

Deepfake, Cyberstalking, and Virtual Sexual Harassment: Emerging Challenges to Women's Digital Rights and Safety

Ms. Gouri Chakraborty¹ & Dr. Vidushi Puri²

¹Ph.D Scholar, Amity Law School, Amity University, Haryana

²Assistant Professor, Amity Law School, Amity University, Haryana

Abstract

Technology innovation and development of artificial intelligence have not only revolutionized communications and social interactions, but also resulted in emergence of new types of technology-enabled violence against women. For instance, technology is utilized to produce and distribute deepfake pornography, conduct cyberstalking and perpetrate virtual sexual harassment. In this respect, the issue raises questions about women's privacy, dignity, autonomy, and security online. This paper explores the phenomenon and nature of technology enabled violence against women, focusing especially on deepfake pornography, cyberstalking, and virtual sexual harassment. It also analyses the implications of these kinds of abuses for women's digital rights- right to privacy, dignity, equality, and freedom of expression. The paper draws attention to the problems of rapid technological development, jurisdiction, and anonymity of perpetrators, evidence gathering, and platform liability. Further on, the issues related to technology development, jurisdiction problems, and offenders' anonymity, evidentiary issues and digital platform responsibility are discussed in regard to these forms of violence. As a result of the growing dependence of people on digital tools for interacting, learning, working, and socializing, women have been subjected to more cases of violence enabled by the use of modern technology. Misuse of artificial intelligence and other evolving digital technologies has opened up new avenues of abuse that are hard to notice, manage, and prevent. These not only violate the rights of individuals but also hinder efforts towards gender equality, digital access, and social justice. Continuous online victimization keeps women from actively engaging in digital spaces and exploiting their digital potential. The solution to such problems would entails a combination of both innovation and regulation.

Keywords: Deepfake Pornography, Cyberstalking, Virtual Sexual Harassment, Technology-Facilitated Violence Against Women, Digital Rights, Privacy, Artificial Intelligence.

Introduction

Internet has become one of the most significant technological advancements of the present-day world that has brought about revolutionary changes in the means of communication, information acquisition, doing business, and participating in politics and society in general. Often referred to as "a global village," the internet has erased the boundaries of the geographical world and opened up unparalleled possibilities in terms of education, work, entrepreneurship, advocacy, and socializing. The Internet has allowed people to voice out their views and takes part in discussions and social and political activism. The advent of social networking sites like Facebook, Instagram, X, LinkedIn, and many others dating websites has paved the way for interactive and participative digital communities.¹

While there are many benefits that exist in the digital world, there are still many threats and problems that exist in this realm as well. In many cases, online sites and forums become places where people encounter instances of aggression, harassment, discrimination, and different types of cybercrime. Individuals who hold an opposing opinion or who voice their disagreement with the popular view are subjected to

harassment, threats, and exclusion from participation in digital forums. Technological advancement has surpassed the creation of legal and other mechanisms for protecting Internet users, which makes it difficult to track down those responsible for cybercrimes.² Digital victimization has emerged as an important issue in modern times. While it is true that cybercrime had always existed since the advent of technology, academic and legal researches have always paid more attention to the problem of criminality and efforts to identify and apprehend perpetrators than the issue of victims and its repercussions. Digital victimization refers to the broad spectrum of online activities that harm the privacy, safety, dignity, and well-being of people.

Victimization is experienced by both men and women in the digital sphere; but studies have found that women suffer more from different kinds of cyber abuse than men. The rising cases of cyberbullying, cyber stalking, photo tampering, pornographic deepfakes, voyeurism, sexual harassment in cyberspace, and unauthorized sharing of intimate pictures portray the gendered aspects of digital violence. Social media sites, being accessible and widespread, frequently serve as a chance for offenders to victimize women via activities grounded in gender discrimination.³ There are many examples from around the world, including India, that prove how technological. Examples include cyber bullying, stalking, hacking, phishing, identity theft, and online fraud. Moreover, the increased use of social networking sites has created room for newer forms of online abuse in the form of trolling, creating fake online identities, image morphing, cyber defamation, sexual exploitation online, and harassment using technology. This clearly demonstrates the necessity for the need to respond legally and technologically against the rising issue of digital violence.

The fast pace of development of artificial intelligence and other forms of digital technologies have made worries about online harassment and victimization even more pressing. New types of technology-enabled violence that is associated with deepfake porn, cyber-stalking, and online sexual harassment have emerged as serious dangers for women's privacy, dignity, and safety in cyberspace. In these cases, perpetrators use digital and safety in cyberspace. In these cases, perpetrators use digital technologies to harass, intimidate, and monitor their targets and to spread manipulated or sexually charged material with their victims' consent. Such acts can lead to significant consequences including traumatization, damage to reputation, social isolation, and limited involvement in cyberspace. With the increasing number of women turning to digital platforms for learning, working, socializing and politics, the need for legislation becomes even more relevant.⁴

Conceptual Framework for Technology-Enabled Violence against Women

Violence against women facilitated by technology (TFVAW) describes violence carried out via digital technologies where the target group is predominantly women and girls. TFVAW includes such acts as cyberstalking, harassment on the internet, image-based sexual abuse, cyberbullying, and non-consensual distribution of intimate images and technology-assisted coercive control. The UN and other intergovernmental organizations acknowledge technology-facilitated violence as an extension of gender-based violence off-line. Technologies do not cause gender discrimination; they simply highlight the pre-existing structural inequalities and discrimination. Therefore, violence perpetrated using digital technologies should be seen as one end of the violence against women spectrum.⁵

There are several differences between technology-enabled violence and conventional violence. Firstly, technology allows perpetrators to target their victims quickly and continuously. Secondly, violent materials can spread worldwide almost immediately. Thirdly, anonymity and encryption prevent authorities from identifying and prosecuting offenders. Fourthly, digital materials may be preserved for an indefinite amount of time. The effects of technology-enabled violence on human rights are serious. It is because it violates people's rights to privacy, dignity, equality, freedom of expression, and physical safety. Victims of online harassment tend to avoid being active in cyberspace, which makes them less democratic.

Deepfakes: A New Form of Image-Based Sexual Abuse

The word Deepfake is a blend of "deep learning" and "fake". It is form of manipulated audio, video or image content generated using artificial intelligence and machine learning tools. Deepfake can manipulate one's face, voice, or movements in order to make the fake content seem realistic. Although there are valid

applications of such technologies in areas such as entertainment, production of media content, and education, it is now being used maliciously for creating non-consensual pornographic material, spreading false information, identity theft, and fraudulent activities. Unlike conventional editing, contemporary AI software can help people create realistic deepfake content even without any experience.⁶

The deepfakes refer to images, videos, or audio clips that are made using the artificial intelligence and deep learning technology. The technology is capable of creating very real images such that it becomes hard to tell between what are real images such that it becomes hard to tell between what is real and what is not real. Although there are positive uses of deepfakes like in the entertainment, education, and media production sectors, their misuse has been on the rise. Women have especially been on the rise. Women have especially been affected as their images have been altered using the technology to fit in pornographic films without their consent. This goes against their privacy, dignity, and autonomy, leading emotional, social, and reputation harm.

Application of Deepfake Technology

Deepfake technology has become a very sophisticated AI technology with diverse uses across various industries. Depending on the intentions behind its deployment, deepfake technology may have either positive or negative implications. Some of the ways that deepfake technology has helped positively are through innovations in entertainment, education, medicine, digital marketing, virtual reality, and content creation through the provision of realistic audio-visual content and increased user experience. The technology has however been increasingly used for inappropriate reasons and sometimes illegal activities such as creation of fake news, identity fraud, political manipulation, propaganda, and pornography. Such inappropriate uses of the technology may have far-reaching consequences like damage to reputation, emotional trauma, violation of privacy, financial loss, and loss of confidence in digital information. Considering the wide spread of social media and online communication channels, misuse of deepfake technology has been magnified through the sharing of manipulated content among huge numbers of people within a short period. As a result, those individuals who actively participate in digital environments are more prone to deepfake technology risks. However, despite these limitations, the controlled and responsible application of deepfake technology is a dual-purpose innovation that should be harnessed for its positive applications while being appropriately countered for any abuse.⁷

Negative Application of Deepfake Technology

Even as an innovative technology, deepfake technology is increasingly being abused for unethical purposes. Deepfake technology has been increasingly applied to produce non-consensual pornography against individuals, mostly women and celebrities, resulting in significant reputational damage. Moreover, deepfakes can be applied for malicious purposes, including blackmailing, identity theft, fraud, and spreading misinformation. Deepfakes have been extensively applied in the politics sector by creating doctored videos of politicians and world leaders to influence public opinion. Deepfakes can be circulated quickly on social media sites, thus making them a huge threat to the modern society.⁸

Positive Application of Deepfake Technology

In spite of being misused, there are quite a few uses of deepfake technology that are helpful in different industries. In the creative world, including the entertainment industry, deepfakes are used in order to enhance movies, create digital arts, and provide interaction possibilities for audiences. Enterprises and advertisers use deepfakes for the development of personalized and interesting content, while the movie industry enjoys decreased production costs and advanced special effects. Deepfakes can also serve the purpose of providing immersive educational experience in recreating the images of historic characters or situations. There are also promising possibilities for healthcare with deepfakes being able to generate synthetic data for research purposes while preserving privacy of patients. Moreover, there are deepfake AI systems that can be used for awareness campaigns, raising money for certain purposes, multilingual communication, and personalized news delivery services.⁹

Concluding Remarks

Deepfake technology is a very promising invention that is based on artificial intelligence and can be applied not only for good but also for bad purposes. On the one hand, there are plenty of benefits that deepfake technology provides for entertainment, education, medicine, and digital communications. On the other hand, its inappropriate application can lead to many dangerous consequences such as deepfake pornography, stealing identities, frauds, and misinformation. Women are especially at risk of the abuse of deepfake technology that can threaten their privacy, dignity, and honour.

Cyberstalking: Persistent Digital Surveillance and Harassment

Cyberstalking is defined as an online harassment activity that uses digital technology to stalk another person repeatedly through threatening, intimidating, harassing or monitoring without permission. Cyberstalking can involve activities such as persistent messaging, dissemination of false information, defaming on the web, sexually harassing others, identity theft and more which are meant to cause fear, distress and emotional trauma to the victim. In certain cases, cyberstalking can even escalate from cyberspace and move towards physical stalking which may become dangerous for the victim. As it causes negative effects, cyberstalking is considered a criminal offense in many nations and is punished under cybercrime laws, harassment laws, and stalking laws. Actress Patricia Arquette was known to have removed her Facebook account in 2011 because of an online stalker. Following safety precautions, she reduced communication with fans to Twitter and asked people to make friends only with those whom they personally know¹⁰.

Women are increasingly being cyberstalked on social media sites, emails, messaging apps, and other digital technologies. Offenders frequently monitor women's online activity, sending threatening or abusive messages, creating phony profiles, spreading false rumours, and sharing intimate or modified photographs without their consent. In some situations, cyber stalkers may infiltrate accounts to gain access to personal information, photos, and contacts, increasing the danger of harassment, blackmail, and identity theft. Many women are unaware that they are constantly monitored online, until the harassment increases. The exploitation of personal information available on digital platforms can expose women to emotional anguish, reputational harm, privacy violations, and even offline intimidation, making, cyberstalking a significant danger to women's safety and autonomy in the digital age.¹¹

Forms of Cyberstalking

Unauthorized surveillance: Continuous observation or gathering of information about the online activities, personal data, or whereabouts of a particular individual without their consent.

Recurrent unwanted contact: Consistent communications through messages, emails, phone calls, or other means despite the requests of the individual to cease these contacts.

Cyber-stalking on social media platforms: Constant monitoring of the victim's social media accounts and online interactions on these sites.

Online harassment: Continuous communication or messaging through threatening, intimidatory, or abusive language that causes fear, stress, or emotional distress to the individual.

Bullying and Cyberstalking: Combining both behaviours to inflict greater psychological harm to the victim and gain control over them.

Distribution of intimate content without consent: Sharing of private or sexually explicit images or videos with the aim to humiliate, seek revenge, or exert pressure on the target.

Location and GPS surveillance: Using digital devices and applications to track the physical locations of a person without their knowledge.

It is very important to recognize all these different types of cyberstalking in order to be able to prevent and address such victimizations properly. With further advancements in technology, more and more techniques of cyberbullying will probably become evident.¹²

Concluding Remarks

Cyberstalking has become one of the major issues in the rapidly growing digital world in India, and there are serious threats to individual security and mental well-being. The issue needs to be addressed using different methods such as law, enforcement, public awareness, protection technology, and victim services. Collaboration between various government departments and law enforcement authorities along with other concerned parties is required to provide safety in the cyberspace. With the rapid evolution of technology, constant vigilance and education will be necessary to counter this crime in the future.

Online Harassment against Women

Rapid advancements in digital technologies and social media have made it possible for many women to engage in cyberspace. However, despite these advancements that make it possible for one to communicate, learn, and gain knowledge, women have been victimized by harassment online. Online harassment of women is unwanted, offensive, threatening, or abusive acts committed through cyberspace in order to intimidate, humiliate, or silence women. It encompasses actions like cyberstalking, sexually abusive threats, sending harassing messages or emails, trolling, doxing, unauthorized dissemination of intimate images, and gender-based hate speech. The extensive reach of cyberspace and anonymity accorded to the perpetrators make it easy for one to harass someone online, putting women at risk of abuse on the internet.¹³

Sexual harassment has always been viewed as a grave violation of a person's dignity and right to privacy. When such behaviour takes place through digital medium and via online communication, the act is known as cyber harassment. Cyber harassment can include threatening behaviour, bullying, and blackmailing, unwanted sexual proposal, and many other kinds of offensive behaviour that take place towards women in cyberspace. In India, protection from sexual harassment has been given under Section 354A of the Indian Penal Code where offenses like touching someone in an offensive manner, asking for sexual favours, making any kind of obscene remarks or showing any kind of pornographic matter have been made punishable.¹⁴

The rapid development of digital technology has also led to the development of some other types of offences that have been committed through the use of digital devices, such as voyeurism, cyber stalking, doxing, creepshots, revenge porn and cyber flashing. Most people who use the internet do not know much about the meaning and significance of these crimes since they have developed quite recently. Moreover, the outbreak of the COVID-19 pandemic has intensified the reliance on digital technology and brought about new types of offenses committed in the cyberspace, such as "Zoom bombing".¹⁵

Acknowledging the dynamic nature of the threats in the digital environment, the Indian government is contemplating the enactment of the Digital India Bill, 2023, which will act as a replacement for the Information Technology Act of 2000. The new bill aims at bringing forth a regulation regime for enhancing accountability and ensuring safe digital governance. It addresses various challenges pertaining to artificial intelligence, social media algorithm, and intermediary liability, new technologies, and user protection in the digital environment.¹⁶

Concluding Remarks

Harassment of women through the Internet has become a significant problem in the modern era, posing threats to women's privacy, dignity, safety, and equal rights to use the Internet. In addition to the growing problem of cyber stalking, cyber harassment, doxing, revenge porn, and cyber flashing, there are many other forms of technologically facilitated violence that have raised alarms about women's vulnerability to such attacks in the Internet world. Despite the existence of some laws in India that prohibit sexual harassment of women and any form of cybercrime, technological innovations continue creating new

problems for law making bodies in India. Thus, there is a need for effective enforcement of existing laws, digital literacy, awareness programs, victim assistance mechanisms, and the enactment of necessary legislation to combat harassment in cyberspace.

Impact on Women's Digital Rights and Safety

Technology-enabled abuses such as deepfake pornography, cyberstalking, and virtual sexual harassment have radically changed the definition of violence against women in the digital era. Despite the fact that technology-enabled violence occurs through the use of the internet and technology itself, its impact the lives of victims on a personal, social, economic, and psychological level. Victims of technology-enabled violence are likely to suffer from anxiety, depression, fear, trauma, decreased self-respect, social isolation, and others. The non-consensual creation and distribution of deepfake materials, constant cyberstalking, and online sexual harassment may seriously harm the reputation of a woman, her career, and relationships with people. Often victims of technology enabled violence stop using social networks, avoid participating in public life, and do not express their opinions due to fear of being victims again.¹⁷

Scholarly inquiry into violence against women facilitated by technology and online has identified it as critical human rights challenge rather than just a concern related to cybercrimes. According to Rigotti and McGlynn, digital violence is entrenched in pre-existing gender inequality and represents a grave violation of the rights of women in the broader context. Similarly, recent academic work on technology facilitated sexual violence highlights the role of digital space as a site where gender hierarchies are perpetuated and women are denied opportunities to participate socially, politically, and professionally. With the increasing application of artificial intelligence and advanced technologies, the scope and severity of technology-facilitated violence against women have increased even further in forms such as deepfake pornography and image-based sexual abuse.¹⁸

Violation of Privacy and Data Protection

The right to privacy can be said to be one of the fundamental rights that are highly affected by the use of technology to commit acts of violence against women. In an age when information has become highly digitized, personal information, images, videos, locations, and even activities done on the internet become highly vulnerable to any form of illegal use. The use of deepfake pornographic materials is definitely one of the violations of privacy where one is forced to give consent for their likeness to be used in creating pornography. Recent research indicates that the practice mainly affects women.

In the same way, cyberstalking violates a person's right to privacy due to continuous monitoring, surveillance, and collection of private information on social networking sites, online communications, and online databases. Cyber-stalking results in fear, stress, and feeling vulnerable all the time, thus inhibiting women from being able to use digital space in a safe manner. Virtual sexual harassment is even more detrimental to violating one's right to privacy because it entails the dissemination of intimate photos or sexually explicit messages or any form of private information. Since digital data can easily be duplicated, recorded, and shared on online platforms, it often becomes difficult for the victim to control his/her private information. According to Rigotti and McGlynn, technology-mediated violence against women must be regarded as a matter of human rights because it infringes upon women's rights because it infringes upon women's rights to privacy, respect, equality, and safety within the digital world.¹⁹

Threats to Human Dignity and Personal Autonomy

The increasing menace of deepfake pornography, cyber stalking, and online sexual harassment is a major threat to the honor and autonomy of women in the digital age. This abuse through technology takes away any autonomy that women have regarding their identity, choices, and online presence. Women are subjected to false portrayals of themselves in sexually explicit situations by means of the production of deepfakes which is not consensual, thereby affecting their reputation and sense of self-respect. Similarly, cyber stalking and harassment of women online involve the monitoring and intimidation of women from

expressing themselves or engaging in online space. The loss of autonomy involves losing control over one's personal information, pictures, and decision making abilities. Therefore, technology abuse not only has psychological consequences but also has implications on values such as honor, autonomy, freedom, and equality protected by the Indian Constitution.²⁰

Indian Constitutional Perspective

The Constitution of India safeguards human dignity, liberty, and privacy by virtual of Article 14, 19, and 21. The right to live with dignity has been accepted as part and parcel of the right to life and liberty guaranteed under Article 21. Technology-enabled violence against women including Deepfake porn, cyberstalking, and virtual sexual harassment is in direct violation of the constitutional provisions that ensure dignity, privacy, and freedom of expression of the woman. In *K.S. Puttaswamy v. Union of India* (2017)²¹, the Supreme Court has upheld that the right to privacy, bodily autonomy, and dignity of the individual. The exploitation of women through technology thus amounts to a grave violation of the rights guaranteed under the constitution. This form of online harassment not only impacts the dignity and autonomy of women but also their liberty to engage freely in digital spaces. Hence, protecting women from technology enabled violence becomes imperative for the proper enforcement of constitutional principles of equality, liberty, dignity, and privacy.

Constraint on Freedom of Expression

Use of deepfake pornography, cyberstalking, and virtual sexual harassment discourages women from taking part in any kind of activity in the digital environment. The fear of being harassed, threatened, and having one's reputation damaged makes women reluctant to give opinions and contribute to any public conversation. Women journalists, activists, academicians, and other public personalities in particular are targeted in online abuse campaigns that intend to silence them.²²

Psychological and Emotional Impacts

There are significant psychological impacts on victims as a result of technology-assisted violence. Victims of deepfakes, cyberstalking, and online sexual harassment often go through emotions such as anxiety, depression, psychological distress, shame, and lack of self-respect. The continuous occurrence of online attacks may cause fear, vulnerability, and powerlessness. In extreme cases, victims may become socially isolated and have suicidal behaviours.²³

Social and Economic Impact

The consequences of digital violence can be felt strongly on both the social and economic fronts by women. Digital violence such as deepfakes can cause damage to reputation, which results in social stigmatization and damaged interpersonal relations. The victims might find it hard to pursue their careers or get employed due to online abuse and manipulation. Moreover, the time wasted in combating abuse, protecting oneself from hackers and seeking legal redress might have an adverse effect on productivity and economic well-being.²⁴

Artificial Intelligence and Rapid Technological Change

The first one is the constant development of AI technology itself. The programs for creating deepfakes have already been perfected, became cheaper and easier to use. People with no prior knowledge about the topic can create deepfakes with the help of special software. There are problems with keeping pace between legal system and technology development. Some of the current laws on the matter were created long ago and do not refer directly to the modern types of digital abuse. Therefore, judges should find ways to interpret them correctly. At the same time, lawmakers find themselves facing the challenges of making laws up-to-date without having them outdated in a couple of years²⁵.

Jurisdictional Challenges

Violence through technology often involves crossing national frontiers, thereby raising jurisdictional problems. The creation, upload, and distribution, of deepfake images can occur in several nations, making any investigations difficult. Legal differences also pose a problem to the process.²⁶

Offender Anonymity

Online perpetrators have the ability to hide their identity through anonymous online profiles, encryption, and virtual private networks (VPNs). The anonymity gives the perpetrators the capacity to indulge in cyber-stalking, online sexual harassment, and the sharing of deepfake pornographic content without being detected.²⁷

Evidence Issues

Collecting evidence of crimes is quite difficult. It is due to the fact that the information can be altered, deleted or distributed on different platforms. Detecting deepfake pornography content needs a special kind of forensic investigation that would prove the falsity of the content as well as the harm caused to the victims.²⁸

Platform Liability

Digital platforms serve as the main platform for spreading the abusive content online. Despite the fact that social media sites and other online service providers have the capacity to identify and eliminate the abusive content, deciding about the degree of the responsibility of these platforms is rather challenging.²⁹

Underreporting and Stigmatization

A number of cases of technology-mediated violence against women do not get reported owing to fear of stigmatization, victim blaming, reprisals, and public disclosure. Societal pressure makes it difficult for the victims to seek help through the law, causing underreporting of cyber-violence.³⁰

Need for a Coordinated Approach

Regulation of digital violence faces a number of hurdles that show how the law is not enough. The response needs to be a coordinated one that includes governments, tech companies, law enforcement bodies, academic institutions, and nongovernmental organizations.

Recommendations and Future Directions

The problem of deepfake pornography, cyberstalking, and virtual sexual harassment needs to be handling in an inclusive and collaborative manner. There is need for governments to create laws that will enable them to deal with deepfake abuses and cybercrimes that take place via the use of AI tools. Specific regulations and measures such as AI watermarking, transparency measures, and the deployment of technology to detect deepfakes should be employed in order to minimize their misuse. Cybercrime law enforcement should be improved through the creation of cybercrime units, enhanced forensic capacity, and regular training for the police, prosecutors, and judges. The victim-oriented approach should incorporate legal, psychological, and digital security aid, emergency services and rapid removal of content, cooperation with law enforcement agencies, and publication of transparency reports. In light of the transnational aspect of cybercrime, there is a need for increased international cooperation in areas of information exchange, mutual legal assistance, cross-border investigations, and collection of digital evidence. Last but not least, policy frameworks for digital governance ought to be gender-sensitive through promoting the involvement of women in policy formulation process and conducting research on technology and gender issues.

Conclusion

The rising cases of deepfake pornography, cyberstalking, and virtual sexual harassment prove that the form of violence perpetrated against women has changed with time through technology. The above- stated technology-enabled violence not only infringe on women's privacy, dignity, autonomy, and right to freedom of expression but also result in grave consequences that can be social, psychological, and economic. Although digital technologies give people an amazing platform to interact and exercise their freedoms and rights, these same technologies have led to the creation of new forms of exploitation and gender-based violence. Current legal regimes are often unable to cope with the changing technologies, which makes regulation difficult. Hence, tackling the growing dangers of technology-enabled violence against women needs an approach that comprises legislation, law enforcement, regulation, digital literacy, and victim services among others. It is imperative that women remain safe even when it comes to the digital environment because of the human rights aspect. In addition, the problem of violence against women through the use of technology is not only about regulating it legally but involves the wider process of societal transformation. In order to protect women from suffering from the negative effects of technology, it is important to raise awareness, enhance digital literacy skills, practice ethical use of artificial intelligence, and involve various stakeholders in the process. With the emergence of new technologies, the regulatory measures should be updated in order to tackle the problem of abuse. The protection of women from becoming victims of violence online is significant in order to provide them with equal rights to participate in education, work, discussion, and other areas of digital environment.

¹ Akanksha Pathak and Prateek Tripathi, "Digital Victimization of Women in Cyberspace: An Analysis of Effectiveness of Indian Cyber Laws", 7 *NLUA Law Review* (2023).

² *Ibid.*

³ Deeksha Saini, "Cyberstalking, Deep Faking and Harassment of Women: Legal Frameworks and Enforcement Challenges", *Lex Scripta Magazine* (May 14, 2026)

⁴ Laura Bates, "AI-powered Online Abuse: How AI is Amplifying Violence Against Women and What Can Stop It" (Nov. 18, 2025).

⁵ United Nations Entity for Gender Equality and the Empowerment of Women (UN Women), "Repository of UN Women's Work on Technology-Facilitated Violence Against Women and Girls (2025)".

⁶ Bahar Uddin Mahmud and Afsana Sharmin, "Deep Insights of Deepfake Technology: A Review", 5(1&2) *DUJASE* 13 (2020).

⁷ *Ibid.*

⁸ *Ibid.*

⁹ *Ibid.*

¹⁰ John Sammons and Michael Cross, "Beyond Technology—Dealing with People" in *The Basics of Cyber Safety: Computer and Mobile Device Safety Made Easy* (Elsevier, 2017) 179.

¹¹ Himanshi Menghani, "Cyber Crime Against Women in India: Legal Remedies and Persistent Challenges in the Digital Era", *Renaissance Law College* (10 June 2026).

¹² Rachna and Rahul Varshney, "Cyberbullying and Cyberstalking: Belongings and Anticipation Measures in India" (2024) 5(1) *ShodhKosh: Journal of Visual and Performing Arts* 1469, 1470.

¹³ European Institute for Gender Equality, *Combating Cyber Violence against Women and Girls* (European Institute for Gender Equality).

¹⁴ Radha Ranjan and Jivantika Gulati, "The Sexual Harassment against Women in Cyber Space: Concept, Reality and the Law" (2023) X(1) *Kashmir Journal of Legal Studies*.

¹⁵ *Ibid.*

¹⁶ *Ibid.*

¹⁷ Akanksha Pathak and Prateek Tripathi, "Digital Victimization of Women in Cyberspace: An Analysis of Effectiveness of Indian Cyber Laws", 7 *NLUA Law Review* (2023).

¹⁸ Carlotta Rigotti and Clare McGlynn, "Online and Technology-Facilitated Violence against Women: The EDVAW Platform's Contribution to Human Rights Protection and Monitoring" (2025) 43(2) *Netherlands Quarterly of Human Rights*.

¹⁹ *Ibid.*

²⁰ Radha Ranjan and Jivantika Gulati, "The Sexual Harassment against Women in Cyber Space: Concept, Reality and the Law" (2023) X(1) *Kashmir Journal of Legal Studies*.

²¹ *Justice K.S. Puttaswamy (Retd.) v. Union of India*, (2017) 10 SCC 1.

²² UNESCO, *The Chilling: Global Trends in Online Violence Against Women Journalists* (2021).

²³ Powell, A. & Henry, N., "Technology-Facilitated Sexual Violence," *Violence Against Women*, Vol. 24, No. 11 (2018), pp. 1250–1267.

²⁴ Danielle Keats Citron, *Hate Crimes in Cyberspace* (Harvard University Press, 2014).

²⁵ Danielle Keats Citron & Robert Chesney, "Deep Fakes: A Looming Challenge for Privacy, Democracy, and National Security," *California Law Review*, Vol. 107 (2019).

²⁶ Clough, J., "Cybercrime," *Principles of Cybercrime* (Cambridge University Press, 2022).

-
- ²⁷ Halder, D. & Jaishankar, K., "Cyber Gender Harassment and Secondary Victimization of Women," *Victims & Offenders* (2011).
- ²⁸ Kshetri, N., "The Economics of Deepfakes," *Computer*, Vol. 53, No. 3 (2020).
- ²⁹ Keller, D., "Who Do You Sue? State and Platform Hybrid Power over Online Speech," *Hoover Institution Aegis Series* (2021).
- ³⁰ Powell, A. & Henry, N., "Technology-Facilitated Sexual Violence: A Literature Review of Empirical Research," *Trauma, Violence & Abuse* (2018).