INTERNATIONAL JOURNAL OF LEGAL STUDIES AND SOCIAL SCIENCES [IJLSSS]

ISSN: 2584-1513 (Online)

Volume 4 | Issue 1 [2026] | Page 364 – 372

DARK SIDE OF TECHNOLOGY: DEEPFAKES AND ARTIFICIAL INTELLIGENCE IMPACT ON WOMEN'S RIGHTS AND PRIVACY

- Parul[1]

ABSTRACT

The paper will look into the "dark" aspect of technology; more specifically deepfakes and Artificial Intelligence in relation to women's rights and privacy issues. There are existing AI technologies that encourage the creation and dissemination of deepfake videos and images among other contents, and this has come as a huge concern thanks especially to the very obscure use of such technology to scale insidious violence against women. The purpose of this paper is to examine the degree to which deepfakes are used to harass, malign, and infringe on the privacy of individuals all of which serve to compromise the dignity and autonomy of women. Such cases include the weaponization of deepfakes in non-consensual porn and impersonation crimes, demonstrating the physical and emotional tolls of these crimes on its targets. We also examine some institutional and regulatory concerns and ethics that have already arisen, in this case, to call attention to the necessity of legal protection as well as informational campaigns aimed at protecting women's rights in the internet era. Therefore, by focusing on the role of AI-based technology in gender violence, this paper seeks to address the issue of responsible technology development and individual privacy concerns.

KEYWORDS

Deepfakes, Artificial Intelligence, women's rights and privacy issues, institutional and regulatory concerns, legal protection, informational campaigns.

[1] 5th Year, B.A. LL.B. Student, DAV University, Jalandhar (Punjab)

INTRODUCTION

Deepfake technology involves transforming moving imagery, still imagery, and sounds using deep learning and sophisticated hardware. It is employed for the spread of fake news and perpetrating financial crimes as underhanded purposes, among other things. Nowadays, deepfake technology has been misemployed for a great variety of scams and hoaxes such as pornography with the likeness of famous people, as well as for the manipulation of elections, interception of social networks, fake news creation, impersonation of others for theft of finances and a host of other criminal activities. Deepfakes use Artificial Intelligence - which is advanced technology, deep learning specifically – to help create and modify visual and auditory images. These are large image, video and audio datasets that a young model active in this field is simply learning to correlate the unique patterns, traits and facial movements of certain people. After they have learned such aspects, the deepfake systems are able to create completely believable and realistic images. This brings up moral issues such as concern for privacy, fidelity between individuals and the information they communicate and the information itself. Such developments whereby media contents are easily altered or manufactured with the utmost accuracy and attention to detail are not without threats like misinformation, character assassination and swindling.[2]

Deepfakes are merged videos in which realist modification is done to make the subject look like he/she said or done something which he/she never did. Since cost and technology of developing deepfake AI-based techniques are improving and available to many, deepfakes have framed and continue to frame technological, policy and legal difficulties. It is alarming how deepfake technology can be exploited. Video manipulations are a significant concern during a political campaign as video alterations may depict opponents saying negative statements damaging the chances of the candidates for elections. Curbing 'deepfakes' involves issues such as the creation of synthetic media in which an individual appears in sexually explicit material even when she did not partake in the video shoot. Deepfakes can be said to distort reality, thanks to the womb-to-the-tomb integration of smart technologies, proliferation of information, and azimuth expectations on the visual data. Because they advance the fallacy of 'seeing is believing,' they tend to create imaginative realities that are hard to disassociate physically. And a more grounded observation – as the presence of deepfakes becomes more commonplace in society there is also a more dangerous reinforcement: that they make any video

[2] Drishti IAS " Perspective: Combating Deepfakes " Accessed 5 November 2024. https://www.drishtiias.com/loksabha-rajyasabha-discussions/perspective-combating-deepfakes

regardless of whether it is real or not highly mistrusted. Many Deepfake methods are researched and developed in the context of GANs-based motion and face swap techniques. Deepfakes are mostly targeted at public figures and celebrities. In order to circulate inappropriate false messages of different political leaders Deepfake technology has been utilized on many occasions and it may fuel political instability. It can also be used to distract service members through fake maps accuracy of which can lead to dangerous consequences. Not all aspects of this technology however are negative. Tones and voices once lost by people can be restored with this technology. As we are aware, fake news is easier to spread wide and far and the more difficult it becomes to limit its spread. In order to understand Deepfakes, one must go beyond the surface and ask questions pertaining to what Deepfakes are, Where, how and with what perhaps, when one speaks of creating them, and then of identifying them.[3] Deepfakes have a huge range of uses such as creating fake pornography of well-known celebrities, spreading fake news, creating fake voices of politicians, financial fraud, and many other forms of misuse. By using Artificial Intelligence, such images can be created that infringe the privacy of women and affect them mentally, sometimes leading to defamation.

OBJECTIVE

The primary objective of this research paper is as follows:

1. To analyse the current scenario of Artificial Intelligence impacting women's rights & privacy.
2. To review the ongoing efforts to detect and counter deepfakes.

METHODOLOGY

This research paper adopts a descriptive and analytical design to analyse and understand the impact of Deepfakes and Artificial Intelligence on women's rights and privacy concerns. This research is based on primary as well as secondary resources (by reviewing existing research papers). Sources used include articles, case studies, and online data resources.

LAWS SURROUNDING DEEPFAKES

There are some provisions in different laws to protect the women's rights and privacy from deepfakes. More specifically, it deals with deep machine learning and the generation of fake images, videos or

[3] Research gate "Deep Insights of Deepfake Technology: A Review". Accessed November 5, 2024. https://www.researchgate.net/publication/351300442_Deep_Insights_of_Deepfake_Technology_A_Review

even sounds. An AI capable of generating images and/or sounds of individuals can be constructed after a thorough exposure to many images and sounds. This technology has permissible applications in the film and education industries. However, this is a technology that is abused in most cases. First and foremost, the growth of deepfake technology has been accelerated by the development of user-friendly applications and better access to high-quality data. Social networking sites have been very encouraging for the growth of transformational content. Therefore, enhancing the scope and reach of enhancement.

INDIAN PENAL CODE, 1860

Sections 499–500 IPC – Defamation under IPC: Posting deepfakes that satirize or deepfakes that malign the reputation of an individual/organization tend to infringe Section 500 of the IPC, Defamation and the like. This clause punishes making any expression or reproduction of a person's words whether it is a positive or a defamatory context if a person intends that those words will be published with the object of harming that person's reputation. Offenders found guilty of the provision of the law under Section 500 may be incarcerated for not more than 2 years or pay a fine or both except for any other provision of this Act. A breach of this provision can result in imprisonment for a period not exceeding three years, a fine, or both. Section 67B – Prohibition of publication or transmission of obscene material in electronic form in the recommendations set out in Section 67B of the Information Technology Act, 2000 these types of deepfakes may fall under creation of injury and offences against public morality. Violent and sexual deepfakes that represent explicit sexual practices and graphic nudity are included under Section 67B. Anyone convicted under Section 67B may face as long as three years in jail, pay a fine or face both sanctions.[4]

THE INFORMATION TECHNOLOGY ACT, 2000

According to Section 66D of the IT Act, any person found guilty of cheating by impersonation and using electronic means shall be punished with a term of imprisonment extending up to three years or fine which may extend up to one hundred thousand rupees or both. Section 66E also identifies the offender as an individual who publishes, transmits or captures an image of any person's private part of his or her body and is punishable on the offence with a term of imprisonment for a period which may not exceed three years and a fine not more than two hundred thousand rupees. Section 67A also

4 Indian penal code, 1860 (Act 45 of 1860)

seeks to punish those published or transmitted sexually explicit contents in electronic form, where the convicted person is liable to an imprisonment term not exceeding five years or both with a fine which may reach up to ten lakh rupees. Section 67B punishes also the publication and transmission by electronic means of materials containing child pornography with the imprisonment not of more than five years and fine which could be ten lakh rupees. Other provisions which can be taken into account are Section 292 and Section 294 of the IT Act as they also speak about the punishment regarding the offence of obscenity. [5]

PERSONAL DATA PROTECTION (AMENDMENT) BILL 2024

The amendment bill creates a new additional obligation upon the data users or data controllers to alert the commissioner and the affected data subjects of the occurrence of personal data breaches. The phrase "personal data breach" is defined rather broadly in the amendment bill to capture any breach, loss, misuse, or unauthorized access of personal data. Under the bill, the word 'data user' will be reshuffled and be referred to as 'data controller'.

In simpler terms - Most of the time a data controller is also known as data processor, but present definition applies to persons only who directly determine, alone or in concurrence with other persons, the purposes and means of processing personal data excluding those persons who process personal data and are controlled by data controller's rules only. In this sense, if person is referred

in this Policy as 'data processor', it means individual or entity engaged in the processing of personal data on behalf of the data controller and receiving respective payment but does not perform any processing activity for his own needs.

It is essential to note that all data controllers are required to comply with the mandatory provisions of the Data Protection Act which require them to notify the Data Protection Commissioner without delay in the event they suspect or believe that personal data maintained by them has been subjected to systems security breach. 'Personal data breach' means breach of the personal data protection measures put in place damage to or loss of personal data, improper use of personal data and access to personal data without permission.[6]

5 Information Technology Act, 2000

6 Roedl.com , "Personal Data Protection (Amendment) Bill 2024 passes second reading in Parliament" Accessed 5 November 2024 https://www.roedl.com/insights/newsflash-asean/2024_03/malaysia-personal-data-protectionamendment-bill-2024-second-parliament-reading&ved

INDIAN PERSPECTIVE

Non-Consensual Deepfakes. However, in India, the threats of deepfake pornography have raised alarming alarms. In one of the cases which was reported in the early days of February 2020, individuals were allegedly able to create naked pictures of women through the use of deepfake technology, which were subsequently posted on the networks. The case, however, revealed that the digital world is not a safe space for women as such actions – and many others of this nature – are directed towards them.

PRIVACY VIOLATIONS

The Supreme Court of India in the case of Justice KS Puttaswamy (Retd) v Union of India upheld the right to privacy as a constitutionally guaranteed right in the country. The bill seeks to ascertain the safety of personal data of an individual, which is defined in the bill as any information which is related or can be traced to a living human being.

The bill places restrictions on the processing of data except for a lawful purpose. The impact of deepfakes further makes the issue of privacy an abstract one by ensuring that there are divisions in the public domain with the help of the media people's images to construct a narrative that is untrue. This however is inconceivable for many women as society tends to look down upon them
because of some social attributes. Most present-day laws cannot sufficiently guard against the increasing threat of deepfake technology. The issues of consent, defamation, and infringement of intellectual property rights stymie attempts at justice for the victims of the act. In India as well, the legal provisions concerning these aspects are most of the time very poor thereby leaving a large number of victims helpless.[7] Disinformation campaigns especially with the use of deepfakes can be carried out against women in public office as well as in public domains. This has a devastating effect not only on the persons implicated in such campaigns but even discourages women who are on the verge of rising into leadership positions.

TECHNOLOGICAL SOLUTIONS

Creating new tools for effective detection of deepfakes will serve to lessen the effect of deepfakes. For instance, to counter content-centric issues, Indian companies and research institutions are also

7 ORF, Observer research Foundation" Debating the ethics of deepfakes" Accessed 5 November 2024 https://www.orfonline.org/expert-speak/debating-the-ethics-of-deepfakes&ved

beginning to focus on the development of Artificial Intelligence-based technologies aimed at video content analysis. Active measures aimed at educating the public regarding the threats posed by deepfake technologies are of utmost importance. In India, for instance, CyberPeace India has mobilised to protect not only the legal rights of women but also sought to educate the masses on the adverse effects attributed to the deepfakes. Campaigns using real pictures of women from the public who have been harmed by deepfake technology are capable of invoking emotions that can hasten the process of solving such social vices.[8]

TYPES OF DEEPFAKES

A deepfake could be an image or even a sound. Images: Deepfakes demystified involve images created by advanced Artificial Intelligence and deep learning. Deepfakes as a term also includes the tissue grafting, manipulation and synthesis of images to produce convincing illusions. Videos: They succeed in faking any facial expressions and lip synchronization with the respective sounds. Also, this is done by transferring facial features of a subject to a video of another person. Voice Cloning and Audio Manipulation. In addition to visual manipulation, deepfakes can also alter audio content.[9]

The increasing prevalence of deepfake technology presents a threat to the rights and privacy of women within a contemporary information society.[10] Deepfakes pose significant dangers despite being largely legal, including Blackmail and reputational harm that put targets in legally compromising situations. Political misinformation such as nation states' threat actors using it for nefarious purposes. Election interference, such as creating fake videos of candidates. Indian celebrities including Rashmika Mandanna, Aamir Khan, Ranveer Singh, Sachin Tendulkar, and Virat Kohli have all been the subject of deepfakes.[11]

8 CyberPeace, "Understanding Deepfake Threats on Organizations" - Mr. Neeraj Soni. Accessed 5 November 2024 . https://www.cyberpeace.org/resources/blogs/understanding-deepfake-threats-on-organizations

9 Baeldung, " An Introduction to Deepfakes "Accessed 5 November 2024 Baeldung https://www.google.com/url?sa=t&source=web&rct=j&opi=89978449&url=https://www.baeldung.com/cs/deepfakes-ai

10 Tech target " What is deepfake technology? " Accessed 5 Nov 2024 https://www.techtarget.com/whatis/definition/deepfake&ved

11 The Hindu " Most Indians have come across deepfake content online and worry about cyberbullying: Report" Accessed 5 November 2024, https://www.thehindu.com/sci-tech/technology/most-indians-come-acrossdeepfake-content-online-worry-about-cyberbullying-report/article68119802.

CONCLUSION

The increasing prevalence of deepfake technology presents a threat to the rights and privacy of women within a contemporary information society. With the advancement and reduction of the cost of producing such technology, the negative applications of this technology appear to be growing explosively. This is especially true with regards to making fake pornographic films and spreading false information.

These attacks are often aimed at women, and as a result, women face serious psychological trauma, harm to personal image, and social backlash. The examples of elevated risk of abuse through deepfakes are dramatic and serve to highlight the adverse effects on individual victims as well as the dangerous risk of normalising such technology in today's society. Most of the countries, including India, existing laws – if any – do not suffice to deal with the challenges brought by deepfakes. The absence of particular legislations often leaves the victims with meagre options for redress. It is equally crucial to introduce legislative amendments that make the legal framework more responsive to the threats posed by deepfake technology.

As an example, in addition to the general provisions against cybercrimes in India, there is a need for specific penal code amendments to deal with the offence of making and distributing nonconsensual deepfakes. The solutions offered by the DPDPA are welcome, however there should be sections which deal solely with preventing deepfakes. There are also other approaches that are critically important in fakes' damaging effects at the society level. These include improvements in algorithms that make it possible to put a stop to the usage of altered materials. Such approaches would benefit from the participation of technological devisers, scholars, and right advocates so that such technologies would be developed in a way that they would work properly within a given society. In addition, it is essential to encourage the public on the risks posed by the deepfakes, thereby creating a better rather than a worse, society.

REFERENCE

1. Drishti IAS, "Perspective: Combating Deepfakes" Accessed 5 November 2024. https://www.drishtiias.com/loksabha-rajyasabha-discussions/perspective-combating-deepfakes.

2. ResearchGate "Deep Insights of Deepfake Technology: A Review". Accessed November 5, 2024. https://www.researchgate.net/publication/351300442_Deep_Insights_of_Deepfake_Technology_A _Review
3. Indian Penal Code, 1860 (Act 45 of 1860)
4. Information Technology Act, 2000
5. Roedl.com, "Personal Data Protection (Amendment) Bill 2024 passes second reading in Parliament". Accessed 5 November 2024 https://www.roedl.com/insights/newsflashasean/2024_03/malaysia-personal-data-protectionamendment-bill-2024-second-parliamentreading&ved
6. ORF, Observer research Foundation " Debating the ethics of deepfakes" Accessed 5 November 2024 https://www.orfonline.org/expert-speak/debating-the-ethics-of-deepfakes&ved
7. Cyberpeace "Understanding Deepfake Threats on Organizations" - Mr. Neeraj Soni. Accessed 5 November 2024 . https://www.cyberpeace.org/resources/blogs/understanding-deepfake-threatsonorganizations
8. 8.Baeldung " An Introduction to Deepfakes " Accessed 5 November 2024 Baeldung https://www.google.com/url?sa=t&source=web&rct=j&opi=89978449&url=https://www.baeldun g.com/cs/deepfakes-ai
9. Tech target " What is deepfake technology? " Accessed 5 Nov 2024 https://www.techtarget.com/whatis/definition/deepfake&ved
10. The Hindu " Most Indians have come across deepfake content online and worry about cyberbullying: Report" Accessed 5 November 2024, https://www.thehindu.com/sci-tech/technology/mostindianscome-across-deepfake-content-online-worry-about-cyberbullying-report/article68119802.