

Women's Human Rights in Cyberspace Addressing Online Violence and Digital Abuse

Dr. A. Aswini¹, Prof. Dr. P. B. Pankaja²

¹Professor, Dr. Ambedkar Global Law Institute, Tirupati, affiliated to Sri. Venkateswara University, Tirupati.

²Faculty of Law, Dr. MGR Education and Research Institute Chennai. Former Professor, Law Centre1, Faculty of Law, University of Delhi, Delhi.

Abstract

The explosion in digital technologies and online platforms of communication have changed people's communication, economic engagement and democratic involvement all over the world. But cyberspace has also become a major location of gender-based violence, disproportionately targeting women, through cyberstalking, online harassment, non-consensual sharing of intimate images, trolling, doxing, identity theft and technology facilitated abuse. These are examples of digital violence that not only violate the dignity, privacy and freedom of expression of women but also pose a threat to internationally agreed human rights standards. The article critically discusses the relationship between women's human rights and cyberspace, through a discussion of the legal, constitutional, and socio-technical aspects of online violence and digital abuse. It examines the effectiveness of the current international human rights documents, cyber legislation and Indian law in tackling new forms of online gender-based violence. The research subsequently examines the contribution of social media platforms, state institutions, law enforcement bodies and judicial bodies to digital safety and accountability. Constitutional safeguards on equality, privacy, dignity and freedom under the Indian law system are particularly emphasized. It suggests that a combination of comprehensive legal changes, a gender-oriented cyber governance framework, increased platform accountability, digital literacy programs and coordinated international cooperation are needed to effectively protect women in digital environments. It emphasizes that protecting women's human rights in cyberspace is integral to the realization of substantive equality and inclusive digital democracy in the twenty-first century.

Keywords: Women's Human Rights, Cyber Violence, Digital Abuse, Online Harassment, Cyber Law

1. Introduction

Digital revolution has revolutionized the relationships, communication, governance, business and social participation of humans. As a key element of contemporary life, cyberspace has ushered in new opportunities for empowerment in particular for women who have been socially excluded and structurally discriminated. Women have gained access to education, work, politics, entrepreneurial activities and worldwide avenues for expression through digital technologies. At the same time, the emergence of these developments has brought cyber space into an important space of violations of the human rights of women. Internet violence and cyber abuse targeted at women is becoming a serious issue that impacts dignity, equality, privacy, freedom of expression and personal security on a global scale. It is no longer a question of

technological misuse, but a tremendous human rights problem that demands legal, constitutional and policy responses.

Women's human rights in the context of the internet are based on universally recognized human rights principles, as reflected in international instruments like the Universal Declaration of Human Rights, the Convention on the Elimination of All Forms of Discrimination against Women and the International Covenant on Civil and Political Rights. These rights are guaranteed, among others, equality before the law, freedom from discrimination, privacy, bodily autonomy, freedom of expression, access to information and participation in public life. The rights apply to virtual environments as well, since online environments play an increasing role in social, economic and political realities in the real world. Digital rights are extensions of human rights and this recognition reflects the vision that technology spaces should not be beyond the reach of legal and constitutional protections.

Cyberspace is the term used to describe the virtual world that exists as a result of Internet technologies, social media, communication applications and digital networks. The use of cyberspace by women has grown significantly with the growing penetration of the internet, the access to smart phones and the digital governance programmes. However, digital inclusion has also brought about new forms of violence against women that reflect and exacerbate women's existing inequalities. Gender-based discrimination has taken on technologically enhanced forms and leaves women at risk of being harassed, intimidated, exploited and abused via online communication.

Conceptualizing online violence against women is a broad category that includes many forms of harmful acts that are carried out online. They range from cyberstalking, revenge pornography, online threats and hate speech, trolling, impersonation, sexual harassment, deep fake technology, unauthorised distribution of personal images, and the dissemination of defamatory content. Digital abuse is not a subject to location, as it can continue for as long as a person desires and the information is accessible online. Online abuse can be extremely damaging to a person's mental health, leading to feelings of anxiety, depression, damage to a person's reputation, social isolation and loss of career opportunities. In some instances, victims of online harassment have suffered self-harm and have even committed suicide.

2. Forms and Dimensions of Online Violence against Women in Cyberspace

Violence towards women in digital life is one of the most alarming forms of gender inequality of the digital age. As social media sites, instant messaging applications and digital communication technologies have developed and grown, there has been an increase in opportunities for interaction, alongside spaces for abuse, intimidation and exploitation. Digital abuse can be ongoing, anonymous, and trans-border and is hard to regulate and control because of its nature. The multi faceted character of online violence is a good example of how technology can be used to serve as a tool to consolidate a male dominant control and marginalize women from public life.

The most common type of online violence against women is cyberstalking. It is defined as using digital technology to persistently monitor, harass, threaten or communicate with someone without permission. The perpetrators may monitor what women do online, send them abusive

messages, or use personal information to frighten and control women. Cyberstalking can cause anxiety and emotional trauma, greatly impacting victims' well-being and mobility. The internet helps anonymity of perpetrators allows them to carry on with harassment with no immediate consequences.

Revenge pornography or the non-consensual sharing of intimate photos is another serious aspect of digital abuse. In such instances private photos or videos are leaked online without permission, typically to shame, blackmail or retaliate against women. Internet platforms are viral and have irreparable consequences in terms of psychological trauma and damage to reputation. The victim may be subject to social rejection, victim-blaming, and career repercussions. With the rise of AI, this has been further exacerbated by the advent of deep fake technology which generates manipulated images and videos where women are shown in explicit or compromising situations, when they actually are not.

Another prevalent issue is sexual harassment online. Many women receive sexually explicit messages, comments on social media sites and communication platforms, threats to be raped, and images that are not requested that they see. Female journalists, activists, politicians and public figures are especially exposed to coordinated online attacks designed to silence or silence dissenting voices. This is harassment that deters women from engaging in democratic discourse and freedom of expression. The digital world is then hostile and exclusionary to women who want to be equal partners in public places.

There are other forms of cyber violence, such as trolling and hate speech. Misogyny is used to attack women who express their opinions on politics, social and cultural matters, with communal slurs and threats to women's life. Online groups can form and organize a coordinated harassment campaign against women who violate the traditional gender norms. Digital discrimination or differential access to and utilization of the internet exists at an intersectional level for minority women, such as women from marginalized castes, religions, and ethnic groups. Online abuse is thus a manifestation of wider social prejudice and systemic inequalities.

Another highly dangerous digital abuse is called “doxxing,” which is the unauthorized release of personal details like addresses, phone numbers, workplace information, or family information. This practice puts women in a situation of offline threats, stalking and physical violence. Likewise, fraudulent activities such as impersonation and identity theft have become commonplace, involving the use of women's photos or information to defame reputations or fraudulently impersonate them. These are breaches of privacy and can cause social and economic effects which will last into the future.

Online violence has psychological consequences, but its impact is not limited to that. Victimization often leads to anxiety, depression, fear, social isolation and loss of employment. Many women limit their engagement with the online world or even avoid it entirely because of harassment. This is affecting the digital inclusion of women and their participation in democracy. Trust issues around abuse have a chilling effect on freedom of speech and access to information, which impacts fundamental human rights.

The increased use of online platforms for work, education and social interaction during the COVID-19 pandemic also exacerbated online violence against women. The number of cases

of cyber harassment, online exploitation and domestic abuse that occurred through technology rose strongly in lockdown times. Children and young women were especially at risk of cyber-bullying and online grooming.

3. International Human Rights Standards and Legal Responding to Digital Abuse

The international human rights regime has come to acknowledge that digital technologies play an important role in respect and enjoyment of fundamental rights and freedoms. With cyberspace playing an increasingly important role in communication, governance, economic activity and social interaction, international organisations and human rights institutions have stressed that the same rights as are guaranteed offline must also be guaranteed online. Digital violence and online abuse as a form of violence against women has thus become a significant issue in international human rights debates. The development of international standards reflects a growing awareness that online gender-based violence is a violation of human dignity, equality, privacy and freedom of expression.

The Universal Declaration of Human Rights is the basis for protecting human rights in the digital era. The rights of equality, freedom of expression, freedom from discrimination, security and privacy are applicable in cyberspace. Likewise, the International Covenant on Civil and Political Rights provides for freedom of speech, privacy and freedom from arbitrary interference. These principles are used as the normative framework when tackling online violence against women.

Today the most important international document on the issue of women's rights is the Convention on the Elimination of All Forms of Discrimination against Women. It was drafted prior to the advent of the internet, but its content on discrimination, violence and gender inequality is very relevant to digital abuse. The Committee on the Elimination of Discrimination against Women (CEDAW) has defined gender-based violence as a much wider concept that encompasses technology-facilitated violence. The General Recommendation No. 35 is the first UN Committee on the Elimination of Discrimination against Women to acknowledge online harassment and cyber violence as acts of discrimination against women in society.

The United Nations Human Rights Council has repeatedly stated that human rights are relevant both on and off line. During debates on digital privacy, internet freedom, and online safety, the duty of the states to secure the protection of individuals from digital abuse is underlined. The Special Rapporteur on violence against women has also recognized the potential for online violence to cause serious psychological and social harm on par with physical violence. There is growing advocacy for gender-responsive cyber governance and more robust accountability systems for digital platforms from international human rights institutions.

Online abuse has also been greatly addressed through regional human rights systems. The Convention of the Council of Europe on Cybercrime is an international instrument for combating cybercrime, such as illegal access, misuse of data and exploitation in cyberspace. Psychological violence and harassment (including digital harassment) is acknowledged under the Istanbul Convention. Likewise, EU laws on digital services and data protection prioritize the rights of privacy, platform responsibility, and safeguards against online harm.

International legal measures against digital abuse are still less uniform, owing to geographical and national differences in the legal system. Cybercrimes often cross national boundaries, and investigations and prosecutions may be difficult. The law, evidentiary requirements and regulatory enforcement are not harmonized. However, cooperation with other countries via extradition arrangements, cybercrime treaties and mutual legal assistance treaties has grown in significance in the fight against cross-border crimes in the digital sphere.

In addition, technology firms and social media networks are vital to global digital governance. Social media like Facebook, Instagram, X, and YouTube have enormous power in shaping online communication and content decisions. Human rights groups say that these companies are obligated to stop violence and harmful content online, both ethically and legally. The transparency of platforms, the accountability of algorithms, and measures to protect users are turning into an international issue. Critics argue that poor moderation practices and profit-seeking algorithms tend to promote harmful and abusive content targeted at women.

Digital literacy and awareness is also a key element of the international human rights vocabulary. Women need to be empowered through education, technological training and awareness on cyber safety and protection of privacy in order to be empowered. Civil society organizations, international agencies and academic institutions all play important roles in the advocacy, research and policy development related to online gender-based violence.

4. Constitutional Protections and Cyber Laws in India: How to tackle Gender-based Online Violence

India is undergoing a rapid digital transformation, and as a result, Internet penetration, social media usage, and online communication have become much greater. Digital participation has been growing through policy and innovation initiatives that facilitate digital government and technological development in both urban and rural settings. But in parallel to these progressions, women online has become a significant area of law and social concern. The prevalence of cyber stalking, revenge porn, identity theft, online harassment and the distribution of obscene material has increased over time. The Indian constitutional framework and cyber laws, therefore, are significant in the protection of women's rights and holding them accountable in cyberspace.

The Constitution of India lays the foundation for protecting women from online violence. Article 14 also provides for equality before the law and equal protection of laws, which means that women have a right to protection from discriminatory and abusive practices on the Internet. Article 15 bans discrimination on the basis of the sex and gives the state the power to take special measures for the protection of women. These constitutional protections incorporate gender equality as fundamental and extend it into cyberspace.

With the advent of the digital age, Article 21, which guarantees the right to life and personal liberty, has become of tremendous importance. The courts have given wide interpretation to Article 21 and added the rights to privacy, dignity, reputation, and mental health. In the case of Justice K.S. Puttaswamy V. Union of India, the Supreme Court had declared privacy as a fundamental right that is embedded in dignity and autonomy. This verdict has significant

ramifications for digital privacy, control of information and preventing the unauthorized dissemination of personal information.

The right to freedom of speech and expression as guaranteed by Article 19(1)(a) also has a significant place in the cyberspace. Women have a right to freedom of expression online, but this is often limited by harassment, trolling and abusive speech. The state may reasonably restrict under the Article 19(2) for the sake of public order, decency, morality and defamation. Balancing freedom of expression with an anti-abuse law against online harassment continues to be a constitutional challenge.

The basic law regulating cyber crimes in India is Information Technology Act, 2000. The Act brings into the legal realm several types of cybercrime and remedies that may be enforced in response to online crimes. Section 66E imposes a penalty for acting in a manner that intrudes upon a person's right to privacy by taking and sharing photos of them without their consent. Section 67 applies to obscene material in electronic form, Section 67A to sexually explicit material and Section 67B to child pornography. The latter is especially important in situations of revenge pornography and sharing of intimate content.

The Indian Penal Code, which has now been largely updated with the Bharatiya Nyaya Sanhita, also has certain provisions pertinent to online abuse. Digital actions that fall under the category of stalking, sexual harassment, criminal intimidation, defamation, and insult to modesty may also apply. These provisions cover cyberstalking and threats using electronic communication. However, there are issues with implementation because law enforcement agencies are not as experienced in handling cybercrime cases and don't have the necessary technological knowledge.

The cyber law jurisprudence in India has been greatly influenced by judicial interventions. In *Shreya Singhal v Union of India*, Supreme Court said that Section 66A of IT Act violates freedom of speech and out of proportion. The judgment contributed to the strengthening of the constitutional protections of expression, but there were concerns that there was a lack of effective mechanisms to deal with online abuse and harassment. The courts remain struggling to strike the right balance between civil liberties and safety in the digital realm.

Cybercrime cells and online complaint portals have been set up by the government institutions and law enforcement agencies to deal with cybercrime. It is the National Cyber Crime Reporting Portal that allows victims to report online abuse and exploitation. Women and children have also been introduced into specialized mechanisms for dealing with cybercrimes. However, social stigma, the victimization of the women, limited awareness, and fear of retaliation are all significant factors in underreporting.

5. The role of social media platforms, law enforcement institutions and judiciary in ensuring digital safety.

The three most important institutional actors in the area of digital safety and protection of women from online violence are social media platforms, law enforcement and judiciary. Social media platforms in the modern digital landscape have become the main means of communicating, politically engaging, enjoying entertainment, educating and engaging in economic activities. But they've also been the platforms that have allowed for harassment,

cyberbullying, trolling, hate speech and technology-facilitated abuse. Given the increase in online violence against women, coordinated institutional responses that create accountability, protect victims and facilitate effective implementation of legal norms are imperative.

Another significant worry is algorithmic amplification. Social media algorithms work to serve the viewers' interests such as getting them to engage with the content they tend to show the most sensational and emotional, which can lead to the dissemination of abusive or harmful content. Violent, sexist material, trolling campaigns and harassment targeting particular individuals often end up in front of viewers because of the recommendation systems of algorithms. With the help of human rights organizations, algorithms need to be made accountable; and technology companies need to undertake impact assessments on gender discrimination and online safety.

Another important human rights issue in connection with the use of social media platforms is their data collection and monitoring. Personal details, photos, location information and communication records of women can easily be misused, accessed or exploited. Lack of privacy can make it easier for them to be stalked, doxxed, impersonated, or blackmailed. This means that effective data protection policies and user consent procedures are crucial to ensuring the protection of women's digital rights.

The police are important in helping to investigate cybercrimes and look for accountability for online abuse. In India, cybercrime cells and dedicated police have been set up to tackle cybercrime offences. The National Cyber Crime Reporting Portal is a place where victims can report cyber harassment, online exploitation and cyber abuse. Inconsistencies, however, in the effectiveness of law enforcement responses are attributed to infrastructural constraints, technological competence, limited trained manpower and jurisdictional issues.

When victims reach out to the police, they can often find themselves facing insensitive responses, and possibly victim-blaming or delays in the process. There is a lack of understanding of technology facilitated GBViD and digital evidence collection among many police officials. This deters women from reporting crimes and adds to under-reporting. The use of gender-sensitive trainings, digital forensic capacity-building, and victim-centred investigation mechanisms are thus crucial to enhance institutional effectiveness.

The judiciary is tasked with the role of protecting the rights enshrined in the Constitution and have a key role in the interpretation of the legal safeguards on digital safety. A growing number of courts have declared that privacy, dignity, reputation and informational autonomy are part of the fundamental rights. Judicial developments have been a key factor in shaping cyber law jurisprudence in India, dealing with subjects such as free speech, intermediary liability, privacy, and online abuse.

Indian courts have consistently held that cyber harassment and cyber abuse infringe upon rights to equality (Article 14), freedom of expression (Article 19), and freedom from inhuman or degrading treatment (Article 21). Judicial measures include compensation, criminal prosecution, injunctions and content removal orders to safeguard victims. However, technology issues, shifting patterns of cybercrime, and balancing freedom of expression with digital regulation are challenges for the judiciary.

6. Gender Justice in Cyberspace: Challenges, Policy reform and future directions

Although there is an increasing awareness of the problem of online violence against women, there are still many issues which have to be addressed to be able to effectively protect the rights of women in the cyberspace. Complex legal and institutional challenges emerge due to the dynamism and changing nature of digital technologies, the transnational dimension of cyber offenses and the prevailing patriarchal social attitudes. Current legislation and existing enforcement procedures often fail to take into account new types of digital abuse and the laws are not well enforced in most countries. Comprehensive reforms of the law, technology, governance, education and international cooperation are therefore essential for achieving gender justice in cyberspace.

The lack of harmonized and comprehensive laws which specifically reflect on technology-facilitated gender-based violence is one of the biggest challenges. The majority of cyber laws were created before the advent of sophisticated digital platforms, artificial intelligence, deepfake technology, and algorithmic systems. Many laws, therefore, fail to adequately reflect the nature of online abuse. The traditional criminal laws are often written around a set of concepts which are not always directly applicable to harms in the virtual world.

Jurisdictional complexity is another significant impediment. Cybercrimes are able to cross national lines as offenders, victims, crime servers, and digital platforms can be in various countries. Investigation and prosecution of cross-border offences need International cooperation, mutual legal assistance treaties, and harmonisation of cyber laws. Problems with differing legal requirements, rules of evidence and priorities for action make it difficult to take effective action against offenders when they cross jurisdictions.

Vulnerabilities in the digital world are further compounded by the digital inequality. There are disparities in access to digital resources, technological literacy, and internet connectivity between social-economic groups. Economically deprived, marginalized, and rural women may not have an awareness of cyber safety, privacy settings, and legal remedies. This is why the digital divide is a factor that is exacerbating unequal protection and vulnerability to exploitation.

Gender justice policy reforms for the cyberspace need to be multi-dimensional and rights based. Governments should pass comprehensive laws that explicitly cover online GBV, such as cyberstalking, deepfakes, doxxing and the sharing of intimate content without consent. Definitions should be technologically flexible and gender responsive. There also needs to be more robust intermediary liability laws and clear, accountable actions by platforms.

Second, the nature of the criminal case needs to be specialized training for law enforcement, digital forensic infrastructure, and a procedure for investigating the crime in a victim-centered manner. Creating dedicated cyber units with gender sensitive staff can create better reporting and investigation practices. Additionally, there are fast-track systems for content removal and emergency protection orders that can improve victim safety.

Thirdly, significant extension of digital literacy and awareness programmes is required. The promotion of cyber safety education, privacy awareness and responsible digital conduct by

educational institutions, civil society organizations and governments. Women and girls need to be equipped with the technological know-how to operate safely and confidently in cyberspace.

Fourth, it is essential to have international cooperation to respond to transnational cyber offenses. The States should cooperate via international conventions, information-sharing channels and coordinated cybercrime investigations. International human rights bodies can play a role by creating a common framework on digital safety and platform responsibility.

7. Conclusion

Much of human interaction, government, communication and social engagement has been changed by the digital era. Technological progress has brought women unprecedented opportunities for empowerment and inclusion, but it has also resulted in new forms of violence, discrimination and exploitation in cyberspace. Harassment, cyberstalking, revenge pornography, trolling, hate speech and technology facilitated abuse have become a serious threat to women's dignity, privacy, equality and freedom of expression. These challenges illustrate that cyberspace does not exist outside the social realities but rather mirrors and magnifies current inequalities between women and men and structural discrimination.

Women's human rights are being violated in digital environments and need a multifaceted and holistic approach. Constitutional rights to equality, privacy, dignity, and liberty should be meaningfully given expression in the virtual world through progressive judicial interpretation and strong legal protocols. The normative foundations of digital safety and accountability are laid out by international human rights standards, cyber laws and principles of national constitutions. But legislation cannot alone achieve the desired results in the absence of enforcement, institutional readiness, and technological readiness.

Social media platforms, the police, governments, and judicial bodies need to engage one another in developing safe, inclusive and rights affirming digital spaces. Enhancing platform accountability, fostering gender-inclusive cyber-governance, promoting digital competency programs, and promoting international collaboration are key for tackling new technological risks. In conclusion, protecting women's rights in the cyberspace is essential for substantive equality, democratic participation and social justice in the twenty first century. True inclusion of a digital society will only be achieved when women can access and participate online free from fear, discrimination and violence.

References

1. Citron, D. K. (2014). Hate crimes in cyberspace. Harvard University Press.
2. Danielle Keats Citron, & Franks, M. A. (2014). Criminalizing revenge porn. Wake Forest Law Review, 49(2), 345–391.
3. Henry, N., & Powell, A. (2018). Technology-facilitated sexual violence: A literature review of empirical research. Trauma, Violence, & Abuse, 19(2), 195–208.
4. Jane, E. A. (2017). Misogyny online: A short (and brutish) history. SAGE Publications.
5. Mantilla, K. (2015). Gendertrolling: How misogyny went viral. Praeger.
6. Powell, A., & Henry, N. (2017). Sexual violence in a digital age. Palgrave Macmillan.
7. Salter, M., & Crofts, T. (2015). Responding to revenge porn: Challenges to online legal impunity. In B. Larkin (Ed.), New perspectives on cybercrime (pp. 233–256). Palgrave Macmillan.

8. United Nations Human Rights Council. (2018). Report of the Special Rapporteur on violence against women, its causes and consequences on online violence against women and girls from a human rights perspective (A/HRC/38/47). United Nations.
9. United Nations. (1979). Convention on the Elimination of All Forms of Discrimination against Women (CEDAW). United Nations Treaty Series, 1249, 13–20.
10. Justice K.S. Puttaswamy v. Union of India, (2017) 10 SCC 1 (India).