ABHIDHVAJ LAW JOURNAL

[www.abhidhvajlawjournal.com]

The goal of Abhidhvaj Law Journal is to offer an open-access platform where anyone involved in the legal profession can contribute their research on any legal topic and aid in building a quality platform that anyone can use to advance their legal knowledge and experience.

Editor In chief – Assistant Professor Mr. Janmejay Singh

Publisher & Founder – Vaibhav Sangam Mishra

Frequency – Quarterly (4 Issue Per year)

ISSN : 2583-6323 (Online)

REGULATING DEEPFAKES: ADDRESSING THE LEGAL AND ETHICAL CHALLENGES.

AUTHOR'S NAME – Krishna Raj Sharma, LL.B, Final year.

INSTITUTION NAME - Dr. B.R. Ambedkar Law University, Jaipur.

ABSTRACT:

Deepfakes are a growing threat in today's digital environment. They are produced using artificial intelligence (AI) techniques, which have become a major concern. In the Indian context, the legal system in India is examined, its legal system is compared to that of other nations, and risks are identified as they are being used in the market. India's existing legal framework provides some recourse for addressing these threats, but specific legislation and dedicated regulatory measures are needed to effectively combat this growing threat. Various case studies are discussed in order to foresee the potential of this technology. This manuscript also discusses various risks involved in videos and other media created or morphed using deep fake technology. Although various nations have taken notice of this technology and its possible usage, they are yet to make a proper system to control the repercussions of this innovation. In the final section, various suggestions that are either implemented or could be implemented are discussed in order to take advantage of this new technology and at the same time minimize the damages. By implementing comprehensive regulations, promoting media literacy, and fostering collaboration among stakeholders, India can navigate the complex legal and ethical challenges posed by Deepfake, safeguarding individuals and society as a whole.

Keywords: Deepfakes, Artificial intelligence (AI) Regulation, Legal framework, Copyright infringement.

INTRODUCTION:

In today's digital environment, deepfakes—artificial media produced using artificial intelligence (AI) techniques—have become a major concern. These altered audio, video, or visual representations have the power to deceive, control, and hurt people, societies, and organizations. The regulation of deepfakes is essential in the Indian context, where false information and fake news have already disrupted society. Deepfakes present serious risks to many aspects of society as their use spreads more widely. Deepfakes can imitate real-world situations convincingly due to their extraordinary precision in manipulating both the visual and

audio content, making it difficult for viewers to distinguish between actual and manipulated content. It poses not only ethical problems but legal problems as well. It can possibly be used to fabricate evidence for the court or to defame a person or a brand in a subtle manner which can damage the reputation of that person or brand which wouldn't be proved in the court thereby escaping justice. Here, the legal system in India is examined, its legal system is compared to that of other nations, risks are identified, and deepfakes are discussed as they are being used in the market.

EXISTING LEGAL FRAMEWORK IN INDIA:

The defamation, privacy, identity theft, and intellectual property laws now in force in India serve as the foundation of the country's legal framework for dealing with deepfakes. The two main sources of law governing digital content are the Information Technology Act, 2000[1] (IT Act) and the Indian Penal Code[2] (IPC). To address deep fake-related offenses, Sections 66E (Violation of privacy) and 66F (Cyber terrorism) of the IT Act, as well as Sections 463 (Forgery), 464 (Making a false document), and 499 (Defamation) of the IPC, are invoked.

Deepfakes are a growing issue, but the existing legal framework does not specifically deal with them, leaving loopholes that must be filled. Additionally, specific laws must be passed to address deep fake-related crimes due to the procedural difficulties in locating and prosecuting deep fake creators.

Additionally, section 52 of the Copyright Act, of 1957[3] goes on to list the instances and circumstances in which there is no copyright infringement and discusses the principle of fair dealing. Deepfakes in this instance are not covered by the exceptions listed in section 52 of the Copyright Act, of 1957. Therefore, any crime performed utilizing deep fakes will be considered a copyright violation.

The liabilities of intermediaries can also come into question because the intermediaries are the platforms where the deep fake content is uploaded and thus are subjected to Section 79 of the Information Technology Act, 2000.[4] According to the section, the intermediary may remove the content in question after realization/knowledge of its presence or court order.[5]

[1] The Information Technology Act, 2000, No. 21, Acts of Parliament, 2000 (India).
[2] The Indian Penal Code, 1860, No. 45, Acts of Parliament, 1860 (India).
[3] The Copyright Act, 1957, No. 14, Acts of Parliament, 1957 (India).
[4] Jai Khurana, Is Indian law equipped enough to deal with deepfakes, blog.ipleaders, (Jun. 27, 2023, 9:29 AM), https://blog.ipleaders.in/is-the-indian-law-equipped-enough-to-deal-with-deepfakes/
[5] *Id.* at 02.

COMPARISON WITH OTHER COUNTRIES:

Several nations have taken action to control deep fakes. For instance, various states in the United States have laws that address electoral interference, defamation, and privacy. For example, Texas (a state in the United States of America) adopted a law that was more concerned with interfering in elections.[6] The production and distribution of a deep fake video within 30 days of an election with the intention to "injure a candidate or influence the result of an election" is now considered a Class A misdemeanor, according to the law.[7] A deep fake is defined by law as a video that was "created with the intent to deceive, that appears to depict a real person performing an action that did not occur in reality."[8]

2019 saw the introduction of regulations by the Chinese government requiring people and organizations to disclose when deep fake technology has been used in videos and other media.[9] Additionally, deepfakes cannot be distributed according to the regulations without a clear statement that the content was generated artificially.

The law passed in the United States also only applies to certain states, not across the country. Consequently, the law is inapplicable if the person who created the pornographic deep fakes is not a resident of the relevant state, therefore anyone who may have been humiliated or misled by them has no legal remedy.

The three-pronged Canadian approach to deepfake regulation consists of prevention, detection, and response.[10] In prevention, The Canadian government seeks to raise public awareness about the technology and develop preventative technology to stop the production and spread of deep fakes.[11] In detection, the government has made investments in the study and creation of deep fake-detecting technology. In response, the government is looking into new legislation that would make it unlawful to produce or distribute deepfakes with malicious intent.[12]

[6] David Ruiz, *Deepfakes laws and proposals flood US*, MALWAREBYTES LABS (Jun. 18, 2023, 6:30 PM), https://www.malwarebytes.com/blog/news/2020/01/deepfakes-laws-and-proposals-flood-us
[7] David Ruiz, Deepfakes laws and proposals flood US, malwarebytes, (Jun. 27, 2023, 9:29 AM), https://www.malwarebytes.com/blog/news/2020/01/deepfakes-laws-and-proposals-flood-us
[8] *Id.* at 03.
[9] Amanda Lawson, *A Look at Global Deepfake Regulation Approaches*, RESPONSIBLE AI INSTITUTE (Jun. 19, 2023, 7:10 PM), https://www.responsible.ai/post/a-look-at-global-deepfake-regulation-approaches
[10] *Id.* at 03.
[11] *Id.* at 03.
[12] *Id.* at 03.

India, in contrast, has not yet passed any particular regulation that targets deepfakes. The lack of a specific legal framework emphasizes the necessity of comprehensive rules for addressing the possible risks posed by deep fakes.

CASE STUDIES:

1. Rana Ayyub Deepfake: In 2018, journalist Rana Ayyub fell victim to a deep fake video where her face was superimposed on a pornographic video, aiming to discredit her.[13] Rana Ayyub's image had been modified into a sex tape and spread as though she had performed in it. This vicious assault happened not long after she started a campaign for the victim of the Kathua rape[14]. Rana also saw herself part of several fake tweets circulated on the Twitter platform, all edited to look authentic: the blue tick intact. The incident highlights the potential damage that deep fakes can inflict on an individual's reputation and mental well-being.[15]
2. Political Deepfakes: Political figures in India have also been targeted. Deepfake videos of politicians, depicting them engaging in controversial acts or making false statements, have the potential to disrupt elections and sow discord among citizens.[16] A former chief minister Vijay Rupani was seen in a morphed video where he is singing a Taylor Swift song which was a dead giveaway that the video is a fake. A businessman named Kishan Arvind was arrested for circulating that video. In another case, a politician named Gulab Singh Yadav was seen in an obscene video that was allegedly being circulated to defame the politician and his party.[17]
3. Deepfakes used for promotion: There have also been some instances, where political leaders used Deepfakes to efficiently appeal to more people for campaigning in election

[13] *I was vomiting: Journalist Rana Ayyub reveals horrifying account of deepfake porn plot,* INDIA TODAY (Jun. 19, 2023, 7:45 PM), https://www.indiatoday.in/trending-news/story/journalist-rana-ayyub-deepfake-porn-1393423-2018-11-21

[14] *Trial Of Main Accused In Kathua Rape-And-Murder Case To Resume Today*, NDTV (Jun. 20, 2023, 6:30 PM), https://www.ndtv.com/india-news/trial-of-main-accused-in-kathua-rape-and-murder-case-to-resume-today-4128894

[15] By India Today Web Desk, I was vomiting: Journalist Rana Ayyub reveals horrifying account of deepfake porn plot, indiatoday, (Jun. 27, 2023, 9:29 AM), https://www.indiatoday.in/trending-news/story/journalist-rana-ayyub-deepfake-porn-1393423-2018-11-21

[16] *Deepfakes or poll weapons? Gujarat cops worried over morphed videos*, THE TIMES OF INDIA (Jun. 20, 2023, 8:10 PM), https://timesofindia.indiatimes.com/city/ahmedabad/deepfakes-or-poll-weapons-gujarat-cops-worried-over-morphed-videos/articleshow/98287670.cms?from=mdr

[17] *Id.* at 04.

season. For example, in 2020, during the campaigning of the Delhi legislative assembly elections, a deep fake of Manoj Tiwari, the president of India's ruling Bharatiya Janata Party (BJP), went popular around the nation on WhatsApp.[1819] This was the first time a political party had ever employed a deep fake during a campaign. In the original video, Tiwari addresses the audience in English while criticizing his political rival Arvind Kejriwal, and urging them to support the BJP.[20] Using deep fake technology, the second video had been modified so that the man's lips genuinely move while he speaks Haryanvi, the Hindi dialect used by the BJP's target electorate. Although the technology was used with no bad intention, it shows how potentially it can be used to mislead people into believing something that is not true.

Deepfake technology will certainly gain popularity during the next several years. Although this technology has certain useful applications, deepfakes can have a significant negative impact on social institutions as well as personal interests. These include the weakening of the media, the rule of law, and democracy as well as fraud, identity theft, reputational injury, and fraud. Most dangerous deep fakes are already regulated and forbidden by the legal system. An enforcement problem is the main issue with deep fakes.

RISKS INVOLVED:

Deepfakes are frequently employed for the aim of spreading misleading information. They may be made with the intention of intimidating, humiliating, and undermining someone. Deepfakes have the potential to spread false information and confusion about important issues. The risk is not only getting false information from someone but also getting yourself involved in the sharing cycle.[21] Video or photo which contains or shows some kind of strong emotion towards some celebrity, politician or anyone, must not be shared with anyone, even with your friends, because not only you are contributing to the popularity of that media but also you are putting yourself at risk of legal liability.

[18] Charlotte Jee, *An Indian politician is using deepfake technology to win new voters*, MIT TECHNOLOGY REVIEW (Jun. 21, 2023, 6:00 PM), https://www.technologyreview.com/2020/02/19/868173/an-indian-politician-is-using-deepfakes-to-try-and-win-voters/

[19] By India Today Web Desk, I was vomiting: Journalist Rana Ayyub reveals horrifying account of deepfake porn plot, indiatoday, (Jun. 27, 2023, 9:29 AM), https://www.indiatoday.in/trending-news/story/journalist-rana-ayyub-deepfake-porn-1393423-2018-11-21

[20] *Id.* at 05.

[21] *How are deepfakes dangerous?*, NEVADA TODAY (Jun. 23, 2023, 7:10 PM), https://www.unr.edu/nevada-today/news/2023/atp-deepfakes

If you come across a deep fake, stop spreading it right away. You might think that you can use this to show your friends what a deep fake looks like, but once you share something, it often develops a life of its own.[22]

A lawyer with competence in media law should be contacted right away if you find yourself in a deep fake. Even if a picture or video appears to have been created for "fun," it is still unlawful if it was created without your knowledge or consent.

EFFORTS BEING MADE AND SUGGESTIONS:

Recognizing the need to regulate deepfakes, various stakeholders, including legal experts, policymakers, and technology companies, have called for stringent measures. The establishment of a dedicated regulatory authority, amendment of existing laws, and the introduction of new legislation specific to deep fakes have been suggested as potential solutions to address the challenges. Here are some key efforts and recommendations:

1. Dedicated Regulatory Authority: There have been proposals to establish a specialized regulatory authority or a task force that focuses on monitoring and addressing deep fakes.[23] This authority could coordinate efforts between law enforcement agencies, technology experts, and other stakeholders to develop strategies and guidelines for tackling deep fake-related offenses effectively.
2. Awareness and Education: Promoting awareness and educating the public about deep fakes and their potential risks is crucial.[24] Initiatives to enhance media literacy and critical thinking skills can empower individuals to identify and combat the spread of deepfakes. Collaboration between government bodies, educational institutions, and civil society organizations is essential to implement effective awareness campaigns.
3. Technological Solutions: Collaborations between technology companies and policymakers are vital to developing advanced detection and authentication tools. Investing in research and development of AI algorithms capable of identifying deepfakes can aid in their detection and mitigation. Encouraging the responsible use of AI technologies, through ethical guidelines and standards, can also contribute to reducing the misuse of deepfakes.

[22] *Id.* at 05.
[23] Yvette Wagensveld, Bart van der Sloot, *Deepfakes: regulatory challenges for the synthetic society*, 46 Computer Law & Security Review, (2022), https://www.sciencedirect.com/science/article/pii/S0267364922000632/pdf
[24] *Id.* at 06.

4. Legal Reforms: Amending existing laws or introducing new legislation specifically targeting deep fakes is necessary. The legislation should focus on criminalizing the creation, distribution, and malicious use of deepfakes. It should also outline penalties for offenders and provide mechanisms for the speedy removal of deep fake content from online platforms.
5. International Cooperation: Given the borderless nature of deep fake dissemination, international cooperation is crucial. Collaborating with other countries to share best practices, intelligence, and technological advancements can help establish a coordinated global response to deep fake-related challenges.
6. Public-Private Partnerships: Engaging in public-private partnerships can foster a collective approach to addressing deepfake challenges. By bringing together stakeholders from government, industry, civil society, and academia, collaborative efforts can be undertaken to develop comprehensive solutions, share best practices, and establish codes of conduct for the responsible use of AI technologies.
7. Ethical Guidelines and Standards: Developing ethical guidelines and standards for AI and deep fake technologies is crucial to ensure responsible development and deployment. These guidelines should focus on transparency, consent, accountability, and the protection of individual rights. Industry bodies and professional organizations can play a significant role in formulating and promoting these ethical standards.

CONCLUSION:

Regulating deepfakes in the Indian context requires a multi-pronged approach involving legal reforms, technological advancements, awareness campaigns, and international cooperation. While India's existing legal framework provides some recourse for addressing deep fakes, specific legislation, and dedicated regulatory measures are needed to effectively combat this growing threat. Various nations that already have implemented some kind of law or regulation for controlling the deep fakes can be studied in order to devise the law that suits India best. While regulating the possible bad effects of deepfakes, the good effects should not be ignored like the efficiency it can provide in schools and other educational institutions for providing language and how body language and lips movements work in different languages. Every new piece of technology has it's good and bad. It is like how a simple pair of scissors is a weapon for a person but on the other side, it is a necessary tool for a doctor to operate to save a life.

Similarly, endeavors are required to be made to embrace the good of the deep fakes while minimizing the bad. By implementing comprehensive regulations, promoting media literacy, and fostering collaboration among stakeholders, India can navigate the complex legal and ethical challenges posed by deepfakes, safeguarding individuals and society as a whole.