, 2024).

to criminalise deepfakes that expose children engaging in sexual activities. Besides the newly enacted legislations, people falling prey to deepfakes can take recourse to the existing defamation laws, proving their innocence and demonstrating the harm caused to their reputation due to such act.

European Union

The Artificial Intelligence Act, 2024 passed by the European Parliament is a landmark legislation in addressing the Artificial Intelligence systems. The Act divides the AI systems into four risk categories-

Unacceptable risk- these systems are at highest level of risk. Systems like which exploit the vulnerabilities of children etc and are prohibited under the Act.

High risk- the AI systems will be subjected to specific legal obligations. Before the system is made publicly available, businesses need to undertake compliance tests and sign a declaration of the compliance. The system must be registered in a specialised European Union database.

Limited risk- these systems are susceptible to manipulation. For these, the Act imposes special transparency duties such as informing the users of their interaction with the AI, in order to let them make and informed choice about using the system.

Minimal or no risk- these systems have lowest level of risk. Examples include AI- enable games, spam filters etc.

The Act does not put a complete ban on deepfakes but binds the users and providers of the AI systems under some obligations such as related to issues related to transparency, accountability etc. For example, persons generating deepfakes must maintain records of their data and processes, ensuring awareness to the users interacting with the content etc.

France

In addition to the laws passed by the European Union, France has also passed a legislation to regulate the Artificial Intelligence environment. The newly enacted SREN law "(*Loi Visant à Sécuriser et Réguler l'Espace Numérique*)" aligns French legislation with new EU regulations

such as the Digital Services Act, 2022, the Digital Market Acts, 2022 and the Data Act, 2023.[23] The law seeks to govern the digital environment, tackle online fraud and shield minors from internet pornography. The law expressly outlaws the non-consensual dissemination of content created by deepfake unless it is evident that the content is generated artificially. The SREN Law adds to the Article 226-8 of the French Criminal Code to expressly "prohibit the act of sharing visual or audio content generated by algorithm processing and representing the image or speech of a person, without their consent, unless it is obvious or expressly mentioned that the content is algorithmically generated."[24] France has also taken steps to update its Criminal Code to insert provisions related to deepfakes, penalise the non-consensual dissemination of deepfakes related to pornography.

United Kingdom

As of yet, there are no laws in the United Kingdom that specifically deals with deepfakes. However, some current laws may apply for settling down disputes arising out of deepfakes. Under the Data Protection Act, 2018 and the General Data Protection Regulation, a person is entitled to claim in case of his personal data being misused. This personal data could include any information relating to the identity of a natural person. The use of personal data for generating deepfakes is likely considered to be use of personal data that an individual has not consented to, according to the General Data Protection Regulation.[25]

Again, if a person feels that his data has been used to create a deepfake, leading to the damage of his reputation, he can file a suit under the Defamation Act 2013 against the accused. The accused can be either the creator, the editor, the printer or publisher of the deepfake. The Online Safety Act, 2023 also contains provisions to address revenge pornography. Under the Act, the non-consensual sharing of intimate photos is regarded illegal, which also comprises images that have been digitally edited.

UK also entered to the world's first binding treaty on Artificial Intelligence- "the framework

[23] The SREN Law: 5 Things to Know About New French Legislation to Supplement the EU Data Act, Digital Services Act, GDPR and More, https://www.orrick.com/en/Insights/2024/06/The-SREN-Law-5-Things-to-Know-About-New-French-Legislation-to-Supplement-the-EU-Data-Act (last visited Nov 25, 2024).

[24]Christine Gateau, *France Prohibits Non-Consensual Deep Fakes*, (2024), https://www.hoganlovells.com/en/publications/france-prohibits-non-consensual-deep-fakes (last visited Nov 25, 2024).

[25]Considering deepfakes from a data protection perspective, (2023), https://www.brownejacobson.com/about/news-media/legal-issues-with-deepfakes (last visited Nov 25, 2024).

convention on AI and human rights, democracy and the rule of law".[26] The Government of the United Kingdom has however announced for the introduction of a consolidated legislation that will cater to all the problems arising out of the Artificial Intelligence systems and improve AI safety. The government aims to create an "appropriate legislation to place requirements on those working to develop the most powerful [AI] models".

Australia

There are no such laws relating to deepfakes in Australia as of now, but in June 2024, the Australian government has introduced the Criminal Code Amendment (Deepfake Sexual Material) Bill, which proposes to criminalise the dissemination of sexual content that shows or seems to show another individual, if-

> The content has been made without their consent
>
> The person making the content is careless regarding whether the agreement of communication has been received by him

The rule applies to both unaltered and altered digital material. Like the defamation laws in the UK, people being prey to deepfakes may also be able to submit their cases under the defamation laws in Australia. Most of the defamatory laws we come across often speaks about defamation caused through written or spoken words, but Australia's defamation laws also include images, along with digitally altered images to be considered as defamatory.

National responses

Even the abuse of deepfake technology is grippling the entire globe, as of now, India does not have any specified law to address the issue of deepfake or any other AI-related crime. However, the existing provisions related to cyber space such as the Information Technology Act, 2000, aided by the Bharatiya Nyaya Sanhita, can be taken recourse to for both criminal and civil violations relating to such technology. Deepfake crimes which violate people's privacy by capturing, publishing or transmitting their pictures in mass media are covered by Section 66E of the Information Technology Act, 2000. Such offences carry a maximum sentence of 3 years

[26] UK signs first treaty on AI and human rights, democracy and the rule of law, (2024), https://www.hoganlovells.com/en/publications/uk-signs-first-treaty-on-ai-and-human-rights-democracy-and-the-rule-of-law (last visited Nov 25, 2024).

in prison or Rs 2 lakh fine. Similarly, those who use computer resources or communication devices maliciously, resulting in cheating or impersonation are punished under Section 66D of the Act. A violation of this clause entails a fine of Rs 1 lakh and/or maximum sentence of 3 years.

Individuals engaged in the transmitting or publishing deepfakes, obscene in nature or containing sexually explicit acts can be prosecuted under Sections 67, 67A and 67B of the Act. Additionally, the IT Rukes forbid hosting "any content that impersonates another person" and mandate that social media companies promptly remove "artificially morphed images" of people upon notification. They run the risk of losing the "safe harbour" protection, which shields the social media companies from legal responsibility for user shared content from third parties, if they don't remove such content. The newly adopted criminal law, Bharatiya Nyaya Sanhita also consists provisions penalising certain acts such as dissemination of defamatory content via email[27], cheating by personation[28], phishing[29], hacking[30], child pornography[31] etc. Further, if any copyrighted picture or video has been used to produce deepfakes, the Copyright Act, 1957 may be also invoked.

The National Strategy and Responsible AI, published by the NITI Aayog in 2018 listed down a basic framework for using AI responsibly in India, but even though it does not adequately address the concerns posed by deepfakes and the further requirement of safeguarding the privacy of individuals.

The Indian government has made a significant effort to regulate the digital landscape, especially with regard to data security and privacy, via the Digital Personal Data Protection Act, 2023. The act creates a structure to cater to the technological issues particularly arising out of AI generated material. However, this legislation too does not specifically target the deepfake technology and its abuse. The Government of India is planning to make certain amendments to the Intermediary Rules, 2021, aiming to define deep-fakes, broadening the definition of "grievance" and alerting people to content that it is prohibited.[32]

[27] Bharatiya Nyaya Sanhita, 2023, No. 45, Acts of Parliament, 2023 (India) § 356.
[28] Bharatiya Nyaya Sanhita, 2023, No. 45, Acts of Parliament, 2023 (India) § 319.
[29] Bharatiya Nyaya Sanhita, 2023, No. 45, Acts of Parliament, 2023 (India) § 318(4).
[30] Bharatiya Nyaya Sanhita, 2023, No. 45, Acts of Parliament, 2023 (India) § 45.
[31] Bharatiya Nyaya Sanhita, 2023, No. 45, Acts of Parliament, 2023 (India) § 95.
[32] Rathin Bandhyopadhyay, Combatting Deep-Fakes in India- An Analysis of the Evolving Legal Paradigms and its Challenges, 15(1) INDIAN JOURNAL OF LAW AND JUSTICE, (2024).

Through a thorough study of the existing laws, it can be found out that India's regulatory framework for addressing the newly evolving offences in the cyber space, specially deepfakes is insufficient. Problems like identity theft, political disinformation and non-consensual explicit content underscore the pressing need for a strong legislative and judicial action.

Conclusion

After having a look into the global approaches towards the emerging technology of deepfake, it is evident that though similar measures are also in infancy stage in the technologically mature jurisdictions like the USA, EU, India needs quick legislative resolution and involvement to manage deep-fakes. Given the complex nature of India's socio-legal environment, the unchecked availability and usage of such technology might cause trauma and suffering for a large portion of the populace and policymakers should take this seriously. After the multiple deepfake instances in the country, starting from actors being victims to politicians, India is gradually acknowledging the risks and that only theoretical approach to the same will not only suffice. It is high time that India should come with laws specifically talking about deepfakes, its regulation and the ensuring the safety of the online space. In order to regularise such a technology which knows no boundaries, a substantial amount of research is required before any legislation is framed. India must also invest in solutions driven by technology such as AI-tools for detecting deepfakes, promote global cooperation and address the borderless nature of the technology.

Again, the maintenance of fundamental right to freedom of expression while implementing regulatory measures must also be balanced harmoniously. Transparency, public knowledge and accountability must be given top priority by nations and innovation and ethical protections must be balanced. India can establish itself as a captain in risk management and deepfake technology benefits by absorbing global best practices and adapting them in accordance to its requirements. At the end, protecting human rights, upholding social trust and guaranteeing the proper application of artificial intelligence will all depend on a coordinated worldwide strategy.