DOI: https://doij.org/10.10000/IJLSI.112215

INTERNATIONAL JOURNAL OF LEGAL SCIENCE AND INNOVATION

[ISSN 2581-9453]

Volume 6 | Issue 5

2024

The Ethics of Deepfakes: A Digital Age Crisis

AVADHESH PRATAP SINGH[1], MADHAV GOSWAMI[2] AND MUGDHA GARG[3]

ABSTRACT

Deepfake Technology has earned great attention because of its capability to deceive, manipulate and fabricate certain content like images, audio, video and much more. The term "deepfake" is a bifurcation of "deep learning", a subset of Artificial Intelligence (AI) and "fake" which denotes the synthetic or unreal nature of the content. With the use of this technology, audio and video media can be altered to give the impression that someone has said or done something they haven't. This technology is flourishing on social media which is harming children, women and other vulnerable users. This research explores the role of deepfake technology in propagating misinformation or false information throughout the web along with its potential results on public and social cohesion. Legal frameworks have also been discussed in this research on how recent legislation responds to this manipulation. This research also argues that the impact of deep fakes on society is extreme and versatile, necessitating a coordinated response from governments, tech companies, and civil society. By shedding light on these critical aspects, this research aims to contribute to a better understanding of the impact of deepfake technology on social media and to inform future efforts in detection, prevention, and policy development.

***Keywords**: Deepfake, Social Media, Misinformation, Artificial Intelligence, Technology.*

I. INTRODUCTION

Deepfake is a processed media operated by Artificial Intelligence (AI) technology. The Deepfake involves the image or video of an existing person or event, which in turn, is replaced with another person's likeness. Furthermore, there is an emerging want to dive deep into the world of developing or creating a robust mechanism for tackling them efficiently. The major issue associated with the deepfake is the inability of a normal person to distinguish between fake content and real content and this invites the problem of misleading case stories. With the beginning of every new day, there is an enhancement in the cases of mimicking the real people due to which there is a rapid advancement in the problem associated with identity crisis. The Deepfakes have been proved instrumental in leaving the threat upon the minds of people. The

[1] Author is a student at GLA University, Mathura, India.
[2] Author is a student at GLA University, Mathura, India.
[3] Author is a student at GLA University, Mathura, India.

one is not aware when he or she will be deceived. The contemporary swindlers would start rubbernecking as Lilliputian. Assume one bizarre precis that you're on a conference call but how to get assured that discerning of the person on the other side of the call is warrantable and original as claimed by him/her? Cyber fraudsters are most convergent with the use of this technology in order to steal the wealth of the people. The ransomware has been proven incremental in engendering the most advanced descriptions. The Business E-mail Compromise (BEC) has emerged as the most extravagant form of cyber-crimes nowadays. The increasing efforts of the government have made people more watchful or attentive for decreasing the rate of such inciteful crimes but despite the repeated efforts, the people still get caught in the complex net of cyber-crimes like phishing and spoofing in the more delicate circumstances. The Cyber offenders continuously make various attempts to use deepfake videos or audio as a net to catch their prey from the other shore in such a manner that it becomes difficult for the people to deny their requests. Many organizations make available the information of their senior leaders in the public domain. Now such information due to its availability in the public domain becomes more amenable to the possibilities of being misused in this prevailing era of deepfake in order to cheat the stakeholders and general public of the civil society. Moreover, phone calls are the cheapest and most accessible tool for fraudsters which helps them in fulfilling their desire to cheat people easily. The challenges pertaining to cyber-threat, and cyber-security in the present set of circumstances where the internet is a frequently used medium have posed a great challenge for the government and the general public to cope with. On the other hand, despite the guidelines and advisory issued by the FBI regarding the identification of deepfake videos, audio or images, deepfakes have been ruled out as a modern trajectory of cyber-crime.

(A) Research Objectives

(1) To identify the mechanism through which the deepfake content is created and circulated across the internet and social media.

(2) To analyze how deepfakes play a pivotal role in spreading fake information along with destabilizing the peace and harmony prevailing in society.

(3) To decode how the cyber-offenders use AI-driven deepfake technology for committing the cyber-crimes.

(4) To suggest some proactive measures that help in the detection of AI-driven deepfake content.

(B) Research Methodology

The researchers adopted the doctrinal research approach. The legal books, rulings from higher courts, media articles, statutes, e-journals, the Journal of Company Law, and legal websites have all been consulted by the researchers. Information has been gathered from books, reading information from numerous websites, and various online media. The Acts and/or laws are covered in the review content, and the case studies are briefly provided implying how they relate to important topics and will aid the reader in learning in-depth information about the topic.

II. CONTRIBUTION OF DEEPFAKES IN THE DISSEMINATION OF FALSE INFORMATION

The Term 'Deepfake' implies the usage of fundamental technology, namely, "deep learning", which is a fragment of Artificial Intelligence (AI). The Large data stations involve certain algorithmic problems which are solved by deep learning encryptions. The swap faces created by such designed algorithms are empowered and coordinated with Artificial Intelligence (AI).[4] The available information is converted into a desired video or digital content for making such fake media into a realistic set of manipulative information. Deepfake production involves the usage of various available techniques.[5] Moreover, employing the mechanism of deep neural networks containing autoencoders and a face-swapping method is one of the most common methods of deceiving a person and spreading unrealistic information over social media respectively. Under the given method, a target video is identified and selected which is used as the foundation for creating the deepfakes and some random clips are downloaded from the internet which is inserted in the selective time-frame of such target video. The nature of such collected video clips varies in the sense that they can be completely unrelated to the selected target video. It can be understood from an example, that a target can be a short video clip from a Bollywood movie, and the video of targeted prey inserted in the selected clip from a movie can be altogether different. Furthermore, autoencoders refer to the deep-learning AI program that examines the video clips to develop the structure of a person's face from varied angles and under different sets of environmental conditions like cold, hot, dry and aqua and further aligning the face of a person onto the one appearing in the target video by contriving some shared customary facets.[6] One of the most prevalent methods of creating deepfakes involves

[4] DeepFake, *available at:* https://en.wikipedia.org/wiki/Deepfake (last visited on September 18, 2024).

[5] Deepfakes- How they work and what it means for the future, *available at:* https://www.slideshare.net/slideshow/deepfakes-how-they-work-and-what-it-means-for-the-future/182914160 (last visited on September 18, 2024).

[6] **Ian Sample,** *What are deepfakes- and how can you spot them?*, **The Guardian** (Jan. 13, 2020),

the employment of the use of "General Adversarial Networks" (GANs), which is, conjoin to the project and play a crucial role in discovering the flaws in the deepfake media along with improving the same, resulting in increased efforts for the detectors to figure out the authenticity of such AI-generated fake content. Apart from this, the General Adversarial Networks (GANs) are the most popular technique for the construction of deepfakes involving the consistent discovery and improvement of the large quantum data to new prototypes, which in turn, also imitate the primaeval media with obligatory exertion of non-slew faultless outcome. Various software apps like Face Swap, Chinese App Zao, Deep Face Lab, Git Hub etc., help in making deepfakes for postulant learners easily. Git Hub, an open-source community engaged in developing such deepfake creation software has been found to hold the large quantum of Deepfake apps. Moreover, some of the above-mentioned apps are entirely used for the purpose of entertainment only. This purpose of using the deepfake apps also acts as a shield for deepfake creators from the restrictions imposed by constitutional law. Whereas, in reality, many of these apps are also used spitefully for disseminating fake information over social media. Many studies conducted on deepfakes establish that it is not the end of cyber-disasters but just the beginning. It is further predicted that AI-driven deepfakes may further pose a grave threat to the general public along with the stakeholders of civil society.

III. DEEPFAKE IN THE DIGITAL AGE: UNDERSTANDING EXISTING LEGAL FRAMEWORKS

In India, there is not a single piece of legislation drafted on the issue of Deepfake Technology or wrongdoings committed using AI. In regards to this, there is a need to acknowledge the increasing offences of deepfake which is severely affecting many people. Due to the escalating use of technology and the internet, making laws on deepfakes becomes crucial to address the risks and challenges caused by the increased technological advances. Deepfakes can also propagate false information that sparks political violence, panic attacks, or civil unrest. The proliferation of deepfake content might seriously jeopardise national security and public safety in the absence of legislative barriers. The necessity for strict rules to shield people from these kinds of hazards is highlighted by the rise in threats and misuse potential in areas like identity theft, character assassination, harm to one's image, reputation, and dependability, and the quick obsolescence of current technologies[7].

https://www.theguardian.com/technology/2020/jan/13/what-are-deepfakes-and-how-can-you-spot-them.

[7] Adv. Aishwarya, Hemant Hiray, *"Analysis of Deepfake Technology and Present Legislation in India to Tackle it"* 4 *International Journal of Advanced Research in Science, Communication and Technology*, 285, 285-288 (2024).

In the current scenario, there is neither a criminal nor civil law present in India that specifically talks about Deepfake. However, a review of existing laws and legislation could throw light on the prevalence of Deepfake and its related issues[8].

(A) Constitutional Provisions

An outright ban cannot be imposed upon Deepfake because Article 19(1)(a)[9] comes into the picture and protects one's freedom of speech and expression but it can be regulated if it infringes other legal rights. The 9-judge bench of the Apex Court held the Right to Privacy a fundamental right in its landmark judgment of *KS Puttaswamy v. Union of India* [(2017) 10 SCC 641][10]. As digital privacy is a subset of informational privacy, in the Indian context, using a subject's private information, like images or audio-visual snippets, in a deepfake video without that subject's agreement would be a violation of that subject's basic Right to Privacy.

(B) Provisions under the Information Technology Act, 2000

IT Act, 2000 is the first cyber law of India which has the provisions to regulate cybercrimes. However, due to the non-extensive nature of coverage of cybercrimes under the IT Act, of 2000, the Act alone cannot regulate deepfakes[11]. While Section 66E[12] of the IT Act, 2000 states that anyone who intentionally or knowingly captures, publishes, or transmits an image of a private area of another person without that person's consent under circumstances that violate that person's privacy shall be punished, Section 66D[13] of the IT Act, 2000 punishes cheating by personation using communication devices or computer resources[14].

If deepfakes are misused or applied improperly, they may be exploited as a means of committing offences against computers under the IT Act. The creation of a deepfake would be subject to the penalties outlined in Section 67 of the Act for the electronic publication or transmission of obscene information. According to Section 67A of the Act, publishing or transmitting any electronic material containing sexually explicit acts or conduct is punishable, therefore any Deepfake that includes such content will be subject to legal repercussions. Deepfakes featuring children are subject to Section 67B of the Act, which makes it illegal to publish or transmit any electronic material that shows children engaged in sexually explicit acts

[8] Aranya Nath, Sreelakshmi B., *"Deepfakes on Copyright Law- Inadequacy of Present Laws in Determining the Real Issues"* 15 *Indian Journal of Law and Justice*, 285-300 (2022).
[9] **INDIA CONST.** (Act No. 1 of 1950).
[10] KS Puttaswamy v. Union of India (2017) 10 SCC 641.
[11] *Supra* note 8.
[12] The Information Technology Act, 2000, No. 21, Acts of Parliament, 2000 (India).
[13] The Information Technology Act, 2000, No. 21, Acts of Parliament, 2000 (India).
[14] Ankit Burman, *"Challenges of Deepfake Technology, under the Indian Legal System"*, 10 The Lawway with Lawyers Journal (2024).

or conduct. If the deepfake content uses a person's unique identity feature—such as an electronic password—in a dishonest way, the creator of the deepfake will be held accountable for the offence under Section 66C of the IT Act, 2000. This includes taking on the identity of a foreign state or attempting to maintain public order. Section 66D of the Act also makes it illegal to use a computer to conduct fraud by impersonating someone else. Under Section 69A[15], the Central Government can order the intermediary to stop any such deepfake content if it thinks that doing so is essential to upholding India's national security, independence, and territorial integrity, as well as to promote friendly relations with other countries.

(C) Provisions under Bhartiya Nyaya Sanhita, 2023

Section 336[16] of Bharatiya Nyaya Sanhita defines forgery and Deepfake movies are typically counterfeited or replicated. Because of this, they may be considered forgeries and content created to harm someone's reputation or image intentionally is subject to a maximum three-year jail term and a penalty. Section 151[17] of Bharatiya, Nyaya Sanhita addresses deepfakes that incite enmity or disrespect for the government of India and are considered sedition.

If the deepfake content is a fake pornographic video that the deepfake creator disseminates, they may be prosecuted under Section 74 of BNS for sexual harassment and for insulting a woman's modesty. Section 294 of BNS states that it would be illegal to circulate an offending deepfake photo. Defamation is defined as publishing content on the internet to harm someone's reputation. This is a non-cognizable, bailable offence that can result in compounding under Section 356 of BNS. According to this section, the maximum sentence for this offence is two years in prison, a fine, or both. These laws are still in their infancy and are unable to handle the vast array of deepfakes that are now in use.

(D) Provisions under the Copyright Act, 1957

Deepfakes frequently include altered versions of movies or music videos with content that is shielded by copyright rules. According to Section 14[18] of the Copyright Act, 1957, the owner of a cinematographed music video or movie has the exclusive right to grant a license for the creation of any other copy of the film, including any picture or photograph of any image or sound embodying it. Furthermore, anyone found to have intentionally assisted in the infringement of a copyrighted work or any other rights granted to the copyright owner under the terms of the Act faces a maximum sentence of three years in prison and a fine of two lakh

[15] *Supra* note 13.
[16] The Bhartiya Nyaya Sanhita, 2023, No. 46, Acts of Parliament, 2023 (India).
[17] *Ibid.*
[18] The Copyright Act, 1957, No. 14, Acts of Parliament, 1957 (India).

rupees. In the case of movies, the producers have the risk of being targeted rather than the actors, therefore these remedies could not be helpful to someone who has fallen victim to deepfake content if the copyright in question does not belong to the person who is portrayed in the image. Therefore, the remedies permitted by this law could not be advantageous to the actual victim or the intended audience of the deepfake content.

IV. DEEPFAKE: A THREAT TO SOCIAL MEDIA INTEGRITY

Because deepfakes are so dramatic, they can quickly become viral, enthralling viewers and garnering a lot of attention. Deepfakes can propagate quickly on social media, making it difficult to control the transmission of misleading information in this fast-paced environment. It might be impossible to undo the harm caused because the deepfake may have already attracted a sizable audience even after it was refuted[19]. The emergence of deepfakes presents noteworthy obstacles to the veracity of data on social media platforms, safeguarding personal reputations, and upholding public confidence in digital content. A complex strategy that incorporates regulatory frameworks, public awareness campaigns, and technology innovation is needed to address these difficulties.

Deepfake algorithms can modify videos and images to make it appear as though the target person is talking or doing something they aren’t participating in, by smoothly swapping or superimposing faces. Using a vast number of source movies to train a deep neural network is one method for doing this. The target video or image may then be modified by the network using the learned facial features, emotions, and gestures[20]. Deepfake technology is used in an unethical and illegal manner that seriously harms women and children, two groups of people who are already vulnerable in society. Due to their easy access to social media and the internet, children these days are more active users of these platforms, but they still do not completely understand the potential negative effects of modern technology. Every day, there are real-life instances of kids utilizing the internet and operating systems without knowing what kind of content is appropriate for them. This renders kids vulnerable to child pornography, cyberbullying, and other issues.

A complicating factor in this whole problem is the widespread usage of social media and internet platforms for deepfake video and photo generation. The widespread spread of

[19] Samer Hussain Al-Khazraji, Hassan Hadi Saleh, Adil Ibrahim Khalid, Israa Adnan Mishkhal, *“Impact of Deepfake Technology on Social Media: Detection, Misinformation and Societal Implications”* 23 The Eurasia Proceedings of Science, Technology, Engineering & Mathematics,429, 429-441 (2023).

[20] Priyanka Kapoor, *“Study on the Impact of Artificial Intelligence Enabled Deepfake Technology*” 12 International Journal of Creative Research Thoughts, *71,* 71-101, (2024).

scandalous or harmful deepfake content is predicted to be facilitated by the quick and affordable distribution of images, audio, and video on social media and online platforms, as well as cognitive biases that encourage people to share novel, negative, or belief-confirming information[21]. Technology does not inherently cause gender discrimination; rather, poorly managed technology frequently reflects cultural biases and gender power dynamics. Women are disproportionately targeted for a variety of reasons, including objectification, misogyny, sexism, and gaslighting. The targeting of women begins with Photoshop-like tools and continues with deepfake technology. Its impacts are compounded by the fact that deepfake abuse disproportionately targets women[22].

India faces growing concerns over exploitation and misery from revenge porn and deepfake technologies. Retaliation porn involves sharing private images or videos without consent, with deepfake technology creating lifelike fake content. The lack of robust rules has hindered victims' ability to seek justice. Many people who have their privacy violated in such a blatant and degrading way may suffer from psychological distress, harassment, and social isolation. Serious issues, including “post-traumatic stress disorder, suicidal thoughts, depression, among other symptoms of poor mental health”, may arise for the victims of this type of abuse[23].

V. Societal implications of deepfakes

Deepfakes have both positive and negative impacts on society. It has been discovered that celebrities and politicians are the most common targets of deepfake creators due to the availability of an abundance of their free videos and images across the internet. Furthermore, due to the extensiveness and domination of social media in the contemporary world, ambassadors, fashioners, and ordinary people are increasingly becoming the prey of such deepfakes as well.[24] Deepfake always catches a potential target and also tries to get hold of the everyone handful on the internet leaving an enduring disgrace simultaneously. One of the most prevalent and approached forms of deepfake existing across the internet is revenge porn or deepfake porn, which excessively harms the modesty of a woman.[25] The study conducted by Deep Trace Labs in the year 2019 reveals that 96% of the deepfake videos available on the

[21] Dr. Zubair Ahmed Khan, Ms. Asma Rizvi, *“Deepfakes: A Challenge for Women Security and Privacy”* 5 CMR University Journal for Contemporary Legal Affairs, 203, 203-227, (2023).

[22] Dr. Sarigama R. Nair, *“The Emerging Threat: Deepfake and Women in India”* 12 International Journal of Creative Research Thoughts, 140-147, (2024).

[23] *Supra* note 21.

[24] Agarwal, S., Farid, H., Gu, Y., He, M., Nagano, K., & Li, H. *“Protecting world leaders against deep fakes*” 1, CVPR Workshop, 38-45 (2019).

[25] Ajder, H., Patrini, G., Cavalli, F. & Cullen, L. *“The state of deepfakes: landscape, threats, and impact”* Deeptrace (2019).

internet is a deepfake non-consensual porn.[26] Recent news revealing the circulation of deepfake porn of one of the renowned public figures, namely, Taylor Swift in January 2024 is a perfect example that confirms the results laid down by the study conducted by the Deep Trace Labs in the year 2019.[27] Deepfake porn refers to the semblance of cyber-bullying along with virtuous and seclusion issues, which in turn, leaves an ever-lasting traumatic impression on its prey including public and non-public figures. The Politicians and their political agendas are the most targeted prey of the deepfake creators. One can easily find numerous videos of politicians emanating to contend or execute the things that they didn't want to say or perform in reality. The video of former American President Barack Obama is one of the leading examples portraying how deepfakes of politicians are created in order to disturb the harmony prevailing in society. Undoubtedly, this increasing trend of availability of deepfakes over social media and other internet platforms is resulting in the enhanced spreading of fake information, which in turn, is also causing the crisis of originality over social media and the internet. The enhanced circulation of deepfake media on the Russia-Ukrainian war where the fake videos of both, the Ukrainian President, Volodymyr Zelensky, and Russian President, Vladimir Putin, revealing the usage of deepfake AI-driven technology for entertainment and satirical purposes around the crisis sets a very negative perception for the society.[28] The empiricist found the above-mentioned usage of Artificial Intelligence (AI) and Deepfake as the starting of cyber-disaster. The investigation conducted by the researchers concerning the increased usage of deepfake algorithms in such a manner found it as a successful attempt to destroy the image of politicians rather than any entertainment purpose. Another incidental issue connected with the emerging trend of deepfake is the spreading of misinformation by categorizing real media into a set of created deepfake content for hampering the peace and harmony prevailing in society. Deepfakes also aim to enhance the mechanism involved in carrying or executing scams efficiently. Phishing and business E-mail Compromises (BECs) are the major forms of virtual crimes that are carried out effectively with the help of these deepfakes only.[29] The propensity of deepfakes to mutate and recast the audio, or voice of trusted friends or a CEO is cast to ensure the efficacy of hazardous virtual crimes like cyber-bullying, virtual extortion, virtual sextortion, phishing, spoofing, etc. One of the pertinent scenarios involving the efficacious

[26] Britt, K. *"How are deepfakes dangerous?"* Nevadatoday (2023).

[27] Trepany, C. *"Taylor Swift ai pictures highlight the horrors of deepfake porn. Will we finally care?"* (2024).

[28] Twomey, J., Ching, D., Aylett, M. P., Quayle, M., Linehan, C., & Murphy, G., *"Do deepfake videos undermine our epistemic trust? A thematic analysis of tweets that discuss deepfakes in the Russian invasion of Ukraine"* 18 PloS One, e0291668–e0291668 (2023).

[29] Kevin Townsend, *"Deepfakes are a growing threat to cybersecurity and society: Europol*" Securityweek (2022).

usage of AI-driven deepfakes for committing the crime of phishing is 'voice-mimicking' with the help of AI software, which is, most commonly used by the thieves for aspiring the confidence and trust of their prey. Moreover, it is correctly said that like a coin every issue has two aspects, i.e., one is positive and the other is negative. It cannot be denied that this AI-driven deepfake technology only possesses negative attributes. It can also be used for various purposes leading to the betterment and advancement of society. The Deepfakes can be used to bring history to life.[30] The creation of educational simulations and videos that are pleasing and beneficial for the students is one of the crucial advancements that AI-driven deepfake technology can bring into society.[31] The tools that ensure reasoning with accuracy can lead to the development of personalized capacities, which in turn, can also develop the vision of India, i.e., "Vikshit Bharat".

VI. RESULTS AND FINDINGS

The Results and Findings in this paper have been made with regard to the detection of AI-driven deepfake content. The following pointers will help one to detect a deepfake content: -

1. Irregular Movement of Eye: The titling of eyes in a specific direction, not flickering or not professing contact with the camera lens or another person is a clear identification of a deepfake media.

2. Fabricated Movement of Lips: One of the important factors for detecting deepfakes is the unnatural or synthetic lip movement, i.e., regardless of the words spoken, the movements of the lips will be in motion even if the audio is not present in the video.

3. Abnormal Face-Expressions: The Deepfake video or media can be identified when there is no change in the facial expressions of the concerned person present in the video with respect to the spoken words or perceived by another person. In such a case, there is no change in the expression of a person present in the video even if there is some exciting or shocking news.

4. Cumbrous position of the face with regard to the other subjects: Shifting the face towards a vacuous position of the room or an angle that doesn't involve any article or recipient-in-focus.

5. Differences in Skin-Tones: It is quite common that when a prey is entangled with another person present in a target video for creating his or her deepfake, there appears to a patchy skin due to a mixture of two separate skins digitally.

[30] Don Philmlee, *"Practice innovations: Seeing is no longer believing – the rise of deepfakes"* Thomson Reuters (2023).

[31] Ashish Jaiman, *"Positive use cases of synthetic media (aka deepfakes)"* Towards Data Science (2020).

6. Difference in the angle formed by an overhead light: The shadow created by an overhead light will be dwarf in comparison to the one formed by any other angle of light reckoned on the body. Where the shadow remains similar, irrespective of change in the light then it's an unreal shadow.

7. Restrained Body: It doesn't matter who is or what is appearing on the screen, where similar emotions are not projected by the person on screen, then there is some flaw.

8. Lumber some posture of the body: Where a body is leaning in a particular angle or definite side throughout the time-frame of the video or there is an isolated position of the body in the entire video, then it's a deepfake content.

9. Contrived Hair-Looks: The digital mixing of two separate bodies also results in artificial hair which can be speckled easily as they do not have movement in alignment with the head.

10. Irregularity in the shape of teeth: The presence of a similar tooth structure in the mouth of every person (in case of 2 or more persons) during some live video discussion portrays deepfake.

VII. Recommendations

Considering the ramifications and difficulties presented by deepfake technology emphasizes how urgently this problem needs to be resolved. It asks for a multifaceted strategy that includes user education, ethical considerations, legal frameworks, technological improvements, and cooperative efforts to guarantee the responsible use of deepfake technology and safeguard the integrity of digital media. The results support the following recommendations for further study, the formulation of policy, and the development of technology:

1. Legislators must create thorough legal frameworks that deal with the production, dissemination, and nefarious application of deepfakes. This includes thinking about laws pertaining to intellectual property, consent, privacy rights, and the appropriate application of deepfake technology. People affected by deepfakes will have legal recourse and a deterrent in the form of clear and enforced legislation.

2. Education programs should be created to improve users' abilities in digital and media literacy. This involves instructing people on how to assess information critically, spot manipulation, and confirm the veracity of media content. Users who possess the requisite abilities can more effectively navigate the digital terrain and arrive at well-informed conclusions.

3. Encourage responsible behaviour and moral standards among those who develop and utilize

deepfake technology. Stress how crucial it is to get permission, uphold people's right to privacy, and only use deepfake technology for legal, non-malicious uses. Campaigns to raise public awareness can be quite effective in emphasizing the moral issues and proper application of deepfake technology.

4. Provide funds for the investigation and advancement of deepfake detection systems. Governments, tech businesses, and academic institutions can work together to develop and improve systems that detect deepfakes.

VIII. CONCLUSION

With the advancement of data science, high-speed networks, and artificial intelligence, deep learning emerged as a unique technique. Like any other technological advancement, these deepfakes have been put to illegal and immoral use. People’s freedom, national security, and the way an economy functions can all be affected by this deepfake technology. People need to be aware of these technologies, and big social media platform service providers ought to keep an eye on these kinds of activities[32]. Deepfakes technology requires a comprehensive set of rules and regulations to protect individual privacy. This technology may have detrimental effects on people’s lives in addition to its effect on data infringement. It's important to remember that it might make positive use of this technology. Users of this technology ought to think about the ethical and societal ramifications of their work. Everyone is aware that everything has both positive and bad effects. Working together, we can find more advantages to using this technology.

*****

[32] Aranya Nath, Sreelakshmi B., *“Deepfakes on Copyright Law- Inadequacy of Present Laws in Determining the Real Issues”* 15 Indian Journal of Law and Justice, 285-300 (2022).

IX. References

1. Adv. Aishwarya Hemant Hiray*, "Analysis of Deepfake Technology and Present Legislation in India to Tackle it"*, IJARSCT, 285-288 (2024).
2. Agarwal, S., Farid, H., Gu, Y., He, M., Nagano, K., & Li, H., *Protecting world leaders against deep fakes*. In CVPR workshops (1), 38 (2019).
3. Ajder, H., Patrini, G., Cavalli, F. & Cullen, L.,*The state of deepfakes: landscape, threats, and impact.* Deeptrace, (2019).
4. Ankit Burman, *"Challenges of Deepfake Technology, under the Indian Legal System"*, TLLJ (2024).
5. Aranya Nath, Sreelakshmi B., *"Deepfakes on Copyright Law- Inadequacy of Present Laws in Determining the Real Issues"*, IJLJ, 285-300 (2022).
6. Britt, K., *How are deepfakes dangerous?*, Nevadatoday.
7. *Deepfakes session into the state of deepfakes and how the technology highlights an exciting but dangerous future. https://www.slideshare.net/JarrodOverson/deepfakes-how-they-work-and-what-it-means-forthe-future*
8. Dr. Sarigama R. Nair, *"The Emerging Threat: Deepfake and Women in India"*, IJCRT, b140-b147, (2024).
9. Dr. Zubair Ahmed Khan, Ms. Asma Rizvi, *"Deepfakes: A Challenge for Women Security and Privacy"*, JCLA, 203-227, (2023).
10. *Information about the DeepFake which is an independent and non-proprietary content on,* Wikipedia. *https://en.wikipedia.org/wiki/Deepfake*
11. A. Jaiman, *Positive use cases of synthetic media (aka deepfakes), https://Towarddatascience.com*
12. D. Philmlee, *Practice innovations: Seeing is no longer believing – the rise of deepfakes. Thomson Reuters*, (2023).
13. Priyanka Kapoor, *"Study on the Impact of Artificial Intelligence Enabled Deepfake Technology"*, IJCRT, n71-n101, (2024).
14. Samer Hussain Al-Khazraji, Hassan Hadi Saleh, Adil Ibrahim Khalid, Israa Adnan Mishkhal, *"Impact of Deepfake Technology on Social Media: Detection, Misinformation and Societal Implications*, ISRES, 429-441, (2023).

15. *The GitHub repository for all DeepFake software, https://github.com/iperov/DeepFaceLab*

16. K. Townsend, *Deepfakes are a growing threat to cybersecurity and society: Europol,* Securityweek, (2022).

17. C. Trepany, *Taylor Swift ai pictures highlight the horrors of deepfake porn. Will we finally care?*, (2024).

18. Twomey, J., Ching, D., Aylett, M. P., Quayle, M., Linehan, C., & Murphy, G., *Do deepfake videos undermine our epistemic trust? A thematic analysis of tweets that discuss deepfakes in the Russian invasion of Ukraine,* PloS One, 18(10), e0291668–e0291668.

*****