Deepfake Pornography: Examining the Impact on Women's Digital Privacy and Consent

Ms. Muskan Sharma

Teaching Assistant & Research Fellow, School of Law, The NorthCap University

Abstract

Cybercrime is a growing concern in India, particularly for women, due to societal devaluation and inadequate legal recognition of cybercrimes. With the advancements in Artificial Intelligence (AI) have led to various forms of cybercrime, including deepfakes and dark web activities. Currently, India lacks specific legislation to address emerging cybercrimes targeting women. The existing statute, such as the Indian Penal Code of 1860 and the Information Technology Act of 2000, collectively aim to address these issues.

This paper explores deepfake cybercrimes, that significantly impact on women's dignity and violate their right to privacy, particularly on social media platforms. The study highlights the inadequacies of current cybersecurity laws in effectively addressing deepfake-related cybercrimes in our technologically advanced society. The study explores the technological underpinnings of deepfake creation, legal frameworks, and potential solutions to mitigate the harms caused by deepfake pornography.

Keywords: Deepfakes, Pornography, Consent, Cybercrime, Article 21, Right to privacy.

INTRODUCTION

In the 21st century “cybercrime”[1] has become a well-known and prevalent form of criminal activity, particularly targeting women. In India, the technology sector is seeing a significant increase in smartphone and internet usage among consumers, raising concerns about user privacy and security. Recently, there has been a rise in cybercrimes against women, such as deepfakes and dark web activities, potentially driven by technological advancements in the country. In simple terms, a deepfake can be described as the manipulation of someone's identity using various tools, such as photoshop. The term "deepfake" gained prominence in 2017 when a Reddit user utilized the technology to interchange the faces of celebrities with those of adult stars[2]. The essence of the term "deepfake" lies in its components - 'Deep' represents Deep learning, and 'fake' signifies the ‘act of deception’[3]. Broadly, deep fakes are machine learning bases software tool that produce realistic synthetic media content[4]. As per the Merriam Webster Dictionary, “deep fakes” defines as “an image or recording that has been convincingly altered and manipulated to

[1] Oxford University, “Cybercrimes” means “crime that is committed using the Internet” Retrieved from https://www.oxfordlearnersdictionaries.com/definition/american_english/cybercrime

[2] Team, ‘AI in Marketing Case Study:Cadburys Hrithik Roshan Promotion’ (*The Hard Copy*25 August 2021) <https://thehardcopy.co/personalised-celebrity-messages-using-ai/> accessed 24 May 2024

[3] Heidari A and others, ‘Deepfake Detection Using Deep Learning Methods: A Systematic and Comprehensive Review’ (2023) 14 Wiley interdisciplinary reviews. Data mining and knowledge discovery/Wiley interdisciplinary reviews. Data mining and knowledge discovery <https://wires.onlinelibrary.wiley.com/doi/full/10.1002/widm.1520> accessed 24 May 2024

[4] Jennifer Laffier & Aalyia Rehman, “Deepfakes and Harm to Women”, 25 *Journal of Digital Life and Learning*, (2023)

misrepresent someone as doing or saying something that was not actually done or said[5].” Deepfakes employ facial mapping technology and artificial intelligence (AI) to substitute the face of an individual in a video with that of another person. Social media platforms, such as Facebook, also offer bug bounty programmes targeted at identifying solutions to identify deep fake content.

It is a kind of cybercrime against women in India. It is not expressly defining in any Indian statue like Informational Technology Act of 2000. But impliedly section 66E[6] of the IT Act deals with the crime which infringe the privacy of any person. In addition of this, Section 66D of the IT Act, provides that “any individual with malicious intent, to cheat or impersonate someone by using any communicating device or computer resource, can result in imprisonment for up to 3 years or fine upto 1 lakh[7]”. These sections, i.e., section 66D and 66E, are impliedly deal with cybercrime like deep fake. The increasing frequency of cybercrimes, especially those directed towards women, highlights the need for a thorough review of the current legal system and its suitability for handling new risks like deepfakes.

In the 21st century, where technological advancements are integral to societal progress, the dark underbelly of cyberspace poses a formidable challenge to privacy and security. The rise of deepfakes has sparked concerns over the potential negative impact they may have, specifically for women in India under the IT Act 2002. These digitally altered media, which are designed to appear authentic, pose a serious threat not only to individuals but also to larger societal issues such as privacy and trust. As technology continues to advance at a rapid pace, it is crucial to fully understand and address the dangers posed by deepfakes before they cause irreversible harm. The emergence of deepfakes has raised alarm bells for the potential harm they can cause to individuals, particularly women in India. The IT Act 2002, which governs the use of technology in India, does not specifically address deepfakes, leaving a gap in the legal framework for dealing with this issue. This loophole can have serious implications for women, as deepfakes can be used to harass, defame, or blackmail them**.**

The consequences of deepfakes for women in India are not limited to individual harm, but also extend to larger societal issues. For instance, these manipulated media can erode trust in the authenticity of information and images, making it increasingly difficult to distinguish between what is real and what is fake[8]. Further, with the deepfake technology, the deepfake pornographic/ obscene image or content without her consent uploaded on social media. For instance, as per the report of May 20, 2024, a 22-year-old man, Yash Bhavsar, has been arrested in Madhya Pradesh for creating obscene deepfake photos of at least ten women on social media, most of whom are college students[9]. Bhavsar, who worked as a computer operator with the Shajapur municipal council, allegedly created the photos using an AI-based app and created a fake Instagram account. He sent the photos to the women, threatening them to circulate them if they blocked or ignored him. Police have seized Bhavsar's mobile phone and laptop, and a further investigation is ongoing.

[5] ‘Merriam-Webster Dictionary’ (*Merriam-webster.com*21 May 2024) <https://www.merriam-webster.com/dictionary/deepfake> accessed 24 May 2024

[6] Information Technology Act, 2002 (Act 21 of 2000), s.66E “Punishment of Violation of Privacy, “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.”

[7] Information Technology Act, 2000 (Act 21 of 2000), s. 66D

[8] ‘Asking Questions of AI Advertising: A Maieutic Approach’ (*Journal of Advertising*2022) <https://www.informahealthcare.com/doi/full/10.1080/00913367.2022.2111728> accessed 24 May 2024

[9] English, ‘NDTV’ (*NDTV.com*20 May 2024) <https://www.ndtv.com/india-news/man-arrested-for-creating-deepfake-photos-of-women-and-threatening-them-5707344> accessed 24 May 2024

In a society where women already face numerous challenges and discrimination, deepfakes can add another layer of complexity to their lives. This can have a detrimental impact on their mental health, self-esteem, and overall well-being. To address this urgent issue, it is crucial to not only have specific laws and regulations in place but also to educate the public about the dangers of deepfakes. This can include raising awareness about how to identify deepfakes and how to report them, as well as promoting media literacy and critical thinking skills. Additionally, technology companies and social media platforms have a responsibility to develop and implement tools to detect and remove deepfakes, as well as to provide support for victims of deepfake attacks. In conclusion, the emergence of deepfakes has posed a significant threat to women in India under the IT Act 2002. These digitally altered media not only have the potential to cause harm to individuals but also to erode trust and create societal issues. It is imperative to address this issue urgently, through a combination of clear laws, education, and technological solutions, to protect the rights and well-being of women in India. Only through collective efforts can we mitigate the negative impact of deepfakes and ensure a safer and more secure environment for all.

The roots of deepfake technology have substantial origins in India, particularly in its widespread application within the domains of politics, the film industry, pornography, and instances of revenge-defamation. Notable instances involve deepfakes depicting Mr. Manoj Tiwari criticizing the Delhi government, members of the Aam Aadmi Party speaking in English and Haryanvi dialects, and the creation of explicit content involving Ms. Rana Ayyub[10]. It is imperative to acknowledge the potential adverse impact that deepfakes may have on both targeted individuals and society as a whole. The dissemination of manipulated content of this nature has the potential to cause harm by undermining sentiments, ideologies, and perspectives held by individuals within society. Rephrase.ai, identified as a corporate entity, generated a fabricated video featuring Mr. Hrithik Roshan expressing gratitude to his followers. It is noteworthy that Mr. Hrithik had granted Rephrase.ai permission to use his likeness and manipulate it for promotional purposes related to Cadbury confectionery products. While these actions align with legal standards, there persists a necessity for regulations governing the use of deepfakes.

The surge in cybercrimes against women, including the insidious practices of deep fakes and activities on the dark web, points to the evolving nature of threats facilitated by technological progress in the country. Deep fakes, being machine learning-based tools that generate realistic synthetic media content, have emerged as a sophisticated means of exploiting and victimizing individuals[11]. The term "deep fakes" itself, as defined by the Merriam-Webster Dictionary, captures the essence of convincingly altered media that misrepresents individuals, thus intensifying the need for legal scrutiny[12]. While the Information Technology Act of 2000 forms the backbone of the legal response to cybercrimes in India, the absence of explicit provisions addressing deep fakes raises critical questions about the effectiveness of the current legal framework. Despite the implicit coverage of privacy infringements under Section 66E of the IT Act, the intricate nature of deep fake cybercrimes demands a nuanced legal approach. This necessitates a comprehensive review of existing statutes and an evaluation of their applicability to the unique challenges posed by deep fakes.

[10] Awasthi P, 'BJP Leader Manoj Tiwari Used Deepfake Videos to Reach out to Voters in Delhi: Report' (*BusinessLine*19 February 2020) <https://www.thehindubusinessline.com/news/national/bjp-leader-manoj-tiwari-used-deepfake-videos-to-reach-out-to-voters-in-delhi-report/article30857871.ece> accessed 24 May 2024

[11] Pesetski A, 'Deepfakes: A New Content Category for a Digital Age' (*William & Mary Law School Scholarship Repository*2020) <https://scholarship.law.wm.edu/wmborj/vol29/iss2/7/> accessed 24 May 2024

[12] Ibid

INTERNATIONAL PERSPECTIVE ON DEEPFAKE

The international framework on cybercrime against women is evolving, with various countries and conventions working to address the issue. The Istanbul Convention and Budapest Convention have stated that cybercrime is violence against women in digital or online spaces. The Committee on the Elimination of All Forms of Discrimination against Women (CEDAW) extends the definition of violence against women beyond physical space to include "technology-mediated environments," addressing online and ICT-facilitated digital violence against women[13].

The Istanbul Convention provides a comprehensive definition of the types of violence against women, including online and ICT-facilitated violence. It considers violence against women as a violation of human rights and a form of discrimination against women. Article 3(a) and (b) of this convention defines "violence against women" as any acts of gender-based violence that result in, or are likely to result in, physical, sexual, psychological, or economic harm or suffering to women, including threats of such acts, coercion, or arbitrary deprivation of liberty, whether occurring in public or private life[14].

GREVIO is empowered by Article 69 of the Istanbul Convention to adopt general recommendations for the convention's implementation. At its 21st plenary meeting, GREVIO decided to prepare its first general recommendation and dedicate it to the application of the Istanbul Convention regarding the digital dimension of violence against women[15]. The scope of the "violence against women" has wider by including non-consensual image or video sharing, coercion and threats, online sexual harassment, impersonation, online stalking or stalking via the Internet of things, as well as psychological abuse and economic harm perpetrated via digital means against women and girls[16].

The Cybercrime Convention Committee (T-CY) ensures the effective implementation of the Budapest Convention and represents the states parties to the convention. The consultation of the Committee aims at facilitating the effective use and implementation of the Convention, the exchange of information, and consideration of any future amendments.

In November 2023, the Bletchley Declaration was chaired to address the risks and responsibilities involved in AI more comprehensively and collaboratively by focusing more on fostering scientific cooperation. The declaration addresses the hazards of intentional misuse and loss of control over AI technologhotelies, particularly cybersecurity, biotechnology, and disinformation risks. The participating countries will prioritize identifying AI safety risks of shared concern, building a shared scientific and evidence-based understanding of these risks, and establishing risk-based policies across their countries to address AI-related issues.

[13] Reyhanne N and others, 'Protecting Women and Girls from Cyber Harassment: A Global Assessment of Existing Laws Global Indicators Briefs No. 18 Public Disclosure Authorized Public Disclosure Authorized Public Disclosure Authorized Public Disclosure Authorized' (2023) <https://documents1.worldbank.org/curated/en/099456506262310384/pdf/IDU0c7c3a5a70b56a04b250a31b0b32b8f5cd856.pdf>

[14] 'European Union: Istanbul Convention Enters into Force' (*The Library of Congress*2015) <https://www.loc.gov/item/global-legal-monitor/2023-10-10/european-union-istanbul-convention-enters-into-force> accessed 24 May 2024

[15] 'GREVIO Group of Experts on Action against Violence against Women and Domestic Violence (GREVIO)' <https://rm.coe.int/grevio-s-baseline-evaluation-report-on-legislative-and-other-measures-/1680ad79b9> accessed 24 May 2024

[16]'PROTECTING WOMEN and GIRLS from VIOLENCE in the DIGITAL AGE' <https://rm.coe.int/therelevance-of-the-ic-and-the-budapest-convention-on-cybercrime-in-a/1680a5eba3> accessed 24 May 2024

United States of America (USA)

In the United States of America, there is no specific legal statute that directly addresses cybercrime against women. Although, there are various laws and regulations cover different aspects of cybercrime, including those that may affect women. The Computer Fraud and Abuse Act (CFAA) of 1986[17], is a federal law that criminalises unauthorised access to computer systems and networks, as well as the theft or unauthorised disclosure of computer information. While the CFAA does not specifically target deepfake as cybercrime against women, it can be used to prosecute cases involving unauthorised access to personal information or online accounts.

The law was enacted as an amendment to the Comprehensive Crime Control Act of 1984 to address growing concerns about computer hacking. Cybercrimes against women in the USA include blackmail, threats, cyber pornography, the publishing of obscene sexual content, stalking, bullying, defamation, morphing, and the establishment of fake profiles[18].

Deepfakes is manipulated media files that depict a false image or video of a person have been increasing in popularity over the past few years. Previous estimates by wired show that in the first nine months of 2023, at least 244,635 deepfake videos were uploaded to the top 35 websites that host deepfake pornography. Ten states, like Virginia and Texas, have criminal laws against deepfakes, but there is currently no federal law in USA.

In May 2023, Rep. Joe Morelle, a Democrat from New York, introduced *the Preventing Deepfakes of Intimate Images Act* of 2023 to criminalize the non-consensual sharing of sexual deepfake images online[19]. This Act was enacted to protect national security against the threats posed by deepfake technology and to provide legal recourse to victims of harmful deepfakes. The Act entails certain pre-requisites for the producers of the deepfakes like digital watermarks, disclosure requirements etc. It creates both civil and criminal liability for the creation of deepfakes[20].

The U.S. introduced the bipartisan Deepfake Task Force Act to assist the Department of Homeland Security in countering deepfake technology. In Jan 30, US lawmakers introduced a new bill called the *Disrupt Explicit Forged Image and Non-Consensual Edits (DEFIANCE) Act of 2024*, which allows victims of AI-generated porn and deepfakes to sue for compensation[21]. Alongside, US lawmakers María Elvira Salazar and Madeleine Dean on January 10 had, legislators also introduced the *No Artificial Intelligence Fake Replicas and Unauthorized Duplications (No AI Fraud) Act of 2024*, which would protect Americans from having their images and voice manipulated.

[17] 'Computer Abuse: Overview, History, Examples' (*Investopedia*2024) <https://www.investopedia.com/terms/c/computer-abuse.asp#:~:text=1984%20(CFAA).-,The%20Computer%20Fraud%20and%20Abuse%20Act%20of%201984,both%20civil%20and%20criminal%20matters> accessed 24 May 2024

[18] GeeksforGeeks, 'Cyber Crime against Women' (*GeeksforGeeks*3 September 2022) <https://www.geeksforgeeks.org/cyber-crime-against-women/> accessed 24 May 2024

[19] *"Text of H.R.3106 - 118th Congress (2023-2024): Preventing Deepfakes of Intimate Images Act"* available at https://www.congress.gov/bill/118th-congress/house bill/3106/text?s=1&r=1&q=%7B%22search%22%3A%22Preventing+Deepfakes+of+Intimate+Images+Act%22%7D.

[20] Rastogi J, 'Deepfake Pornography: A Legal and Ethical Menace | the CONTEMPORARY LAW FORUM' (*THE CONTEMPORARY LAW FORUM*15 October 2023) <https://tclf.in/2023/10/16/deepfake-pornography-a-legal-and-ethical-menace/#:~:text=India%2D%20There%20is%20no%20distinctive,create%20liability%20against%20the%20perpetrators.> accessed 24 May 2024.

[21] 'Cybercrime - Prosecution Guidance | the Crown Prosecution Service' (*Cps.gov.uk*31 January 2024) <https://www.cps.gov.uk/legal-guidance/cybercrime-prosecution-guidance> accessed 24 May 2024

United Kingdom

The Computer Misuse Act 1990 ('CMA1990') is the main United Kingdom legislation relating to offences or attacks against computer systems such as hacking or denial of service[22]. In the technological era, various other offences like, disclosing private sexual images without consent, cyber stalking and harassment, and coercive and controlling behaviour crimes are predominately but not exclusively perpetrated against women and girls, with online activity being used to humiliate, control, and threaten as well as plan and orchestrate acts of violence

Similar to online romance fraud, offenders may arrange to meet a victim with the intention of committing rape or other sexual offences, using social media or online dating services as a means of facilitating their crime under the Sexual Offences Act of 2003. In 2013, the End Violence Against Women Coalition (EVAW) gathered accounts at a roundtable on the enforcement and prosecution of 'violence and harassment' online, reporting concerns that criminal justice authorities took a different, and less effective, approach to violence and harassment perpetrated online compared to offline[23].

In 2009, the U.K. launched the National Centre for Cyberstalking Research (NCCR), aims to provide research and analysis into the prevalence, motivations, impacts, and risk assessment of cyber violence against women and girls. In 2011, the centre published the results of a study on the prevalence, nature, and impact of cyber stalking[24] and is currently conducting a survey investigating the impact and prevalence of revenge porn.

The Data Protection Act of 2018 (DPA 2018) is the UK government's primary law on personal data processing in the UK, which is enforced along with the UK General Data Protection Regulation[25]. It serves as a data protection framework that regulates all aspects of how companies, organizations, and government agencies control and process personal data. The DPA 2018 requires all UK data controllers (companies and organisations that manage the processing of personal data) to establish and maintain appropriate security measures to protect personal data.

The Online Safety Act of 2023 enacted by UK parliament for the protection from online crime and regulate internet and online safety. It is one of the British legislation that contain provision to penalize "downblousing" and deepfakes porn[26]. The legislation was made with the intent of making UK 'the safest place to be online'. The Bill states that the perpetrators will face severe prosecution irrespective of the fact whether the creator intended to cause distress or humiliation to the victim. Part 10 of the Act, which comes into force on 31 January 2024, introduces a number of new "*communication offences*" for users who send harmful messages on a social media platform, messaging service, dating app or by "*airdrop* ". The new communication offences will apply to users variously across the home nations. Part 10 of the Act will have retrospective effect and include section 187 and 188 of the Act (to be inserted into the Sexual

[22] Ibid

[23] 'New Technology: Same Old Problems Report of a Roundtable on Social Media and Violence against Women and Girls End Violence against Women Coalition' <https://www.endviolenceagainstwomen.org.uk/wp-content/uploads/Report_New_Technology_Same_Old_Problems.pdf>

[24] Maple C, Short E and Brown A, 'Cyberstalking in the United Kingdom: An Analysis of the ECHO Pilot Survey' [2016] Openrepository.com <https://uobrep.openrepository.com/handle/10547/270578> accessed 24 May 2024

[25] 'List of Cybersecurity Laws and Regulations in the UK | UpGuard' (*Upguard.com*2024) <https://www.upguard.com/blog/cybersecurity-laws-regulations-uk> accessed 24 May 2024

[26] 'News, Sport and Opinion from the Guardian's Global Edition | the Guardian' (*Theguardian.com*24 May 2024) <https://www.theguardian.com/international> accessed 24 May 2024.

Offences Act 2003): the offences of sending or threatening to send unsolicited images of a sexual nature (including "***deepfake***" images) or intimate videos[27]**.**
These offences cover communications via social media, dating apps or device-to-device sharing. Offenders will face a custodial sentence of up to 2 years, and a fine. The offences created by the Act target the growing trend of online and digital abuse and aim to create a safer online environment. To date, prosecutors have tended to combat these activities by reference to established common law offences or statutory offences such as harassment, which are not fit for purpose for some online conduct.

LEGAL FRAMEWORK ON DEEPFAKES PORNOGRAPHY IN INDIA

The Information Technology Act of 2000 plays a crucial role in addressing computer-related crimes, but it does not specifically deal with deepfake pornographic content against women. Section 66D of the IT Act specifically addresses instances where a communication device or computer resource is used with malicious intent for cheating and personation[28][29]. This provision pertains to cases where individuals are manipulated into saying or doing actions through technology, leading to fraudulent activities[30]. Furthermore, the use of deepfakes for the invasion of privacy is addressed under Section 66E of the Information Technology Act of 2000. This section outlines the violation of privacy that occurs when deepfakes are employed to capture, publish, or transmit someone's intimate pictures or videos without their consent[31].

Deepfakes containing explicit or pornographic content fall within the purview of Section 67A and 66B of the Information Technology Act of 2000. These sections delineate fines and penalties for the publication and transmission of sexual and explicit content involving both adults and children. Notably, various platforms, including Pornhub, have implemented bans on deepfake sexual content to comply with these legal provisions. The liability of intermediaries, the platforms where deepfake content is often posted, is regulated by Section 79 of the Information Technology Act of 2000. According to this section, intermediaries are required to take down content either upon realization or knowledge of its presence or upon receiving a court order. In the case of Myspace Inc. v Super Cassettes Industries Ltd[32] the court emphasized that intermediaries must promptly remove infringing content following notifications from private parties in cases of copyright infringement, even without a court order.

With the advent of the Information Technology Rules in 2021, Social Media Intermediaries (SSMIs) are subject to additional regulations. SSMIs, which include intermediaries with registered users above a specified threshold, are mandated to appoint personnel responsible for monitoring and identifying the originator of information and specific types of content. The rules also establish a grievance settlement mechanism for intermediaries to address user complaints and grievances, ensuring a more robust framework for managing content-related issues.

[27] 'Online Safety Act 2023' (*Legislation.gov.uk*2023) <https://www.legislation.gov.uk/ukpga/2023/50/enacted> accessed 24 May 2024

[28] 'A Peep into the Future of AI: The Bletchley Declaration and International Collaboration for AI Safety' (*INDIAai*2023) <https://indiaai.gov.in/article/a-peep-into-the-future-of-ai-the-bletchley-declaration-and-international-collaboration-for-ai-safety> accessed 24 May 2024

[29] Section 66D of IT Act states "punishment for cheating by personation by using computer resource" stated "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."

[30] Ibid

[31] Information Technology Act, 2011, s. 66E

[32] Neutral Citation: 2016: DHC:8178-DB

Prior to the adoption of the Digital Personal Data Protection Act of 2023 (DPDP Act), India lacked a comprehensive data protection law. As a result, data protection was regulated by the Information Technology Act (IT Act) of 2000, which provided legal recognition for transactions conducted via electronic data interchange and other forms of electronic communication, commonly known as "electronic commerce.[33]" With the advancement in the technological development, these amendments in IT Act become ineffective for the protection of the personal data. Therefore, parliament enacted Digital Personal Data Protection Act of 2023 (DPDP Act), a separate or comprehensive Act, "to protect digital personal data in a manner that recognises both the right of individuals to protect their personal data and the need to process such personal data for lawful purposes and for matters connected therewith or incidental thereto[34]".

The two more important definitions under the Act are that of 'personal data' and 'personal data breach.' Personal data under the act is defined as any piece of data relevant to a person which can be used to identify them. The use of the phrase 'any piece of data' widens the ambit of this definition to a large extent. This interpretation can be borrowed from the interpretation of the term 'any information' used in the definition of personal data under the EU Data Protection Laws. Even a deepfake itself can be covered under the definition of personal data because it can be used to identify the person being featured in it. A personal data breach under the act is defined as "Any unauthorised processing of personal data or accidental disclosure, acquisition, sharing, use, alteration, destruction or loss of access to personal data, that compromises the confidentiality, integrity or availability of personal data."

Further, this act was enacted to provide protection to personal data, but this act does not specifically deal with the deepfake pornographic content against women.

IMPLICATIONS OF WOMEN'S PRIVACY

Deepfakes, as a technological phenomenon, involve the manipulation of an individual's identity, face, or facial features, resulting in a concerning violation and encroachment upon the right to privacy enshrined in Article 21 of the Constitution of India. This breach extends beyond the traditional boundaries of physical and spatial privacy, incorporating the safeguarding, preservation, and appropriate management of personal information. Over the years, the judiciary in India has demonstrated a vigilant and inclusive approach, acknowledging the significance of recognizing, protecting, and preserving the right to privacy as an inherent aspect of fundamental rights within a democratic state.

In alignment with the principles laid out in the Constitution of India, the concept of privacy has undergone significant evolution both horizontally, within the individual, and vertically, establishing the relationship between the state and the individual[35]. Horizontally, the right to privacy has expanded to include aspects such as sexual autonomy, recognizing the individual's autonomy over their personal choices. Vertically, it imposes a crucial obligation on the state to ensure the protection and conservation of the right to privacy for every citizen. The right to privacy, as revealed through the constitutional framework, is integral to the broader canvas of fundamental rights, harmonizing with the right to life, personal liberty, and the various

[33] Sarvagya Chitranshi, 'The "Deepfake" Conundrum - Can the Digital Personal Data Protection Act, 2023 Deal with Misuse of Generative A' (*IJLT*23 December 2023) <https://www.ijlt.in/post/the-deepfake-conundrum-can-the-digital-personal-data-protection-act-2023-deal-with-misuse-of-ge> accessed 24 May 2024

[34] Digital Personal Data Protection Act of 2023 (Act no. 22 of 2000)

[35] Vasist P and Krishnan S, 'Deepfakes: An Integrative Review of the Literature and an Agenda for Future Research' (2022) 51 Communications of the Association for Information Systems <https://iimk.ac.in/uploads/faculty/CAIS_20220810062848..pdf>

freedoms guaranteed under Articles 19 and 21 of the Constitution. This underscores the constitutional significance of privacy in the democratic fabric of India. Further, in Puttaswamy case, 9 judge bench, delivered cornerstone of the 'Right to Privacy' jurisprudence in India. The court held that the right to privacy as a fundamental right under the Constitution of India. The Court held that the right to privacy was integral to freedoms guaranteed across fundamental rights, and was an intrinsic aspect of dignity, autonomy and liberty. In the words of court, "**t***he right to privacy is inextricably bound up with all exercises of human liberty – both as it is specifically enumerated across Part III, and as it is guaranteed in the residue under Article 21. It is distributed across the various articles in Part III and, mutatis mutandis, takes the form of whichever of their enjoyment its violation curtails.*[36]**"**
Drawing inspiration from the pivotal Puttaswamy judgment, the Supreme Court, in the case of Indian Hotel and Restaurant Association (AHAR) v. The State of Maharashtra[37], addressed the issue of privacy in the context of data stored in CCTV footage. The court asserted that the data captured through complete surveillance of activities within premises, such as dance bars, through CCTV cameras is excessive and disproportionate. The court also highlighted that monitoring, recording, storage, and retention of dance performances can lead to an unwarranted invasion of privacy, posing threats and potential blackmail, especially to women bar dancers. This case establishes a precedent acknowledging that CCTV footage, as a source for identifying individuals, constitutes personal information, invoking the right to privacy. The legal landscape in India recognizes the multifaceted nature of privacy, encompassing not only physical and spatial dimensions but also the protection of personal information. As technology evolves, the judiciary remains crucial in adapting legal principles to address emerging challenges, ensuring that fundamental rights, including the right to privacy, are robustly protected in the digital age.

CONCLUSION AND SUGGESTIONS

The rise of deepfakes and their impact on women in India is a concerning issue that demands immediate attention and action. This essay has presented significant findings on the harm caused by these manipulated videos and their implications for society. It is evident that cybercrimes are on the rise, and they pose a significant threat to vulnerable groups, particularly women. Therefore, it is crucial for effective legal measures to be implemented and for increased vigilance from both government agencies and technology companies to address this issue. The safety and protection of individuals, especially women, must be a top priority in the face of emerging threats like deepfakes. It is essential for legislation to keep pace with advancing technology to combat this form of digital violence. The rise of deepfakes has had a detrimental effect on women in India, with these manipulated videos often featuring their faces and bodies in a sexualized or degrading manner without their consent. As a result, these women face humiliation, harassment, and even threats in their personal and professional lives. This not only violates their privacy and dignity but also perpetuates harmful gender stereotypes and reinforces the objectification of women. To combat deepfakes, there is a need for legal measures to be in place. The Indian Penal Code and the Information Technology Act have provisions that can be used to prosecute individuals who create and distribute deepfake videos. However, there is a need for more specific and comprehensive legislation that explicitly addresses deepfakes and their impact on individuals. This can include provisions for stricter penalties and punishment for those involved in creating and sharing deepfakes. In addition to legal measures, there should be a concerted effort to educate and raise awareness among the public about

[36] Justice K.S. Puttaswamy (Retd.) & Anr. vs. Union of India & Ors AIR 2017 SC 4161
[37] Writ Petition (Civil) No. 793 of 2014

deepfakes and their potential harm. This can help individuals recognize and report deepfakes, thereby reducing their spread and impact.

It is also crucial for technology companies to take responsibility and actively work towards preventing the creation and distribution of deepfakes. This can include implementing stricter content moderation and detection algorithms, as well as collaborating with law enforcement agencies to identify and remove deepfakes. Social media platforms, in particular, have a significant role to play in addressing the issue of deepfakes. They should have clear and accessible reporting mechanisms for deepfakes and provide support to victims who have been affected by these malicious acts.

The existing laws under the IT Act of 2002 are inadequate in addressing this issue, and stricter regulations must be implemented to effectively prevent and address these heinous crimes. Law enforcement agencies must also be equipped with the necessary tools and training to identify and handle cases involving deepfakes. This includes developing specialized skills and expertise in detecting and dealing with deepfake content. Additionally, there is a pressing need for greater awareness among society about the severe repercussions of creating or sharing such harmful content targeting women. It is crucial to educate individuals about the impact of these acts, not only on the victims but also on society as a whole. Moving forward, further research must be conducted to explore effective ways to combat deepfake-related crimes against women. This could involve developing technological solutions such as detection software or collaborating with social media platforms to promptly flag and remove harmful content. It is also crucial to note that the penalties for perpetrators who create or distribute such content should be significantly increased as a deterrent.

Furthermore, these platforms must have strict policies in place to prevent the spread of deepfakes and take swift action to remove them. It is also essential to understand the underlying reasons for the rise of deepfakes in India. Factors such as the patriarchal society and the objectification of women contribute to the creation and spread of these manipulated videos. Therefore, there is a need for a deeper societal shift in attitudes towards women and their rights.

In conclusion, deepfakes in India are a pressing issue that demands immediate action. By implementing legal measures, increasing awareness, and holding technology companies accountable, we can prevent and mitigate the harmful effects of deepfakes and protect the rights and dignity of individuals, especially women. All stakeholders must work together to combat this form of digital violence and create a safer online environment for all individuals.

This will send a strong message that such actions will not be tolerated and will face severe consequences. It is essential for lawmakers and policymakers to urgently address this issue before it becomes even more widespread in Indian society. The potential for harm towards women through deepfake technology has already been demonstrated, and swift action must be taken to prevent it from escalating further into an uncontrollable problem. All things considered, it is evident that stronger measures are necessary at all levels - legal, technological, and societal - to combat the impact of deepfakes on gender-based violence against women in India. Only through proactive efforts can we ensure a safer environment for all individuals, regardless of their gender identity. The protection and safety of women must be prioritized, and it is the responsibility of society as a whole to take a stand against deepfake-related crimes.