ARTIFICIAL INTELLIGENCE AND DEEPFAKES MEDIA: CHALLENGES BEFORE LAW

Mr. Chitranshu Bhaskar, Department of Law, School of Legal Studies, Babasaheb Bhimrao Ambedkar University (A Central University) Lucknow, Uttar Pradesh, India

Ms. Nisha Kumari Agarwal, Department of Economics, Ambedkar School of Social Science, Babasaheb Bhimrao Ambedkar University (A Central University) Lucknow, Uttar Pradesh, India

Mr. Saheb Talukdar, Department of Economics, Ambedkar School of Social Science, Babasaheb Bhimrao Ambedkar University (A Central University) Lucknow, Uttar Pradesh, India

ABSTRACT

The growth of "artificial intelligence" has led to the significant evolution of deepfakes synthetically produces media (Images and Videos) generated through modern technology. While such technology mainly used in the various sectors such as entertainment and education, it also raises critical legal, ethical, and security concerns related to Individuals and State. The capability to fabricate realistic visual raises by the deepfakes technology significant legal risks, which includes the circulation of false information, identity heist, financial fraud, and threats to national security by the various methods. Deepfakes technology may be deliberately used to manipulate public opinion, damage reputations, undermine democratic institutions and spread rumors. The current laws and legal framework faces significant challenges in addressing current legal implications of deepfakes technology. Existing laws, framework and legal doctrines governing defamation, privacy rights, intellectual property, and cybercrime are not completely effective in responding risks posed by AI and generated media through deepfakes technology. The primary legal challenges include establishing liability of wrongdoer, balancing freedom of expression with the "right to privacy and to live with dignity under Article 21 of the Indian Constitution", and ensuring applicability of these laws. Courts, regulatory bodies, and technology entities must collaborate to strengthen forensic AI technologies, promote digital literacy programs, various awareness campaign and implement regulatory frameworks which regulate the creation and publication of such media and related content. Moreover, public awareness initiatives, abiding the law of the land and adherence to ethical AI governance principles which are crucial to addressing the potential threats arising from deepfakes technology.

Keywords: *Artificial Intelligence, Privacy Rights, Freedom of Expression, Cybercrime, Deepfakes Technology*

INTRODUCTION

Deepfakes technology and its misuse have emerged as a significant international point of concern, included the India, due to the significant legal, ethical, societal, and security implications. Deepfakes refer to digitally manipulated or synthetically generated media, often produced through artificial intelligence techniques such as deep learning mechanism, to create or alter the visual content in any manner that appears highly realistic and it is almost impossible to detect with the naked eyes. The application of deepfakes technology extends its access across various domains, encompassing both lawful and unlawful uses as used by its user. The foundation of deepfakes technology lies in machine learning algorithms that facilitate the generation of high resolution realistic digital content by utilizing an individual's facial features, voice, or overall similarity and likeness. Through AI generated content or media, these digital audio/video can be manipulated to create deceptive content that falsely attributes statements or actions to an individual may cause so many unlawful activities which may cause threat to cause sovereignty and integrity of the state. Such content is then circulated in such a manner that may mislead audiences, thereby raising serious concerns related to misinformation, defamation, privacy violations, cyber fraud and also threat to sovereignty of nation.

Deepfakes technology operates through several mechanisms, including face detection and generation of replica, face matching, face swapping, and speech synthesis and voice modulation. Face enactment entails the digital modification of an individual's facial expressions to replicate the fabricated emotions or actions to do fraudulent activities which are prohibited by law. Face generation involves the creation of an entirely new facial identity, which does not correspond to any real person, thereby raising concerns related to identity fraud and deceptive representation which are protected and ensured under Article 21 of Indian Constitution. Face swapping refers to the replacement of one person's facial features with those of another, leading to misrepresentation to his family. Similarly, speech synthesis enables the artificial reconstruction of a person's voice, which can be misused to create fraudulent audio content, implicating any innocent individuals in unauthorized statements or actions. Increase of deepfakes technology the legal frameworks must address issues related to misrepresentation, consent, defamation, cybersecurity, intellectual property rights and to protect the sovereignty and integrity of the country. The significant growth of deepfakes undermines the necessity for amendment in the current legal system to regulate their creation, distribution, and misuse while balancing fundamental rights such as freedom of expression and privacy.

DEEPFAKES AND HOW IT WORKS

"A deepfakes is a video, photo, or audio recording that seems real but has been manipulated with AI. The underlying technology can replace faces, manipulate facial expressions, synthesize faces, and synthesize speech. Deepfakes can depict someone appearing to say or do something that they in fact never said or did".[1] Deepfakes is a technology which used to create highly realistic media for lawful or unlawful purpose and deepfakes technology is generally known as " Deepfakes are videos creating delusion with the use of deep learning, AI and photoshopping techniques to create images of events to spread disinformation. The technologies namely, GANs (Generative Adversarial Networks) or ML (Machine Learning) are interplayed to create the videos."[2]

Deepfakes technology is the type of artificial intelligence that enables the creation of fake or deceptive and highly realistic digital media such image, video and audio. The "deepfakes" consists the technology where highly realistic media is being used to do fraudulent acts and prohibited actions. The primary legal concern raises with deepfakes technology is its significant capacity to disseminate and circulate false or misleading information under the shadow that it originates from authentic source, thereby undermining trust in digital media and and conduct various fraudulent activities such as, defamation, identity theft, or other malicious activities. Despite these risks, deepfakes technology also has various fruitful use such as its use in the entertainment industry for film to look scene much more realistic and authentic and video game development and to achieve clear resolution in it, as well as in business operations such as automation in the customer service, call forwarding systems, and virtual assistance this technology helps in various ways. Legal frameworks governing deepfakes must balance the protection of individuals' rights, including privacy and reputation, with the recognition of lawful and ethical uses of this evolving technology and determination of unlawful use and determine the unlawful use and its related matter.

WORKING AND USE OF DEEPFAKES

Deepfakes content does not made out of edited or digitally altered media, such as photoshopped

[1] "Science,Technology Assessment and Analytics, Science & Tech Spotlight: Deepfakes, February 2020, https://www.gao.gov/assets/gao-20-379sp.pdf , Accessed on 21 January 2025"

[2] "Vikrant Rana, Anuradha Gandhi And Rachita Thakur, Deepfakes And Breach Of Personal Data – A Bigger Pictur, 23 November 2023, https://www.livelaw.in/law-firms/law-firm-articles-/deepfakes-personal-data-artificial-intelligence-machine-learning-ministry-of-electronics-and-information-technology-information-technology-act-242916 , Accessed on 17 January 2025"

images or manually edited videos. Deepfakes are made or generated through the method of advanced algorithm that are made through blend of existed photo or video and mix with synthesized visual or audio media content, sometimes to do deceptive practice. Similarly, in the machine learning techniques are used to synthesize and create manipulative distinct facial features and voice modulation by the help of AI and others technological methods, which enables the blend of separate video or audio median into different contexts sometimes for the purpose of blackmailing. This deceptive and manipulation often governed by artificial intelligence, which raises legal considerations regarding authenticity, misrepresentation, and potential misuse in fraudulent or deceptive activities.

Deepfakes technology generally generates through the two distinct algorithms: firstly, is a generator and secondly is a discriminator. The generator handles the task for constructing an initial media which is in line with the intended output, generating the preliminary artificial fake digital content. Secondly the discriminator evaluates the authenticity and its relevancy to highly realistic quality of the generated content by identifying discrepancies and assessing its and rate its authenticity. This process continues to refining the media to produce increasingly convincing and highly realistic content while it is efficiency of the discriminator to detect imperfections in the generated media, thereby facilitating progressive improvement in content look so realistic like original.

This process between these algorithms forms a Generative Adversarial Network, a deep learning, analyzing and generating framework is designed to analyze the media generated and made it super realistic and use it for a beneficial purpose. Through Generative Adversarial Network technology, artificial intelligence systematically studies patterns in existing images and videos and then applies them in making blend it intended output media in the creation of manipulated content. When generating deepfakes imagery, a Generative Adversarial Network processes where multiple photographs of the subject from various angles to capture and replicate facial details and perspectives. In the case of deepfakes video production, the Generative Adversarial Network examines video footage from multiple angles, analyzing behavioral, movement, and speech patterns of the original videos. The synthesized content undergoes repeated assessments by the discriminator to enhance its quality, authenticity, ensuring that the final digital representation closely mimics real-life visuals and actions of the subject. The use of Generative Adversarial Network based deepfakes technology presents various legal implications related to intellectual property, privacy rights, and its significant

misuse in fraudulent or deceptive purposes, which generated need of hour regarding laws and regulations by various authorities at various level to balance innovation with ethical and legal safeguards.

1. Deepfakes creates accessibility - Artificial intelligence[3] has the capability to develop systems that process audio and visual inputs and, with the development of Artificial Intelligence will progressively enhance its capacity for reasoning and decision making with greater accuracy in different situations. This AI generated synthetic media can contribute to the advancement of accessibility tools by improving their efficiency, and affordability, thereby enabling personalized solutions for individuals with specific need and of person with disability. These AI based solutions present significant opportunities for ensuring equitable access to digital and physical environments. However, the deployment of AI based tools must align with legal and regulatory frameworks to safeguard against potential biases, ensure data privacy, and uphold individuals' rights in the development and application of such technology while following the laws enforces in the land.

2. Use of Deepfakes in field of education - Deepfakes technology offers various uses within the field of education. Educational institutions and instructors have various media resources, including audio and video, as instructional tools in classroom settings to help and aid the students. The integration of deepfakes technology into educational frameworks enables educators to enhance lesson delivery through dynamic and interactive content that surpasses the engagement levels of conventional visual and media formats and increases the efficiency of distant education.

3. Use of Deepfakes in Entertainment Industry - For several decades, the film industry has employed advanced Computer Generated Imagery[4], Visual Effects[5] and Special Effects[6] technologies to produce artificial yet realistic environments for storytelling purposes and entertainment purpose, A notable example is the 1994 film Forrest Gump[7], in which the protagonist interacts with historical figures such as John" F. Kennedy. The creation of these

[3] "Artificial intelligence (AI) is a field of study that focuses on the intelligence of machines, especially computers"
[4] "Computer-generated imagery is the use of computers to create images for visual media"
[5] "Visual effects (VFX) are computer-generated images or manipulated footage that are added to films or other moving media"
[6] "artificial images, especially in a film, that appear real but are created by artists and technical experts"
[7] "Forrest Gump is a 1994 American comedy-drama film directed by Robert Zemeckis. An adaptation of the 1986 novel by Winston Groom, the screenplay of the film is written by Eric Roth"

scenes was achieved through Computer Generated Imagery and other digital enhancement techniques, requiring significant financial investment to generated hyper realistic entrainment media. In contemporary filmmaking, the Computer Generated Imagery[8] and Visual Effects technologies are widely used to generate synthetic highly realistic media, enabling the seamless integration of digitally created elements into cinematic universe. The use of such technologies facilitates enhanced visual storytelling while raising legal considerations related to intellectual property rights, fair use, and the ethical depiction of real or historical figures.

4. Use for Unlawful purpose - Deepfakes content does not made out of edited or digitally altered media, such as photoshopped images or manually edited videos. Deepfakes are made or generated through the method of advanced algorithm that are made through blend of existed photo or video and mix with synthesized visual or audio media content, sometimes to do deceptive practices.

TYPES OF DEEPFAKES TECHNOLOGIES

In the past decade, deepfakes technology has advanced with a rapid growth at significant pace, evolving into three broad and distinct categories, which are as follows:

Face swapping under deepfakes - Refers to the digital modification of visual or media by replacing an individual's facial features with those of another person within a photograph or video for the deceptive practices. This process involves the use of artificial intelligence and machine learning techniques to seamlessly blend the substituted facial image, creating a modified representation that may appear authentic and real.

Lip syncing under deepfakes - This involves the digital modification of audio or video content to create the appearance that an individual is speaking words they did not actually say to highly realistic content. This process utilizes and use the artificial intelligence and machine learning techniques to synthesize the individual's lip movements with altered or artificially generated speech, potentially misrepresenting their statements or intentions.

Puppet Technique under the Deepfakes – "The Puppet technique refers to the fake movements of an individual in an unnatural manner. While deepfakes technology has many benefits, it does affect public figures more negatively than any other sector. (Ask the divorcee!!)

[8] "Computer-generated imagery is the use of computers to create images for visual media"

The nonconsensual deepfakes that may depict celebrities in compromising situations are problematic, but it remains an important example of what this technology can produce. With reference to Bass and Penning (2023) deepfakes of celebrities have been used widely in advertising campaigns but are also now depicting political figures which may affect them with a possible loss of an election".[9]

CHALLENGES POSED BY ARTIFICIAL INTELLIGENCE DEEPFAKES TECHNOLOGY

Detectability of the media – Deepfakes generally not detected by human eye it does need of special detection technologies which require extensive and diverse database to effectively identify and analyze manipulated digital content and an effective mechanism to remove such kind of media. To enhance and effectiveness of this technology and the reliability of these detection tools, technology companies and researchers have developed and released their database for training purposes. However, existing database alone are insufficient completely to address the complexity of deepfakes technology. To maintain the efficacy and efficiency of detection tools, time to time changes are necessary with increasingly data are necessary. These current refinement ensures that detection mechanisms remain capable of identifying and mitigating the risks associated with deepfakes generated media, in accordance with legal and regulatory frameworks governing integrity and privacy of a person, prevention of false information, and data security.

No tool for Automatic Detection of Deepfakes Media - Existing deepfakes detection tools are not that capable of conducting fully automated and comprehensive analyses that reliably identify deepfakes content. Current technological limitations prevent the consistent detection of manipulated digital media without human oversight and supervision. Current ongoing research initiatives are focused on developing advanced devices to automate deepfakes detection, analyze the techniques used in their creation, and evaluate the overall authenticity and originality of digital content without supervision of any human. These aim to enhance the accuracy and reliability of detection mechanisms technologies while ensuring compliance with laws of the land related to digital forensics, media authenticity, and the prevention of fraudulent

[9] "Trishana Ramluckan, Deepfakes: The Legal Implications, March 2024, ResearchGate, https://www.researchgate.net/publication/379221500_Deepfakes_The_Legal_Implications , Accessed on 07 January 2025".

or deceptive practices within its jurisdiction.

Insufficiency related to detection of deepfakes content - Even if deepfakes detection technology were to achieve perfect accuracy, it may not fully prevent the dissemination, circulation or impact of deceptive digital content as most of the public is not aware related to this. A significant number of viewers may lack awareness of deepfakes technology or may not independently verify the authenticity of the media as the tools are not accessible for them. As a result, manipulated content may still be used as a tool for misinformation, influencing public opinion, decision-making, and discourse and also to do deceptive activities in fraud and other such things. This raises the necessity for laws and legal regulatory measures addressing digital media literacy, content authentication, and the responsible dissemination of digital information mitigating the risk of online fraud.

Regular Updates or invention related Deepfakes detection technology - The advancement of deepfakes detection methods raises the development of increasingly highly realistic deepfakes media generation techniques. This current "hide and seek" condition raises need of an hour continuous enhancements in detection technologies to effectively counter the emerging manipulation and deepfakes technologies. To maintain the reliability and effectiveness of deepfakes detection tools, they must be regularly updated and refined to adapt to evolving threats and their efficiency remain highly effective to govern and protect the digital right of privacy of the citizen protected under Article 21[10] of the Indian Constitution held in the case of " *K Puttaswamy V Union of India "*[11].

Challenges related to Law making regarding deepfakes technology – Current laws or regulatory framework targeting deepfakes media are significantly insufficient may give rise to questions concerning the balance between freedom of speech and expression[12] and the privacy rights[13] of individuals who are wrongly deceived in manipulated content. These laws and regulations must carefully address these constitutional and legal principles to ensure that any restrictions on deepfakes media creation and dissemination must not infringe right to privacy. The passing of efficient law to combat the misuse of deepfakes technology and regulation of such technology may present enforcement challenge, including jurisdictional related

[10] Constitution of India 1950, Art21
[11] AIR 2018 SC (SUPP) 1841
[12] "Constitution of India 1950, Art19 "
[13] "Constitution of India 1950, Art 21 and K Puttaswamy V Union of India, AIR 2018 SC (SUPP) 1841"

complexities, technological limitations in detection are the significant challenges present in the current scenario.

Use of deepfakes technology against women – The deepfakes technology generally be used against women and may promote gender inequality, by circulating offensive content made with the use of this technology. Deepfakes content significantly affects women, who are frequently targeted through the creation and dissemination of non-consensual pornographic material or other manipulated media intended to defame, harass, or harm their reputation and violate the right to dignified life under Article 21 and right to privacy under Article 21. Social media platforms have a duty to ensure that their digital spaces remain safe and free from such deepfakes content not promote gender biasness. While Google has included "involuntary synthetic pornographic imagery" in its banned content list, this action alone is not sufficient to solve the problem of the production and circulation of such material in cyberspace. The creation of deepfakes is often driven by malicious intent, including extortion, blackmail, revenge and pornography of women to defame the women. Once such deepfakes manipulated content is uploaded and disseminated online through internet and there are no such laws and regulation which are effective to regulate such issues, its rapid circulation makes it exceedingly difficult to remove entirely. The viral nature of these materials, which includes the instances of sharing, downloading, and re-uploading, complicates the authorities to trace the original source or effectively stop the circulation of the content. This misuse of deepfakes technology has established new avenues for the abuse and victimization of women, and raises the need of hour of stricter laws and legal frameworks to held person liable.

IMPLICATION OF AI DEEPFAKES IN LAWS AND REGULATION

Various Laws and legal framework addresses and restricting the use of deepfakes Laws must be made in accordance constitutional protections of free speech and expression[14]. A primary legal challenge is the differentiation between lawful applications of deepfakes technology, such as satire and artistic expression or media and educational purposes, and the other one is prohibited uses where creator has intended to deceive or cause harm to other person. Effective enforcement of restrictions on malicious deepfakes content raises the concern regarding well established legal framework, whether it is efficient or not and to establish civil or criminal liability, evidence related to actus rea and mens rea must be sufficient which is the point of

[14] "Constitution of India 1950, Art 19"

concern, which is creating significant enforcement challenges for regulatory and enforcement authorities. But to prove mens rea is particularly complex task for the authorities, as deepfakes material may be disseminated under the shadow of various permitted use of deepfakes such entertainment or education. These legal ambiguities create substantial hurdles for law makers in enacting and enforcing the law that effectively mitigate the risks associated with deepfakes while preserving and protecting fundamental rights.

LAWS OF VARIOUS COUNTRIES RELATED TO ARTIFICIAL INTELLIGENCE DEEPFAKES

The European Union laws related to Artificial Intelligence Deepfakes - The European Union Artificial Intelligence Act was the first and foremost comprehensive international step which is aimed to establishing a legal framework for the regulation of artificial intelligence generated deepfakes. The Act establishes the position of the European Union as highest body related to AI and deepfakes by implementing regulations smoothly to governing the development, and commercialization, of AI systems within the European Union. Its primary objective is to ensure that AI generated deepfakes technologies operate in a correct, legal and ethical manner, in accordance with fundamental rights and moral standards. There are three key objectives of this Act Firstly Promoting investment and innovation in AI technologies, secondly Enhancing governance and enforcement mechanisms; and thirdly Establishing a unified EU market for AI-based systems. This act also incorporate the existing regulation enforced by EU, However, the Act does not specifically govern the data protection and online platform related regulations as these matters are addressed under separate legal frameworks made by the EU.

The United States laws related to Artificial Intelligence Deepfakes - Currently, there is no central legislation in the United States that directly regulates or mitigates the deepfakes technology and risk related to it. However, in 2019, Congress enacted the National Defense Authorization Act, which includes Section 5709[15], this section mandating the Director of National Intelligence to assess and report on three points Firstly The use of deepfakes technology by foreign governments in their respective jurisdiction, Secondly The role of deepfakes in spreading misinformation and other related issues; and, Thirdly The potential

[15] " National Defense Authorization Act for Fiscal Year 2020, US, s.5709 "

impact of deepfakes content for national security. A primary criticism of the NDAA[16] act's approach is that, while it provides a framework for monitoring and addressing deepfakes and its related threats originating from foreign entities and the potential harm by them, it fails to regulate or mitigate the domestic risks posed by deepfakes within the United States. The absence of comprehensive federal legislation leaves gaps in addressing the misuse of deepfakes technology for fraud, defamation, election interference, and other malicious activities at the national level and there is no central legal framework to regulate them.

The United Kingdom laws related to Artificial Intelligence Deepfakes - The United Kingdom has implemented legislative measures to regulate deepfakes technology, by Online Safety Act 2023[17]. But this act has various issues regarding the existing legal framework its primary focus on cases involving revenge pornography, rather than addressing the broader impact on misuse of deepfakes technology. Prior to the enactment of the Online Safety Act, prosecutors in deepfakes and its related cases were required to establish that the perpetrator acted with intent to cause distress which was difficult to prove, which presented a significant evidentiary challenge. Under the current legislation: if the intention that is mens rea is proved punishment is of two years under this act and - If mens rea not be established penalty is six months for creation of this kind of deepfakes content. The Online Safety Act 2023 also imposes obligations on deepfakes service providers, regarding user identification and verification measures and its implementation to ensure that malicious deepfakes content can be traced back to its creators and punished with accordingly. Section 13(4)[18] of the Act mandates that online platforms are directed to take action against harmful content targeted at adults, by: Removing such content, Restricting the access of user to such content; and Limiting the recommendation and promotion of such content on digital platforms.

AI DEEPFAKES IN LAWS AND REGULATIONS IN INDIA

"India too has witnessed recent incidents related to deepfakes revenge porn and deepfakes technology being used in political campaigns. One was an incident in October 2019, where a man in Mumbai was arrested for an act of making a revenge deepfakes porn video of his girlfriend just to threaten her. Followed by in early months of 2020, in February two videos of Manoj Tiwari were released by BJP, where there was only one video but in two languages with

[16] "National Defense Authorization Act for Fiscal Year 2020, US"
[17] "Online Safety Act 2023, UK"
[18] "Online Safety Act 2023, UK, s.13"

an intention to reach two different linguistic voters, the achievable solution right now to tackle the upcoming threat of this technology is to combine the technology and the legislation. The recent trend of using this deepfakes technology in making fake pornographic videos and political campaigns do raise several questions over the concerns related to privacy, identity theft and as well as the reality and authenticity of elections and the content available in social media platforms"[19].

UNDER THE INFORMATION TECHNOLOGY ACT, 2000

"Information Technology Act, 2000 and the Information Technology (Intermediary Guidelines and Digital Media Ethics) Rules, 2021" impose laws and regulatory obligations on digital platforms and on online intermediaries. Failure to comply with these provisions may result in the loss of protections granted under Section 79(1)[20] of the IT Act, 2000. Section 79(1)[21] of the IT Act, 2000 provides conditional immunity to online intermediaries, exempting them from liability for any third-party information, data, or communication links that they host or make available. However, non-compliance with the Rule 7[22] could lead to revocation of this immunity, making online intermediaries legally accountable for content hosted on their platforms, Rule 7 of the IT Act, 2000 Rules grants aggrieved party the right to pursue legal action against online platforms under the provisions of the IPC[23] now Bhartiya Nyaya Sanhita 2023[24].

Section 67[25] of the IT Act, 2000 criminalizes the publication or transmission of obscene media in electronic form. Offenders may inflict the penalties for violations of this provision, under the Section 67A[26] of the Informati Act, 2000 create liability on any person who publishes or transmits sexually explicit visual content through electronic means and mode in the case of "*Shreya Singhal v. Union of India"*[27], Hon'ble Supreme Court has held the Section 66A[28] of IT Act unconstitutional, under Section 67B[29] of the IT Act, 2000 specifically prohibits and

[19] "Information Technology Act, 2000. s.79"
[20] "Information Technology Act, 2000. s.79"
[21] "Rules for Information Technology Act 2000, Rule 7"
[22] "Rules for Information Technology Act 2000, Rule 7"
[23] "Indian Penal Code, 1860"
[24] "Bhartiya Nyaya Sanhita 2023"
[25] "Information Technology Act, 2000. s.67"
[26] "Information Technology Act, 2000. s.67A"
[27] "AIR 2015 SUPREME COURT 1523"
[28] "Information Technology Act, 2000. s.67A"
[29] "Information Technology Act, 2000. s.67B"

penalizes the publication or transmission of sexually explicit content which involves minors on digital platforms this is also a punishable offence, Under Section 66C[30] of the IT Act, 2000 criminalizes the fraudulent use of unique identification information of any person, including but not limited to electronic passwords, biometric data, or other personal identifiers of an individual means any other kind of acts also inflict liability and under Section 66D[31] of the IT Act, 2000 penalizes cheating by personation through the use of computer resources, imposing legal consequences for those who impersonate others for fraudulent purposes or use the other person's identity for own benefit.

Section 66E[32] of the IT Act, 2000 criminalizes the unauthorized publication or transmission of an individual's private images without their consent and Violation of Section 66E is punishable by up to three years of imprisonment and a fine of 2 lakh Indian Rupee.

OTHER LAWS RELATED TO DEEPFAKES LAWS IN INDIA

A person may be held liable for the defamation under both criminal law and civil law in the India. Cyber defamation (defamation by the way of online medium) was previously governed by Section 66A of the IT Act. Under civil law, defamation falls within the ambit of the law of torts, where, if the act is proven, the defamed party is entitled to claim damages. Similarly, under old criminal law, Section 499[33] of the IPC, 1860 and under Section 356[34] of BNS, makes defamation as a bailable, non-cognizable, and compoundable offense. This provision encompasses the publication of any material that is likely to harm an individual's reputation. The corresponding penal provision, Section 500[35] of the IPC, 1860 and under Section 356 of BNS, prescribes punishment in the form of imprisonment for a term extending up to two years, a fine, or both but in new criminal laws another punishment introduced for defamation which is community service. However, these legal provisions remain inadequate to comprehensively address the complexities associated with emerging forms of deepfakes technology. Previously, cyber defamation was also governed under "Section 66A of the IT Act", which penalized the transmission of offensive content through a computer source, where such content was intended to cause obstruction, insult, injury, hatred, criminal intimidation, or ill will in the case of *Shreya*

[30] "Information Technology Act, 2000. s.67C"
[31] "Information Technology Act, 2000. s.67D"
[32] "Information Technology Act, 2000. s.67E"
[33] "Indian Penal Code 1860, s.499"
[34] "Bharatiya Nyaya Sanhita, 2023, s.356"
[35] "Indian Penal Code 1860, s.500"

"Singhal v. Union of India"[36], Hon'ble Supreme Court has held the Section 66A[37] of Information Technology Act unconstitutional.

VARIOUS JUDGEMENTS RELATED TO AI AND DEEPFAKES TECHNOLOGY.

The Right to privacy was not mentioned anywhere expressly in the Indian Constitution and this right was not even recognized, the evolution of the right to privacy in India has been established by judicial precedents in the past six decades. Various interpretations arising from two early rulings which led to uncertainty regarding its status as a fundamental right. However, the recent judgment resolves these inconsistencies and uncertainty and declared the right to privacy as a fundamental right under Indian Constitution. Also, the constitutional provisions must be enacted in a manner which is in accordance with India's international human rights obligations. The judgment also establishes that privacy is an essential condition for the effective exercise of other fundamental rights, and in the case of "*Justice K.S. Puttaswamy (Retd) vs Union of India"*[38] where constitutional validity of Aadhar Scheme was challenges before the Hon'ble Supreme Court of India.

There misuse use of deefakes technology violates the right to privacy of other person and violation of judgement of "*Justice K.S. Puttaswamy (Retd) vs Union of India"*[39] and in various cases court's observation was against the misuse of deepfakes technology and to proper regulation of the deepfakes technology. In "*Anil Kapoor v. Simply Life India and Ors"*[40], the Delhi High Court heard upon a suit filed by Bollywood actor Anil Kapoor, who sought protection against the unauthorized use of his name, likeness, voice, and other personal attributes through AI-generated deepfake content, including GIFs, emojis, ringtones, and sexually explicit material. The Court, recognizing the actor's right to privacy and issued an ex parte injunction order restraining sixteen entities from commercially exploiting his identity through AI tools or any other means for financial gain and considered it violation of the right to privacy of person as upheld in the case of "*Justice K.S. Puttaswamy (Retd) vs Union of India"*[41]. Similarly "*Amitabh Bachchan v. Rajat Negi and Ors"*[42], the Court granted an ad interim in rem injunction order, preventing the unauthorized commercial uses his name, image,

[36] "AIR 2015 SUPREME COURT 1523"
[37] "Information Technology Act, 2000. s.67A"
[38] 'AIR 2018 SC (SUPP) 1841"
[39] "AIR 2018 SC (SUPP) 1841"
[40] "CS(COMM) 652/2023 and I.A. 18237/2023-18243/2023"
[41] "AIR 2018 SC (SUPP) 1841"
[42] "CS(COMM) 819/2022"

voice, and likeness of the Amitabh Bachchan. These judgments reaffirm the legal protection given to an individual and protection of life and liberty which includes " right to privacy under Articles 21[43] of the Indian Constitution", particularly through emerging technological tools such as AI and its generated deepfakes technology.

CONCLUSION

The blend or inclusion of digital media and artificial intelligence, particularly in the context of deepfakes technology, presents significant legal and societal challenges that must be properly analysed and addressed by the appropriate authority. The significant growth of deepfakes technology has substantial implications for both individuals and society at large, where need of hour is a comprehensive legal framework that considers the various dimensions of this technology. A thorough examination of deepfakes in digital media is required to assess their impact on legal rights and fundamental right and legal rights of the individual, regulatory policies and legal frame work, and the integrity of information dissemination and integrity of persons against whom it is used. However, the absence of well-established laws and regulation makes it difficult to address the issue and effect thereof. A primary concern is the potential losing the of trust in institutions, and journalism processes, as deepfakes technology may undermine the ability of the public to distinguish between authentic and manipulated content available in Internet and Social Media and it may lead to widespread misinformation and the adoption of an "everything is fake" perception, thereby diminishing confidence in legal and regulatory framework and systems. Although technological measures for detecting, verifying, and eliminating deepfakes content are essential. A comprehensive legal and regulatory framework is necessary, which incorporates statutory provisions, enforcement mechanisms, and international cooperation to mitigate the risks associated with deepfakes technology.

[43] "Constitution of India 1950, Art21"