International Journal for Multidisciplinary Research (IJFMR)
E-ISSN: 2582-2160 ● Website: www.ijfmr.com ● Email: editor@ijfmr.com

Deepfake Technology in Social Media: Social and Legal Implications in India

Sidharth T[1], Guhan T[2]

[1,2]Student, Sastra University

ABSTRACT

Deepfake technology is a latest AI tool which is used for manipulation and fabrication of audio, video and images. This technology first appeared in 2017. It is the realistic swap of a person's face and voice with some other person. Social media has been the major platform for providing deepfake contents. The social media users are witnessing the effects of deepfake technology. Although there are few advantages it has been widely used for illegal purposes. It has been an emerging threat in the virtual world. It has the power to replace the original content with fake which looks real. Lots of misinformation has been spread due to deepfake. The deepfake content can manipulate public opinion. The public has begun to doubt on the originality of the content spread in the social media. The technology has done psychological damage to many people. It is considered to be illegal technology in many aspects and there are penal provisions relating to usage of deepfake. There are certain inconsistencies in the current Indian laws with regard to deepfake. The study aims at giving awareness about the dark side of deepfake technology in social media. The research will be based upon socio-legal effects of deepfake technology in India.

Keywords: Deepfake technology, Social media, Artificial Intelligence, Legislation, Extra territorial jurisdiction

1. INTRODUCTION

The social media has become a major tool for expressing the people's opinion. The content in it can influence the opinion of large numbers. So, there is high chance of fake news to be spread around social media. The advancement in technology has its positive and negative impacts. Deepfake technology is one the negative aspect which has arisen because of technological advancement. Deepfakes are manipulated or synthetic media often created using artificial intelligence techniques like deep learning, to alter or generate videos, audio recordings or image. It is an algorithm which produces realistic appearances. It can manipulate the person's appearance by swapping or merging that person's face and voice with some other person. There are lot of misinformation began to spread because of deepfake. The users are getting confused with originality of the content. Social media is only a tool for spreading the deepfake content throughout the world.

The research focuses on socio-legal consequences that deepfake technology has created in India. The major social media platforms include WhatsApp, Instagram, Facebook, Telegram, Snapchat etc. it has been observed that around 75% of Indian social media users have viewed some deepfake content in a year. The psychological damage that deepfake has created on individuals is huge. The women are the majority victims of deepfake content. Several deepfake content is subjected to punishment under the Indian law. The societal problems which the deepfake has created is connected with law. The law is for

betterment of society. Various acts were formed to eradicate the social evils from society. Deepfake cannot be said to be a social evil. It can be used for good purpose. It is those who treat the deepfake in absurd way. The legalconsequences should arise only in cases of using deepfake for illegal purposes,

The social consequences and legal consequences are linked together. Whenever a negative social impact happens the legal consequences also emerges. The same applies in this research paper. The paper focuses on detailed analysis on social and legal consequences of deepfake onsocial media in India.

Types of deepfake technology

Face Swapping: In this kind of deepfake, a person's face is substituted for another in video footage to give the impression that the subject is saying or acting in ways that they never would have. To produce a realistic replacement of one face with another, (GANs[1]) or autoencoders are typically used.

Lip-Sync Deepfakes: This kind of deepfake aims to mimic the sound of someone uttering things they have never said by timing their lip movements with an audio recording. It makes use of AI to create lip motions that correspond with audio input by analysing and modifying facial landmarks.

Cloning Voices: The goal of this kind of deepfake is to mimic a person's voice. AI can create fresh audio that sounds like the original speaker by learning the traits of a human voice.

[1] Generative Adversarial Network: It is a well-known framework for approaching generative artificial intelligence and a type of machine learning frameworks.

Technique: Produces lifelike synthetic speech by using machine learning models like WaveNet[2] or Tacotron[3].

Full-Body Deepfakes: These deepfakes imitate the full body in addition to faces and voices. They use body language, gestures, and posture to give the impression that someone is doing things they are not.To manipulate full human bodies in videos, this technique often integrates a number of AI systems, such as GANs, motion capture data, and position estimation models.

Text-to-Video Generation: Videos produced by AI that are prompted or described in text. With the use of this technology, scenes, characters, or even real humans performing out text described scenarios can be produced as videos. It creates brief video clips from text descriptions by combining video GANs with models like DALL-E[4] or VQ-VAE[5].

Audio Deepfakes: Their main objective is to alter pre-existing audio tracks. AI can adjust the pitch, tone, or content of speech, creating a synthetic audio clip that seems authentic but is actually created. Based on sample inputs, these technologies can produce or change speech by utilizing models such as WaveNet or Lyrebird[6].

Content Removal Through Inpainting: Removing or changing items within pictures or videos is the main goal of inpainting; it's frequently used to conceal elements from media or realistically fill in any gaps in information. Using surrounding content as a guide, GAN-based models, also known as autoencoders, are trained to anticipate and restore visual gaps.

Puppet Mastering (Motion Transfer): In essence, this kind of deepfake copies the facial or physical movements of one person to another, transforming the original victim into a "puppet." The target performer's movements are projected onto them, giving the impression that they are carrying out the identical actions. It is attained by combining deep learning, pose estimation, and computer vision algorithms.

Computerized Avatars: AI is able to generate fully digital avatars that mimic both fictitious and real-life individuals. You can use these avatars for virtual reality applications, games, and entertainment. To generate avatars that closely resemble human appearance and movement, a combination of motion

capture, deep learning, and computer graphics is employed.

Style transfer: It is the process of "repainting" a scene while preserving its structural integrity by modifying the visual aesthetic of an image or video to resemble the work of another artist or medium. It uses convolutional neural networks[7] (CNNs) and deep learning frameworks such as Neural Style Transfer are frequently used to accomplish style transfer.

[2] raw audio waves in a deep generative model. It can replicate any human voice and produce speech that sounds more natural than the most advanced text-to-speech systems now in use, closing the performance gap with humans by more than 50%.

[3]This is an end-to-end generative text-to-speech model that generates the appropriate spectrogram from an inputcharacter sequence.

[4]OpenAI's text-to-image models that combine deep learning techniques with natural language descriptions toproduce digital images.

[5]It's a kind of variational autoencoder that creates a discrete latent representation by vector quantization.

[6]It is a section of Descript dedicated to AI research, creating a new line of media editing and synthesis tools thatfacilitate more expressive and approachable content creation.

[7]Convolutional neural networks perform tasks such as object recognition and picture classification using three-dimensional input.

Societal issues created by deepfake in India

Deepfake videos can be used to fabricate speeches or declarations from political figures, which can influence public opinion or undermine opponents' legitimacy. Such manipulation has the potential to undermine democratic processes in a nation where elections frequently involve several parties and regional divides. One of the most obvious ways that deepfakes might negatively impact society is by tarnishing people's reputations. This is especially important when it comes to non-consensual deepfake pornography or recordings meant to discredit well- known people or regular people. Deepfake victims may endure excruciating psychological, emotional, and social suffering. India is especially susceptible to deepfakes intended to provoke violence between religious or ethnic groups because of its high levels of communal conflict. With the proliferation of fake news on platforms like WhatsApp, which has already been used to encourage violence in India, false videos depicting one community attacking or disparaging another might spread quickly. Sexually explicit deepfakes are frequently directed at women in public positions (journalists, politicians, activists), with the intention of silencing them or harming their reputation. This makes gender disparity worse and keeps women from fully engaging in public life. Deepfakes have the potential to seriously damage journalism by eroding the authority of audio and visual materials. Journalists run the danger of publishing or disseminating false material because they can find it difficult to distinguish between authentic and fraudulent recordings. The credibility of news organizations may be weakened by this. So these are the major societal issues caused by deepfake technology in India

1.1 BACKGROUND OF STUDY

Deepfake technology has quickly become a major problem in the social media space. It uses artificial intelligence (AI) to produce fake yet incredibly realistic audio and video content. With more than 500 million internet users and a fast-expanding digital population in India, deepfakes provide serious problems

for online abuse, misinformation, and disinformation. The situation had been made worse by the extensive use of social media sites like Facebook, YouTube, and WhatsApp, where deepfake content can spread quickly and influence public opinion, especially in a nation where there are strong communal and socio-political differences. By falsifying the words or deeds of public personalities, deepfakes can influence political discourse, sway elections, and incite civil unrest, eroding confidence in reliable news sources. Furthermore, non-consensual deepfake pornography exposes women and other vulnerable groups to increased risks of exploitation, aggravating already-existing problems with cyberbullying and harassment. Though the Indian Penal Code and Information Technology Act cover certain ground, there are currently no explicit regulations in India that specifically target deepfakes, despite these mounting concerns. To handle the complex ramifications of deepfake technology on social media, broad legislative changes and strong regulatory frameworks are urgently required.

1.2 LITERATURE REVIEW

The research paper by ***Ishan Chaudhari and Bhargavi D. Hemmige (2024) Deepfake: An emerging threat in the digital media manipulation***[8] investigates the social ramifications of deepfake, including how they could influence public opinion harm people's reputation and spread false information. ***Anuragini Shirish and Shobhana Komal (2024) A socio-legal enquiry on deepfakes***[9] explores how deviant actors' misuse of deepfakes lead to cascading social ramifications at various institutional levels. ***Mika Westerlund (2019) The emergence of deepfake technology***[10] provides a comprehensive review of deepfakes and provide cybersecurity and AI entrepreneurs with business opportunities in fighting against media forgeries and fake news. ***Mustafa Kaan, Tuysuz and Ahmet Kilic (2023) Analyzing the legal and ethical consideration of deepfake technology***[11] explores on legal and ethical considerations of deepfake technology with an emphasis on understanding its social impact, regulatory challenges and the ethical dilemmas it presents. ***William Borgen and Mohamed Abdul Hussein (2023) Social Media's take on Deepfakes: Ethical concerns in the public disclosure***[12] revealed how principles such as dignity, transparency, privacy and non- maleficence might be diverged in deepfake application. ***Stamatis Karnouskos (2020) Artificial intelligence in digital media: The Era of Deepfakes***[13] reveals that a combination of technology, education, training and governance are urgently needed in tackling the misuse of deepfake technology.

2. MAIN BODY OF RESEARCH

2.1 RESEARCH OBJECTIVES

- To find out the socio-legal aspects of use of deepfake in social media in India
- To understand the requirement for regulating deepfake technology in India

2.2 RESEARCH HYPOTHESIS

- If existing Indian laws are applied to deepfake cases, then they will be found insufficient to address the complexities of deepfake technology and thus not solve societal issues.
- Societal issues tend to arise due to inadequacy of laws.

[8] Chaudhuri, Ishan, and Bhargavi D. Hemmige. "DEEP FAKE: AN EMERGING THREAT IN THE DIGITAL MEDIA MANIPULATION." *Sampreshan, ISSN: 2347-2979 UGC CARE Group 1* 17.2 (2024): 833-861.

[9] Shirish, Anuragini, and Shobana Komal. "A socio-legal enquiry on deepfakes." *California Western International Law Journal* 54.2 (2024).
[10] Westerlund, Mika. "The emergence of deepfake technology: A review. Technology Innovation ManagementReview, 9 (11), 39–52." (2019).
[11] Tuysuz, Mustafa Kaan, and Ahmet Kılıç. "Analyzing the Legal and Ethical Considerations of DeepfakeTechnology." *Interdisciplinary Studies in Society, Law, and Politics* 2.2 (2023): 4-10.
[12] Abdul Hussein, Mohamed, and William Bogren. "Social Media's Take on Deepfakes: Ethical Concerns in thePublic Discourse." (2023).
[13] Karnouskos, Stamatis. "Artificial intelligence in digital media: The era of deepfakes." *IEEE Transactions onTechnology and Society* 1.3 (2020): 138-147.

2.3 STATEMENT OF RESEARCH PROBLEM

There have been procedural lacunae in Indian laws concerning jurisdictional matters related to deepfake technology. Current Indian laws inadequately address the complexities of deepfakes, resulting in increasing harm to society.

2.4 RESEARCH QUESTIONS

- Whether extra territorial jurisdiction apply to harmful foreign deepfake content shared on social media in India?
- Whether specific legislation is required to regulate deepfake technology in order to prevent societal harm?

2.5 RESEARCH METHODOLOGY

The study is conducted using qualitative method of research. The researchers decide to go for analyzing the research works, articles related to deepfake technology to get the solution for the following research questions.

2.6 FINDINGS

Current Indian laws that are related to deepfake technology

Information Technology Act 2000

- Section 66E of IT Act is applicable in case of deepfake offences which states *whoever, intentionally or knowingly captures, publishes or transmits the image of a private area of any person without his or her consent, under circumstances violating the privacy of that person, shall be punished with imprisonment which may extend to three years or with fine not exceeding two lakh rupees, or with both.*
- Section 66D is also applicable in this offence which states *whoever, by means of any communication device or computer resource cheats by personation, shall be punished with imprisonment of either description for a term which may extend to three years and shall also be liable to fine which may extend to one lakh rupees.*
- Section 66E: The use of someone's likeness in a deepfake without their authorization is prohibited. This could include taking, publishing, or transmitting private pictures without permission.
- Section 67: Addresses the electronic publication or transmission of pornographic material. This clause might come into play if a deepfake contains sexually explicit material.

- Publishing materials that include sexually explicit behaviours is specifically targeted by Section 67A. This includes content that has been digitally altered, such as pornographic deepfakes.

Indian Penal Code

- Section 499 of Indian Penal Code states about Defamation. The definition states *Whoever, by words either spoken or intended to be read, or by signs or by visible representations, makes or publishes any imputation concerning any person intending to harm, or knowing or having reason to believe that such imputation will harm, the reputation of such person, is said, except in the cases hereinafter excepted, to defame that person.* The deepfake content has a high chance of affecting the reputation of an Individual. So, the individual can file a suit for defamation.
- Section 500 of Indian Penal Code states punishment for defamation *Whoever defames another shall be punished with simple imprisonment for a term which may extend to two years, or with fine, or with both.*
- If a deepfake is used to harass or threaten someone, Section 507 (Criminal Intimidation)may be used.
- Section 354C (Voyeurism): Covers situations in which a deepfake uses a woman's image for voyeuristic or sexually exploitative purposes without her agreement.
- Pornographic deepfakes may be considered offensive content under Section 292 (Obscenity).

Bharatiya Nyaya Sanhita (Replacement act of Indian Penal Code)

- Section 356 – Defamation
- Section 77 – Voyeurism
- Section 351 – Criminal Intimidation
- Section 294 and 295 – Obscenity

Constitutional Rights

In a seminal ruling in the 2017 case of Justice K.S. Puttaswamy (Retd.) v. Union of India[14], the Indian Supreme Court upheld the right to privacy as a basic freedom guaranteed by Article 21[15] of the Indian Constitution. On this basis, non-consensual deepfakes that infringe upon someone's privacy could be contested.

Data Protection Laws

Although India is still developing a comprehensive data protection law (which is presently taking the shape of the Digital Personal Data Protection Act, 2023), provisions pertaining to the misuse of personal data may be pertinent in addressing the problems caused by deepfakes, especially when they exploit a person's identity or likeness without authorization.

[14] AIR 2018 SC (SUPP) 1841, 2019 (1) SCC 1, (2018) 12 SCALE 1, (2018) 4 CURCC 1, (2018) 255 DLT 1,
2018 (4) KCCR SN 331 (SC), AIRONLINE 2018 SC 237

[15] Article 21 of the Indian Constitution guarantees right to life and personal liberty

Countries regulating deepfake content in social media

United States

The 2019 Deepfake Report Act[16]: The Department of Homeland Security is required by U.S. federal law to submit yearly reports on the usage of deepfakes and their potential harm to national security. This is a start in the direction of more federal control over deepfake technology.

National Defense Authorization Act (2021)[17]: According to this act's requirements, the US government must create instruments to identify deepfakes and deal with their usage in misinformation operations, particularly when it comes to national security. For the next five years, the Department of Homeland

Security (DHS) will publish an annual report on deepfakes. The report ought to address every possible negative impact that technology could have, from fraud to targeted population harm to foreign influence campaigns.

United Kingdom

Online Safety Act[18]: The act seeks to establish a legislative framework for the regulation of harmful online content, such as deepfakes. It requires tech businesses to take action in order to stop the spread of illicit content, like harmful deepfakes or revenge porn. The measure includes mechanisms for holding platforms accountable if they fail to remove damaging content in a timely manner.

Australia

Australia approved the **Criminal Code Amendment (Intimate Images) Act 2019** which makes it illegal to share intimate photos including deepfakes without consent. Sharing fake or modified media that shows someone in a private setting without that person's permission is illegal under this law.

South Korea

The "Act on the Promotion of Information and Communications Network Utilization and Information Protection[19]" addresses dangerous deepfake content that violates privacy, among other things.

[16] The Act was passed by the Senate on October 24, 2019, by unanimous consent

[17] The Act ensures that American soldiers have the resources, training, and equipment necessary to fulfill their duties by authorizing budget levels and providing authority for the U.S. military and other important defense goals.

[18] The Act came into force on 2023 which controls media and online speech in order to safeguard users especially children from harm.

[19] The Act protects the personal information of those using information and communications services, facilitating the use of these networks, and creating an environment that encourages safer and healthier use ofthese networks, the Act seeks to improve the lives of citizens and advance public welfare.

Case studies on deepfake technology in India

- The Indian actress Rashmika Mandanna’s deepfake video has been circulated on social media which created concerns relating harmful effects of deepfake technology.
- The accused released the deepfake video of Mr. Shah with the malicious aim to defame the Union Minister. It was prepared, published, and extensively circulated online.
- A deepfake video of actor Ranveer Singh has been circulated on social media. The audio was changed using deepfake technology and in the deepfake video he was seen criticising the Indian Prime Minister Narendra Modi for over unemployment and inflation.

Extra territorial jurisdiction challenges relating to deepfake technology in India

1. Deepfakes' Cross-Border Nature

Deepfakes frequently feature actors and platforms that function internationally. For instance, Indian people or entities may be impacted by a deepfake that was made in another nation and posted on a site that is hosted elsewhere. Attempting to prosecute anyone who produce or distribute deepfakes outside of India's borders presents jurisdictional issues. Absence of a formal agreement (such as an extradition treaty) between the nations concerned, Indian laws may not be able to bring charges against offenders who live abroad.

2. Conflict of laws

Different Legal Definitions: Laws pertaining to cybercrime, intellectual property, privacy, freedom of expression, and defamation differ throughout nations. It is possible that deepfakes that are prohibited in India may not be in other nations. For example, a deepfake that breaches privacy regulations or is defamatory in India may not be illegal in countries like the US that have more robust safeguards for free speech. There are many countries without legislation specifically addressing deepfakes, and there are many different ways that deepfake content is handled. When it comes to seeking justice for transnational crimes, this contradiction complicates the legal landscape because it may make it more difficult for India to bring legal action against producers or distributors of deepfake content in nations where proper regulations are inplace.

3. Anonymous and Pseudonymous Actors

Deepfakes can be produced and disseminated anonymously or under fictitious names, making it challenging for Indian law enforcement to find and apprehend those responsible. Jurisdictional claims are complicated by the fact that a large number of harmful deepfakes are created using encryption or through sites that safeguard user anonymity.

4. Data Sovereignty and Geolocation

Data sovereignty concerns are brought up by India's authority over content hosted outside of its borders. It may be difficult for Indian authorities to gain access to data about the production, dissemination, and impact of deepfakes if it is kept in foreign datacentres.

5. Jurisdiction over Platforms and Content Moderation

Different countries have varying legal standards when it comes to privacy, free speech, and digital content. While India may consider a certain deepfake illegal, other countries may treat it as protected speech under their laws. Many global networks, including as Facebook, YouTube, and TikTok, have country-specific restrictions while being popular places for the dissemination of deepfakes. Indian authorities frequently struggle with their limited authority over these organizations, which may have differing legal duties in their home countries, when dangerous deepfakes are posted on these platforms.

6. Cybercrime and Territoriality

Indian cybercrime laws, like the IT Act, are territorial in nature, meaning they mainly cover crimes committed inside India's borders. Because the internet is worldwide, it is possible for someone who is responsible for a deepfake to be located in another nation,making enforcement more difficult.

Reasons for absence of specific legislations regulating deepfake technology in India

- New and Developing Technology: Artificial intelligence (AI) and machine learning advancements have played a major role in the rapid development of deepfake technology in recent years. It's challenging for legislators to keep up with this transformation given its rapid pace. Technology might have advanced by the time a legislation is drafted and passed, making it possibly out of date.
- Unexpected Risks: Deepfakes and other AI-driven technologies were not as well- known or prominent when legislation like the Information Technology Act of 2000 were first drafted. As a result, there are regulatory gaps as lawmakers were blind to thedangers posed by deepfakes.
- Protection of Free Speech: Under Article 19(1)(a)[20] of the Indian Constitution, there is a possibility that regulations tailored specifically to deepfakes will violate people's right to free speech and expression. Legislators need to find a middle ground between preserving legitimate applications of AI, like satire, parody, and art, and preventing dangerous uses of deepfake technology. This

difficulty makes lawmakers wary about writing specific rules that can inadvertently impede free speech or creative expression.

- Slow Legislative Process: In India, new laws are frequently considered, created, and passed over the course of years. To mitigate the immediate harms produced by deepfakes, legislators may find it more convenient to depend on current laws in the interim rather than going through the drawn-out process of creating and passing new legislation.

[20] Article (19)(a) of the Indian constitution guarantees freedom of speech and expression to the citizens.

- Prioritization of Other Issues: The Digital Personal Data Protection Bill[21] and IT Act revisions are two examples of the larger regulatory reforms in the digital and data protection domain that the Indian government is now concentrating on. Regulations unique to deepfakes might be viewed as less important than these more significant changes.
- Limited Legal Precedent: Due to the relatively recent advent of deepfakes, Indian courts have not yet addressed many of the particular issues raised by this technology. In the absence of a substantial corpus of court cases pertaining to deepfakes, legislators might be reluctant to propose particular legislation. Rather, they might postpone creating new legislation until after additional court advice and precedents have been established.
- Public and Policymaker Awareness: Although the public is becoming more aware of deepfakes, politicians may not yet be fully on board. It's possible that awareness of the entire range of possible consequences from political influence to injury to one's reputation isn't yet sufficiently common to motivate the development of deepfake- specific legislation.
- Fear of Over regulatory: Like many other nations, India is eager to foster innovation in artificial intelligence (AI) and digital technology. Overregulation may hinder innovation in the AI industry, especially if strict rules are implemented that target deepfakes explicitly. Legislators are probably attempting to strike a compromise between the necessity for regulation and the goal of creating an atmosphere that will allow AI technologies, especially those that are used for good (like deepfake technologyin entertainment or education), to flourish.

2.7 DISCUSSION AND ANALYSIS

As per the findings the legal provision related to extra territorial jurisdiction has certain limitations. Section 75[22] extends the jurisdiction of the IT Act beyond the territory of India. It states that the Act applies to any offense or contravention committed outside India if the act involves a computer, computer system, or computer network located in India. Even though Section 75 grants extraterritorial jurisdiction, it is nevertheless very difficult to apply Indian laws against foreign persons or organizations. The Indian judicial system is unable to implement its decisions abroad absent a cooperating mechanism, such as an extradition or mutual legal assistance treaty, even though the Act asserts authority over acts committed outside of India. These methods are generally sluggish, cumbersome, and may not guarantee compliance. The operationalization of this extraterritorial jurisdiction is not clearly outlined in Section 75, particularly when foreign actors or platforms are engaged. For instance, it is unclear what legal action Indian law enforcement should take in order to punish the perpetrator of a deepfake that originates abroad and affects a person in India, or to ensure that the damaging content is removed from platforms that are located abroad. Section 75's efficacy is predominantly contingent upon the presence of bilateral or multilateral accords with other nations. In the absence of such agreements, the alternatives available to Indian courts and law

[21] The bill applies to processing of digital personal data within India within and outside India.
[22] Section 75 of Information and technology Act states act to apply for offence or contravention committedoutside India by any person irrespective of his nationality.
enforcement authorities to compel foreign entities to obey Indian court orders are restricted. Many international internet companies and service providers follow the laws of their own nations, frequently putting their own legal requirements ahead of Indian legal requirements. Companies like Facebook, Google, or Twitter, for instance, might not abide by Indian takedown orders or data demands if doing so would violate the laws of their home countries (such as the First Amendment[23] protections in the United States). Crimes pertaining to Indian computer networks or systems fall under Section 75. But as cloud computing has grown, data is now frequently dispersed across servers located in several jurisdictions, making it challenging to decide whether the IT Act applies in a given situation. This complicates the jurisdictional framework, especially for transnational crimes like deepfakes and other cybercrimes.
The deepfake technology is becoming a bigger threat in current society. There are laws which gives punishment for producing deepfake content. But the current laws do not deeply analyse the complexities of deepfake technology. They address the consequences of deepfakes (like fraud, defamation, or obscenity) but fail to comprehensively regulate their creation, detection, or dissemination. There is currently no legal framework that defines or differentiates between safe and dangerous applications of deepfake technology. The technological aspect of how deepfakes are made utilizing AI and machine learning (ML) is not addressed by any regulation. As per the findings, it has to interpreted that there requires a need for specific laws for regulating deepfake as it can has the huge potential to create havoc in society.

3. CONCLUSION

The research brings out the legal gap that are existing in current Indian laws which are not able to solve the complexities of problems that deepfake technology creates in social media. The social issues continue to be existed because of inadequacy of laws in regulating the deepfake technology. Deepfake technology is an upcoming threat which can cause harmful effects on society. Several countries have legislations regulating deepfakes. Although there are provisions in Indian law for individual harm done by deepfake, there are certain areas in which Indian judiciary and administrators find difficulty in implementing Indian laws such as when it comes to extra territorial matters. The research paper was able to find out the extra territorial jurisdictional problems related to deepfake technology and the reasons for absence of specificlaws regulating deepfake in India.
[23]Congress cannot pass legislation restricting the free exercise of religion or establishing an establishment of religion. It safeguards the rights to assembly, free speech, and the press as well as the ability to petition the government for a remedy to a grievance.

4. RECOMMENDATION AND FUTURE DIRECTIONS

The recommendation to be given with regard to extra territorial jurisdictional problems of regulating deepfake are:
International agreements and treaties: In order to combat cross-border deepfake crimes, India should endeavour to negotiate bilateral or multilateral conventions with other countries. Through these treaties, nations would be able to work together more easily to identify, look into, and prosecute those responsible for producing or disseminating dangerous deepfake content.

Mutual Legal Assistance Treaties (MLATs)[24]: MLATs are essential for international law enforcement cooperation. However, diplomatic links and the other nation's willingness to assist in the investigation of deepfakes are prerequisites for the efficacy of such treaties.

Harmonization of Laws: Cooperation among nations to unify legal frameworks pertaining to cybercrimes, such as deepfakes, may contribute to a more cohesive legal system. By ensuring that comparable legal requirements and penalties are applied in various nations, this could facilitate the resolution of deepfake issues across jurisdictions.

Extending Extradition for Cybercrimes: India has the ability to bargain for the inclusion of charges connected to deepfakes in current and upcoming extradition accords. This would allow India to ask for the extradition of anyone who produce or disseminate harmful deepfake content from the countries in which they now reside, given that the offense is considered illegal in bothnations.

Cyber diplomacy and agreements: To promote global cooperation on matters such as deepfakes, India might take a proactive approach to cyber diplomacy. This would entail advocating for international frameworks to address digital harms, taking part in global discussions on cyber governance, and establishing standards for appropriate conduct in cyberspace.

International Cybersecurity Alliances: India may participate in or form international cybersecurity alliances aimed at reducing cyberthreats, such as deepfakes. These partnerships may contribute to the development of frameworks for cross-border information exchange, capacity building, and cooperative enforcement measures.

Cross-Border Data Sharing Agreements: In order to improve the tracking of digital assets used in the production and distribution of deepfakes, India could strike up data-sharing agreements with other countries. To identify and convict perpetrators, this would include exchanging IP addresses, server locations, and other digital identifiers.

Cybercrime Units and Hotlines: To monitor and stop the spread of deepfakes, India can set up specialized cybercrime units and hotlines that collaborate with the cybercrime divisions of

[24]Mutual legal assistance treaty is an agreement between two or more countries for the purpose of gathering and exchanging information in an effort to enforce public or criminal laws other countries. These units could work together to share information on deepfake producers and remove dangerous content hosted on servers situated in different jurisdictions.

Improving Local Capabilities: It's critical to improve Indian law enforcement's technological capacity to look into and deal with deepfakes, particularly when foreign actors are involved. This can entail collaborating with foreign law enforcement agencies, teaching law enforcement professionals in digital traceability and cyber forensics, and more.

Cybercrime Courts: Setting up specialist cybercrime courts in India with the capacity to manage intricate cases involving transnational cybercrimes such as deepfakes can guarantee expedited legal processes and coordinated actions with foreign organizations.

Observing and Drawing from International Legal Cases: India may refer to international legal cases wherein nations have brought criminal charges against persons involved in cross- border deepfake-related offenses. These precedents can influence India's strategy and motivate foreign tribunals to give jurisdictional disputes involving cross-border cybercrime cases significant consideration.

UN Involvement in Cyber Governance: By pushing for global agreements or resolutions, India can use the UN[25] to address the cross-border nature of deepfakes. Setting international guidelines for dealing

with cyberthreats, especially those that cross national borders, is something that the UN can help with.

The existing Indian laws can be made effective by:

- Add clauses that expressly address deepfakes to already-existing legislation, such as the Personal Data Protection (PDP) Act and the Information Technology (IT) Act. This might entail defining deepfakes in terms of the alteration of digital content and establishing precise rules for data protection concerning biometric information utilizedin deepfakes.
- Run public awareness campaigns regarding deepfake dangers, how to spot them, and the legal ramifications of producing and disseminating deepfake content.
- Encourage cooperation between parties to create a coherent strategy for deepfake regulation and management, including government agencies, tech corporations, civil society organizations, and academic institutions.
- It is advisable to establish a specialized regulatory organization to supervise the execution of deepfake regulations, offer direction, and encourage adherence from relevant parties.

[25] United Nations

4.1 LIMITATIONS OF STUDY

The deepfake is an evolving concept so the study finds difficult in providing the concrete solutions to regulation in Indian scenario. There are no landmark Indian case laws relating to deepfake technology in social media.

4.2 FUTURE SCOPE

In future, more research can be done on regulation of deepfake technology in India. It is an evolving technology, so it is encouraged to conduct research on complexities that deepfake create and legal solutions which will help the legislators in formulating laws for regulating deepfake technology.

5. REFERENCES

1. https://www.legalserviceindia.com/
2. https://www.bbc.com/news/world-asia-india-68918330
3. https://www.hindustantimes.com/india-news/delhi-hc-urges-centre-to-frame-law-to-regulate-ai-deepfake-101724853407493.html
4. https://legal.economictimes.indiatimes.com/news/editors-desk/india-needs-to-make-laws-to-combat-deepfake-menace/111605428
5. https://www.lexology.com/library/detail.aspx?g=9157b1f8-4879-4393-89c2-db5238084b1a#:~:text=Copyright%20Infringement%3A%20Unauthorized%20use%20of,prosecuted%20under%20relevant%20cybercrime%20provisions.