IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.53
Volume 4, Issue 5, March 2024

Analysis of Deepfake Technology and Present Legislation in India to Tackle It

Adv. Aishwarya Hemant Hiray
LLM 2nd Semester
School of Law, Sandip University, Nashik, Maharashtra, India
aishwaryahiray77@gmail.com

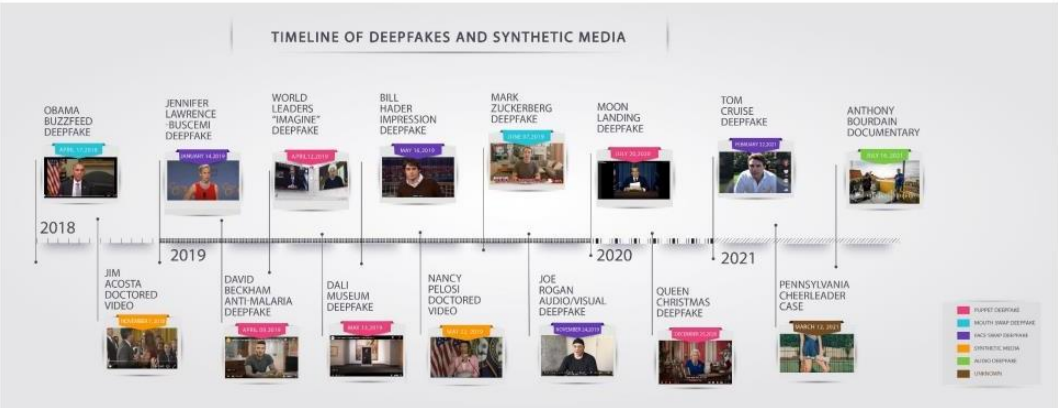
Abstract: *This research paper delves into the rapidly evolving landscape of deepfake technology. It looks at the different uses, possible dangers, and legal issues that deepfake raises. Advanced artificial intelligence algorithms enable the production of hyper-realistic synthetic media that can imitate and modify audio-visual content, a capability made possible by deepfakes. The legal implications of deepfakes are becoming more complicated as these technologies develop. It presents significant obstacles to intellectual property, security, privacy, and public confidence. This study attempts to give an in-depth overview to the idea of deepfake and the legal landscape around deepfake technology. It also analyses current laws and suggests new legal frameworks to deal with new issues that may arise.*

Keywords: Deepfake technology, artificial intelligence, privacy, defamation, Generative Adversarial Networks (GANs), large language models (LLM), Synthetic Media.

I. INTRODUCTION

The term deepfakes is derived from the fact that the technology involved in creating this particular style of manipulated content (or ―fakes‖) involves the use of deep learning techniques. Deep learning represents a subset of machine learning techniques which are themselves a subset of artificial intelligence. In machine learning, a model uses training data to develop a model for aspecific task. The more robust and complete the training data, the better the model gets. In deep learning, a model is able to automatically discover representations of features in the data that permit classification or parsing of the data. They are effectively trained at a ―deeper‖ level.

―Deepfake‖ technology, which has progressed steadily for nearly a decade, has the ability to create talking digital puppets. The A.I. software is sometimes used to distort public figures, like avideo that circulated on social media last year falsely showing Volodymyr Zelensky, the president of Ukraine, announcing a surrender. But the software can also create characters out of whole cloth, going beyond traditional editing software and expensive special effects tools used by Hollywood, blurring the line between fact and fiction to an extraordinary degree.



Rashmika Mandanna, Priyanka Chopra Jonas and Alia Bhatt are among the stars who have beentargeted by such videos, in which their faces or voices were replaced with someone else's.

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.53
Volume 4, Issue 5, March 2024

Pictures are often taken from social media profiles and used without consent.

AI-generated text is another type of deepfake that is a growing challenge. Whereas researchers have identified a number of weaknesses in image, video, and audio deepfakes as means of detecting them, deepfake text is not so easy to detect. It is not out of the question that auser's texting style, which can often be informal, could be replicated using deepfake technology.

All of these types of deepfake media – image, video, audio, and text – could be used to simulate or alter a specific individual or the representation of that individual. This is the primarythreat of deepfakes. However, this threat is not restricted to deepfakes alone, but incorporates the entire field of ‑Synthetic Media‖ and their use in disinformation.

II. METHODS

This research paper is purely based on secondary sources. This is done in order to comprehendthe idea of deepfake and analyse the legal landscape and implications of it. The research makes use of secondary sources of data, including journals, newspapers, websites, and so forth.

III. DISCUSSION

Deepfake technology has a wide range of legal implications in India, including issues with cybersecurity, intellectual property, privacy, and defamation. The production and distribution of deepfakes present serious privacy concerns since people may find themselves inadvertently included in altered content without their knowledge or agreement. This calls into question the Indian Constitution's guarantee of the fundamental right to privacy. Furthermore, deepfakes can be used maliciously, raising questions about the possibility of identity theft, character assassination, and damage to an individual's reputation.

The emergence of deepfakes has presented new obstacles for India's defamation laws since they can disseminate misleading information and damage the reputations of prominent people. The challenge of differentiating between real and fake content adds to the legal complications associated with deepfake defamation cases. Furthermore, the possibility of using deepfakes for misleading information and political manipulation emphasizes the necessity of strict cybersecurity laws to protect the integrity of public discourse.

Increasing threats and misuse potential in areas like identity theft, character assassination damage to image, reputation, and trustworthiness and the rapid obsolescence of existing technologies, highlighting the need for strong laws to protect people from these kinds of risks.

Laws against deepfakes in India:

In the USA, the Deepfakes Accountability Act (passed in2019), mandated deepfakes to bewatermarked for the purpose of identification.

In India however there is no explicit law banning deepfakes. Amidst the current laws in force,Sections 67 and 67A of The Information Technology Act 2000, provide punishment for publishing sexually explicit material in electronic form Section 66E of the IT Act of 2000, Capturing, publishing or transmitting a person's images in mass media, violating their privacy. This offense is punishable with imprisonment of up to threeyears or a fine of up to 2 lakh.

Section 66D of IT Act of 2000 ,It provides a provision to prosecute individuals who use communication devices or computer resources with malicious intent, to cheat or impersonate someone, which can result in imprisonment for up to three years and/or a fine of up to 1 lakh. Section 500 of the Indian Penal Code 1860, provides punishment for defamation, but these provisions are insufficient to tackle various forms in which deepfakes exist.

Section 499 of the Indian Penal Code, 1860 states that any person whose reputation has been damaged (or was intended to be damaged) by the material in question has the rights to sue for Defamation.

Section 51 of Indian Copyright Act of 1957, provides for penalties for certain offenses including infringement of copyright. It serves as a strong legal guardian, essentially discouraging acts ofintellectual property infringement. This particular section expressly prohibits the use of properties—whether they be creative works or anything else—that do not legally belong to another person in order to violate their exclusive rights.

On January 9, 2023, the Ministry of Information and Broadcasting issued an advisory to media organisations to exercise caution while airing content that could be manipulated or tampered with. The Ministry also advised media to clearly

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.53
Volume 4, Issue 5, March 2024

label any manipulated content as manipulated ormodified to ensure that viewers are aware that the content has been altered. But detailed segregation regarding to such newly emerging crimes is not available due to lack of legislation in that area.

IV. FINDINGS

Although there isn't any specific legislation in India that addresses challenges emerged by deepfake phenomena, the legal framework of the nation is supported by numerous initiatives andprovisions that can effectively tackle this threat. Given the increasing prevalence and complexity of deepfakes, it is quite possible that the Indian government, in its unwavering effort to safeguard the public from possible harm, will implement and announce new policies to fully address this growing threat. For example AI Advisory issued by Ministry of Information and Technology on March 1st 2024.

The advisory mandates that all platforms ensure their computer resources do not permit bias, discrimination or threats to integrity of electoral process through the use of AI, LLMs or similaralgorithms.

The safeguarding of individuals' privacy, the preservation of intellectual property, and the preservation of trust in the digital realm remain paramount objectives in the face of this evolvinglandscape of deception.

However, these laws are limited only to the misuse of deepfakes in the domain of sexually explicit content and, in a sense, present only a narrow view of the otherwise various domains inwhich deepfake can percolate. Therefore, laws in the current legal system neither provide adequate solutions for the regulation of deepfakes nor provide any means for detecting deepfakes

V. CONCLUSION

In response to these challenges, legal frameworks in India must evolve to encompass the unique aspects of deepfake technology. This may involve amendments to privacy laws, the introduction of specific regulations addressing deepfake creation and dissemination, and the enhancement of cybersecurity measures to prevent malicious uses. Collaboration between legal experts, technologists, and policymakers is essential to establish a comprehensive and adaptive legal framework that can effectively address the intricate legal implications of deepfake technology in the Indian context.

VI. SUGGESTIONS

Western countries are moving faster than India in formulating laws to tackle threats of emerging technologies. India needs to adapt this behaviour and follow the path West is on.

For example The AI Act is a proposed European regulation on artificial intelligence (AI) – the first comprehensive regulation on AI by a major regulator anywhere. In case of USA in January 2024, representatives proposed the No Artificial Intelligence Fake Replicas And Unauthorized Duplications (No AI FRAUD) Act.

VII. ACKNOWLEDGMENTS AND ETHICAL STATEMENTS

This research Paper would not have been possible without sheer support and guidance by my guide Dr. Sharvari Vaidya, encouragement by my peers and family and resources available at my fingertips through internet.

BIBLIOGRAPHY

[1]. Nobert Young, Deepfake technology: Complete Guide to Deepfakes, Politics and Social Media, 20-70 (Amazon Digital Services LLC Prints,2019)

[2]. Nina Schick, Deepfakes: The Coming Infocalypse,80-150 (Grand CentralPublishing, 2020)

[3]. Micheal Grothaus, Trust No One: Inside the World of Deepfakes, 120-200(Hachette UK,2021)

[4]. Ashish Jaiman, ―The danger of deepfakes‖ article , The Hindu newspaper , Jan 1st 2023

[5]. Vasundhara Shankar, ―Deepfakes Call for Stronger Laws‖, The Hindu Business Line , July 16th 2023

[6]. Mekhail Mustak, Joni Salminen, Matti Mäntymäki, Arafat Rahman, Yogesh K. Dwivedi , ―Deepfakes: Deceptions, mitigations, and opportunities‖ ,in science direct journal

[7]. https://www.buzzfeed.com/craigsilverman/obama-jordan-peele-deepfake-videodebunk-buzzfeed

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.53
Volume 4, Issue 5, March 2024

[8]. https://apnews.com/article/entertainment-north-america-donaldtrump-us-news-ap-top-news-c575bd1cc3b1456cb3057ef670c7fe2a

[9]. https://fortune.com/2019/01/31/what-is-deep-fake-video/

[10]. https://www.campaignlive.com/article/deepfake-voice-tech-usedgood-david-beckham-malaria-campaign/1581378

[11]. https://scifi.radio/2019/05/29/watch-world-leaders-sing-for-peacein-canny-ais-imagine-video/

[12]. https://www.technologyreview.com/2019/06/12/134992/facebook-deepfakezuckerberg-instagram-social-media-election-video/