TACKLING DEEPFAKES IN THE AGE OF GENERATIVE AI 0 AN INDIAN PERSPECTIVE

S. Sirisha

Introduction

Generative Artificial Intelligence (AI) is a large language model that is capable of creating an output based on the data it has been trained on and the prompt initiated by the user of the model. In November 2022, the non-profit OpenAI made ChatGPT freely accessible to the world. Similar generative AI models such as Dall-E, Audiocraft, Dream and Reface are capable of recreating a wide range of creative works. Laws have been tacking misuse of technology in many ways including the expansion of existing laws to fit in the definitions of technology-related crimes. The issue has always been that policymakers cannot keep up with the speed of technological developments in the 21st century. Deepfakes rose to fame quickly as people saw how effective the technology had become. This author believes that technology can be free to bloom until its vines interfere with the rights of the people. There is a need for a clear and effective legal regime that can prevent the violation of these rights and not merely deal with the disruptive aftermath of AI. The paper looks at how the existing laws in India address the concerns raised by deepfake technology and the recent developments in tackling the gaps.

Deepfakes

Deepfakes are created using a machine learning mechanism called the generative adversarial networks[1] in which the neural networks are trained on a large data set of images, videos and audio. The network is capable of generating synthetic data and improves itself through a feedback mechanism. The highly realistic data or outputs are generated after a repeated loop of self-development. Therefore, the technology similar to other generative AI systems is constantly evolving. Imagery forgery is an apt term used to define deepfakes. In recent times,

[1]Shubham Pandey, Gaurav Jadhav, Emerging Technologies and Law: Legal Status of Tackling Crimes Relating to Deepfakes in India, (*SCC Online Blog, 2023*) <-crimes-relating-to-deepfakes-in-india/https://www.scconline.com/blog/post/2023/03/17/emerging-technologies-and-law-legal-status-of-tackling-crimes-relating-to-deepfakes-in-india/> accessed 15 December 2023

it has become more challenging to identify deepfakes. The deception in the minds of the people in itself can cause a plethora of concerns.

Legal Concerns

The use of Deepfake technology can come in various forms. The technology has been around for a while and has been used by the entertainment and media industry to improve the visual effects of cinematograph films. The recent bloom of the AI industry has seen a rise in a large number of deepfake technology applications. In combination with social media, or any other communication platforms, the misuse of deepfake technology can have a wider impact. The technology essentially allows any person to impersonate another, be it public figures or common people. In 2020 videos of politician Manoj Tiwari, one in English and one in Haryanvi, went viral on social media platforms a day before the Delhi Elections, posing a threat to democracy as well.[2] As recently as November 2023, the viral deepfake videos of several Bollywood actors led to them requesting legal remedies in response to the technology.

Disseminating information through the *impersonation* of another person is disseminating *misinformation*. The communication of such videos and content to the general public causes' deception in the minds of the people and is against the general interest of the public. Such use is more dangerous when used to impersonate people of power and influence. It further violates the *personality rights* of public figures, that is protected under various laws in India.

Generative models such as deepfakes are fed data that might contain the personal data of individuals such as images, biometric data, personal information and other categories of personal data without the consent of such individuals. Lack of *consent* is an issue for the generation and publication of this data as well. The new Data Protection laws are yet to address unauthorised use of personal data in a direct violation of the *right to privacy*.

Deepfake technology can act as a *medium for several crimes*, both in cyberspace and in real time. It can enable people to easily generate content that could be used to manipulate public opinion, spew false propaganda, sabotage businesses and markets, and even violate intellectual property amongst a long list of criminal and civil wrongs.

There are global concerns about the governance of AI and the implications of the use of such deceptive technology. In light of this brief discussion on the concerns that deepfake technology

[2] Prashasti Awasthi, 'BJP leader Manoj Tiwari used deepfake videos to reach out to voters in Delhi: Report' (*The Hindu Businessline, 2020*) <https://www.thehindubusinessline.com/news/national/bjp-leader-manoj-tiwari-used-deepfake-videos-to-reach-out-to-voters-in-delhi-report/article30857871.ece> accessed 18 December 2023

brings, it is fair to say that AI is a technology that is more disruptive than most technologies developed in the past couple of decades.

Under Existing Laws

The concerns of privacy, malice in impersonating, misrepresentation and misinformation can in a limited manner be tacked under the Information Technology Act, 2000 (hereinafter referred to as IT Act) and its corresponding Rules. Under the IT Act, Section 66D imposes a punishment of up to three years of imprisonment on anyone who cheats by impersonating another using any communication device or computer resource. Section 66E[3] imposes penalties for the violation of an individual's privacy by "*capturing, publishing, and transmission of images of a person's private area without their consent*". Sections 67, 67A and 67B further address the concerns of publishing or transmitting obscene material.[4]

The Indian Penal Code, 1860 (hereinafter referred to as IPC) consists of several provisions under which malicious use of deepfake technology can be called an offence. However, there is nothing to directly address the extremity of the offences that can be committed. Sections 499 and 500 of the IPC provide a remedy for criminal defamation. Such content creators can also be prosecuted for public nuisance.[5]

Section 79 of the IT Act, on the one hand, exempts the internet intermediaries from any liability due to third-party actions. On the other hand, Rule 7 of the Intermediary Guidelines and Digital Media Ethics Code Rules of 2021 [6] makes them liable for punishment under any law, including the Indian Penal Code where they fail to observe the rules.

Recent Developments

In October 2023, in a significant judgment, the Delhi High Court upheld the personality and privacy rights of the Plaintiff in *Anil Kapoor v Simply Life India & Ors*.[7] The judgement highlights the rights of celebrities in the fact of misuse of artificial intelligence technologies.

[3] The Information Technology Act 2000
[4] The Information Technology Act 2000
[5] The Indian Penal Code 1860
[6] The Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules 2021
[7] 2023 SCC OnLine Del 6914

In the light of increasing cases of deepfakes and the spread of misinformation, the Indian Government has adopted a zero-tolerance policy on the matter. After the minister of state for Skill Development and Entrepreneurship and Electronics and IT expressed that the Government intends to make stricter rules, an Advisory was issued to the significant social media intermediaries.[8]

"*It is a legal obligation for online platforms to prevent the spread of misinformation by any user under the Information Technology (IT) rules, 2021. They are further mandated to remove such content within 36 hours upon receiving a report from either a user or government authority. Failure to comply with this requirement invokes Rule 7, which empowers aggrieved individuals to take platforms to court under the provisions of the Indian Penal Code (IPC). It is imperative that platforms take proactive measures to combat this threat.*"[9]

The purpose of the advisory[10] is

1. to ensure that reasonable efforts and due diligence are exercised in the identification and removal of misinformation and deepfakes
2. Any such cases must be addressed and resolved expeditiously as prescribed under the IT Rules of 2021
3. Users are caused not to host such content
4. Removal of reported content within 36 hours of reporting,
5. To adhere to the timelines under the IT Rules 2021 and disable access to such content.

The Government further urged the victims of such activities to approach the police authorities to file a criminal complaint under the Information Technology Rules 2021 and relevant provisions of the IPC. They are yet to release a set of rules to directly address the adversities of artificial technology, specifically deepfake technology.

While these developments show some action on behalf of the Central Government, there might be a gap in the penalising the users of the technology. While most of these technologies are available to the public freely, there must be governmental regulation in the creation of these applications. For instance, the proposed EU AI Act cat[11]egorises AI systems based on the extent

[8] Ministry of Electronics and IT, 'Union Government issues advisory to social media intermediaries to identify misinformation and deepfakes' (*PIB Delhi, Nov 2023*) <https://pib.gov.in/PressReleaseIframePage.aspx?PRID=1975445> accessed on 15 December 2023
[9] https://pib.gov.in/PressReleaseIframePage.aspx?PRID=1975445
[10] id
[11] European Commission, Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL LAYING DOWN HARMONISED RULES ON ARTIFICIAL INTELLIGENCE (ARTIFICIAL

of risk it can impose. Specific regulations might be effected on deepfake applications based on the high risks especially because they can affect the psyche of the general public.

Conclusion

The way to combat the misuse of technology is a long-fought battle by governments around the world. It is necessary to ensure that the issue is addressed both technically and legally. Where the internet intermediaries can regulate the content on their respective platforms, there is a need for technical regulation as well. For instance, rules to mandate content producers to issue notice to the viewer of the presence of AI-generated content can ensure that the public is aware of the fact and is not largely misled.

Directly violating the right to privacy under Article 21 of the Indian Constitution, there is also a need for awareness amongst the public about the adversities of deepfakes and particularly, the effects of misinformation.

Deepfake technology poses serious legal and ethical concerns to the Indian society. The existing laws are inadequate to address these concerns effectively. There is a nature of ex-post administration of the legal principles while there is a need for preventive action. While this paper only briefly addresses the issues attached to the matter, there is more to be explored in terms of remedies and regulations.

INTELLIGENCE ACT) AND AMENDING CERTAIN UNION LEGISLATIVE ACTS, (2021) < https://eur-lex.europa.eu/resource.html?uri=cellar:e0649735-a372-11eb-9585-01aa75ed71a1.0001.02/DOC_1&format=PDF> accessed 18 December 2023