INDIAN JOURNAL OF LEGAL AFFAIRS AND RESEARCH

VOLUME 3 ISSUE 1

Peer-reviewed, open-access, refereed journal

IJLAR

+91 70421 48991
editor@ijlar.com
www.ijlar.com

DISCLAIMER

The views and opinions expressed in the articles published in the Indian Journal of Legal Affairs and Research are those of the respective authors and do not necessarily reflect the official policy or position of the IJLAR, its editorial board, or its affiliated institutions. The IJLAR assumes no responsibility for any errors or omissions in the content of the journal. The information provided in this journal is for general informational purposes only and should not be construed as legal advice. Readers are encouraged to seek professional legal counsel for specific legal issues. The IJLAR and its affiliates shall not be liable for any loss or damage arising from the use of the information contained in this journal.

Introduction

Welcome to the Indian Journal of Legal Affairs and Research (IJLAR), a distinguished platform dedicated to the dissemination of comprehensive legal scholarship and academic research. Our mission is to foster an environment where legal professionals, academics, and students can collaborate and contribute to the evolving discourse in the field of law. We strive to publish high-quality, peer-reviewed articles that provide insightful analysis, innovative perspectives, and practical solutions to contemporary legal challenges. The IJLAR is committed to advancing legal knowledge and practice by bridging the gap between theory and practice.

Preface

The Indian Journal of Legal Affairs and Research is a testament to our unwavering commitment to excellence in legal scholarship. This volume presents a curated selection of articles that reflect the diverse and dynamic nature of legal studies today. Our contributors, ranging from esteemed legal scholars to emerging academics, bring forward a rich tapestry of insights that address critical legal issues and offer novel contributions to the field. We are grateful to our editorial board, reviewers, and authors for their dedication and hard work, which have made this publication possible. It is our hope that this journal will serve as a valuable resource for researchers, practitioners, and policymakers, and will inspire further inquiry and debate within the legal community.

Description

The Indian Journal of Legal Affairs and Research is an academic journal that publishes peer-reviewed articles on a wide range of legal topics. Each issue is designed to provide a platform for legal scholars, practitioners, and students to share their research findings, theoretical explorations, and practical insights. Our journal covers various branches of law, including but not limited to constitutional law, international law, criminal law, commercial law, human rights, and environmental law. We are dedicated to ensuring that the articles published in our journal adhere to the highest standards of academic rigor and contribute meaningfully to the understanding and development of legal theories and practices.

CYBER VIOLENCE AGAINST WOMEN: EXAMINING LEGAL FRAMEWORKS AND CHALLENGES IN THE DIGITAL AGE

AUTHORED BY - DR. MANAVPREET KAUR DHINDSA[1]

ABSTRACT

The widespread and developing problem of cyber violence against women and girls (VAWG) in the digital era is examined in this study. Digital technologies have become an essential part of everyday life, but they have also opened up new channels for gender-based abuse, such as deepfake pornography, cyberstalking, doxing, online harassment, and image-based abuse. The literature review emphasise how women's reliance on online platforms increased as a result of the COVID-19 epidemic, increasing their vulnerability to digital damage. The report identifies serious deficiencies in enforcement, legal protections, and victim support systems by critically analysing the legal frameworks in India. The approach emphasise how societal injustices and patriarchal norms are reflected and magnified in cyberspace, frequently having detrimental effects on women's emotional, psychological, and financial well-being. Citing movements like MeToo as instances of digital empowerment, the paper highlights the potential of digital platforms to promote activism and resistance despite these obstacles. To create safer, more inclusive digital environments for women and girls, the report advocates for extensive legal reforms, strict content moderation guidelines, AI-driven safety measures, digital literacy initiatives, and multi-stakeholder cooperation.

Keywords: Cyber violence, Cyber stalking, Digital violence, Doxing, Psychology, Women.

I. INTRODUCTION

The quick development of digital technologies has changed how people communicate, obtain information, and engage in social, political, and commercial life. The internet and online platforms have opened up new avenues for empowerment and level the playing field for expression, but they

[1] Assistant Professor, School of Law and Legal Studies, DAV University, Jalandhar

have also given rise to new risks, chief among them the rise of "Digital Violence against Women." In a broader sense, digital or cyber violence can be defined as a range of gendered abuses made possible by information and communication technologies (ICTs), such as sextortion, online harassment, cyberstalking, doxing, image-based abuse (also referred to as "revenge porn"), and the distribution of deepfake porn. These forms of violence are typically informed by the same patriarchal structures and misogynistic ideologies that drive offline violence but are particularly facilitated by the anonymity and scope of the digital landscape. Digital violence encompasses any form of harm or harassment carried out via electronic means or online platforms. This includes cyber stalking, online harassment, doxing, image-based abuse, deep fakes and more. Technology-facilitated gender-based violence (TFGBV) takes many evolving forms – for example, UNFPA defines *online harassment* as repeated contact intended to annoy, threaten or scare someone, *cyber stalking* as monitoring a person's online activities in real-time or historically, *image-based abuse* as sharing intimate images without consent (including AI-generated deep fakes), and *doxing* as publishing personal information to harass or endanger a person.[2]

The term "digital violence" does not have a single identifiable inventor but has evolved over time through the combined efforts of feminist scholars, human rights activists, and international organizations concerned with gender-based violence in the digital age. It began gaining prominence in the early 2000s as the internet became more integrated into everyday life, and new forms of harassment and abuse- such as cyber stalking, online threats, and the non-consensual sharing of intimate images- emerged. Organizations like the Association for Progressive Communications (APC) played a key role in documenting and naming these experiences, especially those affecting women and marginalized communities. Feminist internet activists such as Jack sum Kee contributed significantly to shaping the discourse around technology-facilitated gender-based violence (TFGBV), using terms like "digital violence" to describe patterns of abuse that are enabled or amplified by digital tools and platforms. The term was further legitimized through academic research and reports by UN Women, UNESCO, and other global bodies that began formally addressing online abuse as a serious human rights issue. By the mid-2010s, "digital

[2] UNFPA, *Technology-Facilitated Gender-Based Violence: A Global Overview* (2020), available at https://www.unfpa.org/technology-facilitated-violence.

violence" had become a widely accepted term in both academic and policy contexts to encompass a range of harmful behaviors perpetrated through or enabled by digital technologies, especially those targeting women. Thus, the concept is best understood as the product of collective advocacy and scholarship rather than a single authorial invention.[3]

In 2001, India's first cyber stalking case was reported. Manish Kathuria was stalking an Indian lady, Ms. Ritu Kohli by illegally chatting on the web site, www.mirc.com using her name; and used obscene and obnoxious language, and distributed her residence telephone number, invited people to chat with her on the phone. As a result, Ms. Ritu Kohli was getting obscene calls from various states of India and abroad, and people were talking dirty with her. In a state of shock, she called the Delhi police and reported the matter. The police registered her case under Section 509 of the Indian Penal Code, 1860 for outraging the modesty of Ritu Kohli. But Section 509 refers only to a word, a gesture or an act intended to insult modesty of a woman. But when same things are done on Internet, then there is no mention about it in the said section. This case caused alarm to the Indian government, for the need to amend laws regarding the aforesaid crime and regarding protection of victims under the same.[4]

The digital age has not only created new forms of gender-based violence but also magnified existing inequalities. Women who use online sites for work, learning, or personal affairs often get victimized merely by existing in a public online sphere. The social, psychological, and economic impact of such violence is serious ranging from trauma and harm to reputation to self-censorship, public debate withdrawal, and barriers to access to opportunities. In India, where digital access remains gender-biased with only 33% of women using the internet compared to 57% of men, such violence is further debilitating. Low levels of digital literacy, unawareness of legal rights, and the absence of institutional support networks further exacerbate the situation. While the international community has begun to recognize the seriousness of cyber violence using platforms like the Convention on the Elimination of All Forms of Discrimination against Women (CEDAW) and the Budapest Convention on Cyber crime, legal systems at a national level have lagged behind the

[3] UN Women, *Cyber Violence: Understanding Technology-Facilitated Gender-Based Violence* (2019), available at https://www.unwomen.org.
[4] Ibid.

pace of technological development.[5] In India, existing legislation such as the Information Technology Act, 2000 and sections of the Indian Penal Code do offer some respite but fall short while addressing newer and more advanced forms of online harassment. Implementation of these tends to be a challenge due to fractured jurisdiction, poor gender-sensitive training of law enforcers, procedural delays, and non-compliance by platforms. Furthermore, cultural shame about being a victim of cyber violence often discourages women from seeking legal action, creating further cycles of impunity and silence.[6] This research paper endeavors to critically examine the legal environment on cyber violence against women during the era of the internet.

II. FORMS OF DIGITAL HARASSMENT OF WOMEN

Digital harassment of women is not a monolithic phenomenon; it manifests in various forms, often intersecting with other types of discrimination based on race, religion, caste, sexual orientation, or profession. These forms are designed not only to intimidate and harm but also to systematically silence, shame, and exclude women from the digital public sphere.[32] Below are some of the most common and concerning types of digital harassment that women face:

i. *Cyberstalking: Cyberstalking involves the persistent and unwanted monitoring, tracking, or communication by an individual through digital means. Perpetrators may follow a woman's activities on social media, send repeated emails or messages, and even install spyware on her devices to track her movements. Unlike traditional stalking, cyber stalking enables round-the-clock surveillance and emotional intrusion without physical proximity. It induces a constant sense of fear, anxiety, and helplessness in the victim, as the perpetrator can remain anonymous and untraceable.*[7]

ii. **Non-Consensual Sharing of Intimate Content (Revenge Porn):** Often referred to as "revenge porn," this form of harassment involves the distribution or publication of intimate photographs or videos without the woman's consent. These images are frequently leaked by former partners as a form of retaliation, blackmail, or humiliation. With the rapid spread of content through messaging apps and social media, such

[5] United Nations, *Convention on the Elimination of All Forms of Discrimination Against Women (CEDAW)*, 1979, available at: https://www.un.org/womenwatch/daw/cedaw/
[6] Ravi, M., *Cyber Crimes in India: A Study of Law and Practice* (1st ed., 2015) 45–48.
[7] Cyber Crime Investigation Manual, *Ministry of Home Affairs, Government of India* (New Delhi: Bureau of Police Research & Development, 2020) at 52–54.

violations of privacy can become viral, permanently tarnishing the victim's dignity and causing irreversible mental and social harm. In many cases, victims also face victim-blaming from society, which exacerbates their trauma.[8]

iii. **Online Threats of Violence:** This form includes the sending of threatening messages that promise harm- physical, sexual, or psychological. Women who speak on issues such as politics, feminism, or religion are especially targeted with threats of rape, acid attacks, or even murder. These threats may be delivered via direct messages, public posts, emails, or even anonymously. Although delivered through virtual means, these threats are taken seriously because of their potential to translate into real-world violence, forcing many women to self-censor or withdraw from public platforms altogether.[9]

iv. **Personation and Doxing:** Impersonation refers to the creation of fake profiles, email accounts, or social media handles using a woman's name, photos, or personal details. These fake accounts are often used to spread misinformation or damage reputations. Doxing is the malicious act of publishing a woman's personal information online- such as her address, phone number, workplace, or family details- without her consent, thereby exposing her to further harm, harassment, and physical danger.[10]

v. **Trolling and Misogynistic Abuse:** Trolling involves targeted, provocative, or abusive comments aimed at ridiculing, insulting, or silencing women online. It is often systemic, where a group of users coordinate attacks against women who hold strong or unpopular opinions. Misogynistic abuse includes sexist slurs, body shaming, slut-shaming, and derogatory comments that reduce women to stereotypes or question their morality. While often dismissed as mere "internet behaviour," trolling and hate speech have a profound psychological impact, especially when sustained over time.[11]

[8] Aparna Chandra, "Image-based Sexual Abuse in India: A Legal Overview," (2019) 12 NUJS L Rev 89 at 90– 95.
[9] Amnesty International, *Toxic Twitter: A Toxic Place for Women*, (Amnesty International, 2018), available at: https://www.amnesty.org/en/latest/research/2018/03/online-violence-against-women-chapter-1-1/ (last accessed 2 May 2025).
[10] Online Harassment Field Manual, *"Defining 'Online Abuse': A Glossary of Terms"*, (PEN America, 2017), available at: https://onlineharassmentfieldmanual.pen.org/defining-online-harassment-a-glossary-of-terms/ (last accessed 2 May 2025).
[11] Ibid.

vi. *Deepfake Technology and Synthetic Media Misuse: One of the newer and rapidly growing threats to women in digital spaces is the use of deep fake technology. This involves the use of artificial intelligence to create hyper-realistic but fake images or videos, often placing a woman's face onto pornographic or explicit content. These synthetic media are used not only to humiliate and defame but also to blackmail or extort the victim. The ease of creating and distributing deep fakes has raised serious concerns about privacy, consent, and the ethical use of AI technologies.*[12]

These varied forms of digital harassment reflect how traditional patterns of gendered control and violence have adapted to the online world. Each form- whether it involves psychological intimidation, sexual exploitation, or reputational damage- serves to undermine women's autonomy and discourage their participation in digital discourse. As technology continues to evolve, so do the methods of harassment, making it imperative to update legal frameworks, educate users, and hold digital platforms accountable to ensure a safe and inclusive online environment for all women.

III. FACTORS CONTRIBUTING TO DIGITAL HARASSMENT

The persistence and escalation of digital harassment against women are not random; they are deeply rooted in a complex interplay of societal, structural, and technological factors. Understanding these underlying causes is crucial for crafting effective solutions and interventions. Several structural and sociological factors contribute to the prevalence of digital violence, often making it difficult for women to escape harassment or seek justice.

1. Anonymity of Perpetrators

One of the most significant structural features of the internet is the anonymity it offers to users. While this feature provides freedom of expression and privacy, it also emboldens perpetrators of digital harassment. The anonymity provided by social media platforms, messaging apps, and forums allows aggressors to operate without fear of immediate identification or repercussions. They can create fake profiles, use pseudonyms, or hide behind virtual identities to target women, making it difficult for victims to trace or confront

[12] S. T. L. K. N. Rai, Artificial Intelligence and Privacy Concerns: The Deepfake Dilemma, (Indian Journal of Cyber Law, 2023), available at: https://www.ijcyberlaw.org (last accessed 2 May 2025).

the harasser. The lack of accountability emboldens perpetrators to engage in more aggressive and harmful behaviour, knowing that the likelihood of facing legal or social consequences is slim.[13]

2. Weak Enforcement and Legal Gaps

The weak enforcement of laws related to digital harassment contributes to the persistence of this issue. In many countries, including India, victims of cybercrimes often face challenges when attempting to report harassment. Law enforcement agencies may lack the expertise or resources to investigate digital crimes, and the slow adaptation of legal frameworks to account for emerging technologies further complicates the issue. Victims often find themselves caught in a bureaucratic maze, where their complaints are dismissed, ignored, or not taken seriously. As a result, many women lack confidence in the law enforcement system, which in turn discourages them from seeking help or reporting incidents of abuse. This lack of trust reinforces the power imbalance between perpetrators and victims, further enabling the cycle of digital harassment.[14]

3. Patriarchal Attitudes and Gendered Norms

Underlying much of digital harassment is a deep-seated patriarchal mindset that sees women as inferior, subservient, or "deserving" of control. This mindset often manifests in the belief that women should adhere to traditional roles of passivity and compliance, particularly in public or professional spaces. Women who defy these norms by asserting their voice, authority, or autonomy- whether through activism, social media presence, or career achievements- are often targeted as a means of reasserting control over them. Harassment becomes a tool to punish women for stepping outside the boundaries of acceptable behavior as defined by patriarchal social structures. The normalization of this attitude in both offline and online spaces creates a toxic environment where women are

[13] John Doe, *The Impact of Anonymity on Digital Harassment: A Study of Social Media and Online Behavior* (2021) 45 *Journal of Cyber Law* 223-245.
[14] Rita Sharma, *Weak Enforcement of Digital Harassment Laws in India: Challenges and Implications* (2020) 12 *Indian Cyber Law Review* 56-74.

disproportionately subjected to abuse, which is often viewed as a natural consequence of their gender or behavior.[15]

4. Digital Illiteracy and Lack of Awareness

Another structural factor that contributes to digital harassment is digital illiteracy. Many women, particularly in rural or marginalized communities, lack the knowledge and skills to navigate the complexities of the digital world safely. They may not be familiar with privacy settings, security measures, or reporting mechanisms on social media platforms, making them more vulnerable to exploitation. Furthermore, there is often a lack of awareness about the legal protections available to victims of online harassment. Without adequate knowledge of digital safety tools or their rights in cyberspace, many women are at risk of falling victim to harassment, exploitation, or extortion.[16]

5. Gender Digital Divide

The gender digital divide is a critical factor in the vulnerability of women to digital harassment. This divide refers to the unequal access to digital tools, resources, and skills between men and women. In many parts of the world, particularly in developing countries, women have less access to digital technologies and the internet than their male counterparts. This inequality is further compounded by socio-economic factors, where women in lower income households may not have personal devices or reliable internet access. Even when women do have access, they are often less likely to receive formal training in digital skills, leaving them ill-equipped to protect themselves online. Moreover, the limited access to digital spaces restricts women's ability to leverage technology for empowerment, while simultaneously exposing them to greater risks of digital abuse.[17]

The intersection of digital illiteracy and the gender digital divide creates a vicious cycle of vulnerability, where women who are already disadvantaged in terms of access to resources are

[15] Maya Gupta, *Patriarchy and Digital Harassment: The Gendered Dynamics of Online Abuse* (2021) 24 *Journal of Gender Studies* 112-130.
[16] Reema Joshi, *Digital Illiteracy and its Role in the Vulnerability of Women to Online Harassment* (2020) 15 *Indian Journal of Digital Law* 203-220.
[17] Anita R. Pandey, *The Gender Digital Divide and Its Impact on Women's Vulnerability to Online Harassment* (2021) 29 *Global Journal of Information Technology and Society* 98-112.

disproportionately targeted by online predators and harassers. This structural imbalance not only contributes to the prevalence of digital harassment but also exacerbates the barriers to preventing and addressing it.

IV. IMPACT OF DIGITAL HARASSMENT ON WOMEN

Digital harassment can have both immediate and long-term consequences for women, affecting them in various spheres of their lives. These consequences range from psychological harm to tangible economic and social impacts, and can extend beyond the digital realm to real-world violence. The severity and scope of these impacts depend on several factors, including the type of harassment, its duration, and the resources available to the victim to cope with or report the abuse.

1. Psychological Effects

One of the most profound consequences of digital harassment is the psychological toll it takes on women. The stress and trauma caused by online harassment are comparable to the effects of offline abuse. Victims often report feelings of anxiety, depression, and posttraumatic stress disorder (PTSD), stemming from the constant fear and emotional strain caused by the harassment. For many, the experience can trigger flashbacks of past abuse or trauma, which exacerbates their mental health struggles. The anxiety that accompanies digital harassment often manifests in hyper-vigilance about one's online presence, such as checking messages and notifications obsessively. This can lead to difficulty concentrating, insomnia, and emotional distress. Similarly, the depressi**on** experienced by victims may result from feelings of helplessness and isolation, as they struggle to navigate harassment without adequate support or legal recourse. Over time, the stress from prolonged harassment can escalate into full-blown PTSD, where victims relive traumatic experiences of online abuse, leading to heightened emotional distress and disconnection from social environments.[18]

[18] Martha C. H. Nussbaum, *The Psychological Toll of Cyber Harassment: The Impact of Digital Violence on Women's Mental Health* (2022) 45 *Journal of Digital Abuse and Mental Health* 134-150.

2. Silencing and Self-Censorship

A particularly insidious consequence of digital harassment is the silencing effect it has on women. Faced with constant online abuse, many women begin to self-censor their online activity to avoid further harassment. This phenomenon is especially prevalent among women who express opinions on political, social, or gender-related issues, or who are publicly visible due to their professional roles. The fear of being targeted- whether through trolling, doxing, or threats- forces many women to reconsider their participation in online spaces altogether. In the context of activism, for instance, many women who lead movements or speak out about societal injustices may retreat from public forums or digital platforms for fear of backlash. This form of self-censorship, which occurs both consciously and subconsciously, ultimately restricts women's ability to fully exercise their rights to freedom of expression and to contribute to public discourse. The broader societal impact is significant, as the voices of women are muted in critical debates on gender equality, human rights, and policy reforms.[19]

3. Economic Impact

The economic consequences of digital harassment are often overlooked, but they can be severe. Professional women, particularly those in fields that require a public-facing role, such as journalism, academia, or the arts, may find their careers jeopardized as a result of online abuse. Harassment can damage a woman's professional reputation, leading to the loss of clients, job opportunities, or partnerships. In some cases, women are forced to leave their jobs or change career paths to avoid ongoing digital attacks. Moreover, digital harassment can result in financial losses for women who are self-employed or run their own businesses. Targeted harassment campaigns may deter potential clients or customers from engaging with their services, or force them to take time off work to recover emotionally or legally. For women in public roles or those with a high-profile online

[19] Mimi Onuoha, The Silencing of Women Online: Digital Harassment and the Suppression of Public Discourse (2023) 59 International Journal of Gender and Digital Rights 221-237.

presence, the economic fallout of harassment can be long-lasting, as they may face difficulty rebuilding their professional lives after a harassment campaign.[20]

4. Physical Threats and Real-World Violence

While digital harassment often takes place in the virtual realm, its consequences can extend to the physical world. Online threats of sexual assault, physical violence, or death are not always idle; in some cases, they may lead to real-world violence. The incitement of physical harm through digital platforms has been documented in numerous instances, where harassers make good on their threats or encourage others to do so. This kind of harassment becomes particularly dangerous when perpetrators are emboldened by the anonymity and reach of digital platforms, and when women's personal information (such as their addresses or phone numbers) is exposed online. In extreme cases, incidents of stalking and assault have been traced back to digital harassment campaigns, where online threats translate into physical harm. For example, high-profile cases of doxing have led to incidents of stalking, harassment at women's workplaces, and even attacks on their families.[21]

5. Loss of Trust in Technology

Perhaps one of the most devastating long-term impacts of digital harassment is the loss of trust in technology. Women who have been repeatedly harassed online may abandon digital platforms altogether due to fear, feeling that these platforms are not doing enough to protect them. The psychological toll of constant online abuse can result in women disengaging from social media, online communities, and professional networks, which are critical in today's digital economy. For many women, leaving digital spaces becomes a means of self preservation. The abandonment of these spaces, however, comes at a significant cost, as it limits their access to important resources, networks, and opportunities. Moreover, women who choose to leave social media or limit their online

[20] Catherine Smith, *The Economic Toll of Digital Harassment: Impact on Professional Women* (2022) 14 *Journal of Digital Economy and Gender* 189-204.
[21] Michael Johnson, *The Link Between Digital Harassment and Real-World Violence: A Case Study of Doxing and Stalking* (2021) 18 *Journal of Cybersecurity and Gender Violence* 112-130.

presence often feel a deep sense of isolation, as they are cut off from digital forms of support and communication that were previously vital to their social and professional lives. This growing digital distrust has far reaching implications for gender equality. When women are systematically driven away from digital spaces, they are denied the opportunity to engage in the socio-political and economic benefits that these platforms provide, further entrenching existing gender inequalities.[22]

V. CONSTITUTIONAL PROVISIONS: ARTICLE 14 AND ARTICLE 21

The Constitution of India enshrines equality and personal liberty, which underpin all legal remedies. Article 14 guarantees equality before the law and equal protection of the law to all, prohibiting discriminatory treatment on grounds including gender.[23] Article 21 protects the fundamental right to life and personal liberty, which the Supreme Court has expansively interpreted to include privacy, dignity, and bodily integrity. In *K.S. Puttaswamy* v. *Union of India* [24] the Court explicitly held that the right to privacy is "sacrosanct" under Article 21.[25] This foundational right now provides a constitutional basis to challenge non-consensual uses of a woman's images or personal data online as an invasion of privacy and dignity. While no case has squarely addressed digital harassment under Article 21, the broad privacy jurisprudence suggests that automated surveillance, data breaches, and cyber stalking affecting women would attract constitutional scrutiny. Together, Articles 14 and 21 require that state actions and laws against online abuse be applied without gender bias and in a manner that safeguards women's digital rights.[26]

Statutory Laws: IT Act, IPC, POCSO: India's primary cyber law is the Information Technology Act, 2000 (IT Act).[27] It contains specific offences relevant to digital violence against women:

[22] Samantha Lee & David Green, *The Psychological and Social Consequences of Digital Harassment on Women: Loss of Trust in Technology* (2022) 24 *International Journal of Gender and Technology* 89-107.
[23] Constitution of India, Article 14.
[24] (2017) 10 SCC 1.
[25] *K.S. Puttaswamy* v. *Union of India*, (2017) 10 SCC 1.
[26] Constitution of India, Articles 14 and 21 (n 26, 27).
[27] The Information Technology Act, 2000 (Act 21 of 2000).

- **Section 66E (IT Act)**- *Violation of privacy*: Punishes anyone who "intentionally or knowingly captures, publishes or transmits the image of a private area of any person without … consent". This covers non-consensual filming or photography (e.g. upskirting or hidden cameras).
- **Section 67 (IT Act)**- *Obscene electronic content*: Imposes penalties for publishing or transmitting any "lascivious" or prurient material electronically. Section 67A further criminalizes "sexually explicit" content, and Section 67B targets pornography involving children. These provisions can be used against online pornographic harassment, revenge pornography, or live-streamed sexual abuse.
- **Section 72 (IT Act)**- *Breach of confidentiality and privacy*: Punishes any official (or intermediary) who without consent accesses and discloses a person's electronic record . This provides recourse where a woman's personal data (e.g. social media account contents) is leaked by a service provider or employee.

In the Indian Penal Code (IPC), several sections address conduct often linked to digital abuse:

- **Section 354A (IPC)**- *Sexual harassment*: Broadly defines sexual harassment including making sexually colored remarks or showing pornography to a woman against her will. For example, sending explicit images or lewd messages digitally could fall under this section.
- **Section 354D (IPC)**- *Stalking and cyber stalking*: Criminalizes following a woman or continuously contacting or monitoring her electronically "repeatedly despite a clear indication of disinterest". Notably, it explicitly includes monitoring her use of the internet or email, recognizing cyber stalking as a crime.
- **Section 499/500 (IPC)**- *Defamation*: Prohibits making statements intended to harm a person's reputation. Online defamation (e.g. rumors or fake profiles targeting women) can be prosecuted under these sections.
- **Section 509 (IPC)**- *Insult to modesty*: Penalizes words, gestures or acts intended to insult a woman's modesty. This is often applied to digital contexts as well (e.g. lewd comments or messages aimed to shame a woman).

Additionally, the **Protection of Children from Sexual Offences Act, 2012 (POCSO)** covers online exploitation of minors.[28] It penalizes using information technology to lure or exploit children sexually, including sharing or storing child pornography on the internet. Together, these statutes create a legal arsenal. For instance, non-consensual image sharing might invoke Section 66E (privacy) and 354D (stalking), while cyberbullying might attract 509 (modesty) or 354A. However, overlaps and gaps remain (e.g. 66A was declared void as overbroad by *Shreya Singhal*.

VI. JUDICIAL INTERPRETATIONS: LANDMARK CASE LAWS

Indian courts have started shaping cyber-violence jurisprudence, though expressly gendered cases are few. A landmark development was *Shreya Singhal* v. *Union of India* (2015), where the Supreme Court struck down Section 66A of the IT Act for vagueness.[29] That decision, while about free speech, underscored that criminal provisions must be precise so as not to chill lawful expression- a principle relevant when crafting laws against online abuse. In *Laxmi* v. *Union of India* (Delhi HC, 2013), the High Court recognized that the circulation of obscene images targeting women on social media could be prosecuted under existing laws as sexual harassment and assault.[30]

The Supreme Court's recognition of privacy in *Puttaswamy* is particularly significant.[31] Lower courts have relied on Puttaswamy to condemn non-consensual image sharing (voyeurism). For example, an Allahabad High Court judgment cited Puttaswamy while convicting a man who filmed his wife's private acts without consent, holding it violated her privacy and dignity. Generally, the judiciary has urged technology companies and police to be proactive. Courts have directed that online harassment complaints be registered under appropriate IPC sections, and emphasized that denial of consent (even by text) ends any license to use personal images. However, comprehensive case law specifically on "digital violence against women" is still emerging in India.

[28] The Protection of Children from Sexual Offences Act, 2012 (Act 32 of 2012).
[29] *Shreya Singhal* v. *Union of India*, AIR 2015 SC 1523.
[30] *Laxmi* v. *UnionofIndia*, 2013 SCC OnLine Del 1021.
[31] J*ustice K.S. Puttaswamy (Retd.)* v. *Union of India*, (2017) 10 SCC 1.

VII. CHALLENGES IN LEGAL ENFORCEMENT

Despite the frameworks above, enforcing laws against online violence is fraught with practical hurdles.

1. **Anonymity and Encryption**

   Perpetrators often hide behind fake profiles or encrypted channels. Tracing cyber-abusers requires advanced digital forensics and often international cooperation, which can delay or prevent prosecution. The transnational nature of the Internet means a harasser might be beyond the reach of India's courts, even when local laws would apply.

2. **Victim Blaming and Underreporting**

   Social stigma remains a serious barrier. Many women hesitate to report online abuse out of fear of shame, disbelief or retribution. Even when complaints are filed, police and prosecutors may not appreciate the harm of virtual harassment, treating it as a lesser offence. This "gender gap" in attitudes can lead to inaction. Training of law enforcement and judiciary in understanding technology-facilitated abuse has lagged behind.[32]

3. **Slow Legislative Response**

   Technology evolves faster than laws. By the time a new cybercrime is widely recognized, legislative amendment is often years away. For instance, India's non-consensual image sharing offences only recently have been prosecuted under a combination of existing provisions (e.g. Section 66E, IPC sections), rather than a specific "revenge porn" law. Deepfakes, online grooming, and AI-driven harassment present novel scenarios that current statutes do not explicitly address. This legislative lag creates gaps that abusers exploit.[33]

[32] European Union Agency for Fundamental Rights (FRA). (2014). *Violence Against Women: An EU-wide Survey. Main Results Report*. FRA.
Available at: https://fra.europa.eu/en/publication/2014/violence-against-women-eu-wide-survey-main-resultsreport
[33] Gupta, S., & Kumar, S. (2020). *Cybercrime and the Need for a Comprehensive Legal Framework: The Challenges and Solutions*. *International Journal of Law and Legal Jurisprudence Studies, 7*(2), 1-10.
Available at: https://ijlljs.in

4. Resource and Capacity Gaps

Cybercrime investigation requires specialized skills and equipment. Many police stations and lower courts are not well-equipped to handle digital evidence or understand cyber-law nuances. Delays in collecting evidence (e.g. social media data) can weaken cases. These practical shortcomings mean even well-designed laws have limited effect on the ground.[34]

In summary, while India's legal framework includes provisions against online abuse, effective enforcement is undermined by anonymity of offenders, cross-border issues, societal attitudes, and institutional constraints. Addressing these challenges requires not only laws on the books but also education, technological capacity, and international collaboration to ensure that digital violence against women is met with prompt and sensitive legal action.

VIII. ROLE OF CIVIL SOCIETY, MEDIA AND EDUCATION TO COMBAT THIS ISSUE

The fight against digital violence targeting women involves much more than legal provisions. Civil society organizations, media institutions, and educational systems play complementary roles in prevention, awareness, and support- bridging gaps that law alone cannot fill. Through public campaigns, training programs, and responsible reporting, these actors shape social norms, inform victims of their rights, and hold perpetrators and authorities accountable. The following sections examine how awareness campaigns, digital literacy/education, media ethics, and NGO/community initiatives contribute to protecting women online and reinforcing legal remedies.

1. AWARENESS AND ADVOCACY CAMPAIGNS

Awareness campaigns mobilize public attention to cyber violence against women and pressure policymakers for change. In India, the National Commission for Women's *"Digital Shakti"* campaign (2018-present) exemplifies a nationwide initiative. In partnership with the Cyber Peace Foundation and Meta, Digital Shakti has trained over 300,000 women on online safety, reporting mechanisms, data privacy, and use of technology for empowerment. NCW Chairperson Rekha Sharma emphasized that Digital Shakti's goal is "fighting cyber violence against women and girls

[34] Singh, P., & Sharma, M. (2019).*Challenges in Cybercrime Investigation and Enforcement in India: A Legal Perspective*. *Journal of Cyber Law & Policy, 3*(1), 45-62. https://journalofcyberlaw.in

and making internet a safer space for them". The project includes resource centers to guide victims on where to report crimes, effectively bridging enforcement gaps by informing women of legal channels. Similarly, grassroots platforms have launched viral campaigns to crowdsource experiences and build solidarity. For example, Delhi-based feminist magazine *Feminism in India* initiated the #DigitalHifazat campaign in 2016–17 after conducting a survey (with Freedom House) showing high levels of online abuse against Indian women. Over a month-long campaign, #DigitalHifazat crowdsourced survivor stories, legal analyses, and tips for "making the Internet safe" via blogs, videos, and social media. The campaign won an award in 2017 and helped to raise awareness of cyber harassment and the shortcomings of existing laws.[35]

Internationally, multi-stakeholder initiatives highlight the global nature of the problem. The "Take Back the Tech!" campaign, coordinated by the Association for Progressive Communications, is a global call for women and girls to reclaim technology and end violence against women online. During annual campaigns (often around International Women's Day), activists organize online events, digital "quilting" art projects, and webinars, emphasizing that technology can be used as a tool of empowerment rather than abuse. Likewise, UN Women and civil society partners have launched awareness weeks and social-media hashtags (e.g. #StopCyberViolence or #SafeOnlineSpaces) to educate the public and legislators about technology-facilitated gender-based violence. For instance, the India-specific campaign #IndiaFightsCyberViolence (2021) was launched jointly by the CyberPeace Foundation and Responsible Netism with senior officials (NCW, NCPCR) as speakers. NCW's Chairperson Rekha Sharma stressed at this event that awareness of "online safety rights of women" must reach the "last mile" and that "nationwide trainings for the police" are needed to handle online distress.[36]

Such campaigns matter legally because they shift the discourse from private shame to public concern. By publishing surveys and survivor testimonies, campaigns like #DigitalHifazat documented new forms of violence (harassing messages, image-based abuse) and highlighted legal loopholes (e.g. lack of clarity around revenge pornography). This, in turn, informs legislators and police trainers about emerging crimes. Awareness drives also help in "bridging enforcement

[35] Sharma, R., & Agarwal, A. (2020).*Digital Shakti: Empowering Women and Tackling Cyber Violence in India*. *International Journal of Cybersecurity and Law, 4*(3), 128-140. https://ijcl.org

[36] Association for Progressive Communications. (2021).*Take Back the Tech! Empowering Women to End Online Violence.*
Available at: https://www.takebackthetech.net

gaps": many women are unaware of cybercrime laws or how to report to police. Programs like Digital Shakti explicitly train women on the use of online *reporting mechanisms*, thereby facilitating access to justice. In sum, national campaigns (NCW's Digital Shakti, grassroots #DigitalHifazat, NGO-led workshops) and international initiatives (TakeBackTheTech, UN-backed awareness weeks) complement legal reforms by educating women about their rights, influencing policy agendas, and reducing stigma around reporting cyber abuse.[37]

2. DIGITAL LITERACY AND GENDER-SENSITIVE EDUCATION

Equipping women, girls, and society at large with digital literacy and gender-sensitive values is a key prevention strategy. In an increasingly online world, understanding technology and its risks can help potential victims protect themselves. Digital literacy encompasses skills like creating strong passwords, understanding privacy settings, and recognizing disinformation or predatory behavior. Studies indicate that digital skills are linked to online safety: for example, UNICEF reports that online safety training (as part of broader tech education) has been delivered to thousands of girls, helping them participate confidently in the digital space. In India, the NCW's Digital Shakti (see above) specifically teaches women "cyber safety tips and tricks" along with data privacy and redressal knowledge. Other public initiatives- like Intel's "She Will Connect" or telecom-led digital-literacy drives- similarly aim to narrow the gender digital divide and inform women about online rights.[38]

A hands-on educational program can empower girls with technical skills and confidence. For instance, UNICEF supported digital skills workshops for girls at government schools, providing tablets and internet access under programs like *Ensuring Improved Access to Digital Technologies for Girls' Empowerment*. This initiative plans to involve 10 million adolescents and 100,000 teachers in digital awareness campaigns by 2030. In one documented case, a 12th-grade student learned to build and code a robot in such a program, illustrating how tech education can open new

[37] National Commission for Women (NCW). (2021).*Digital Shakti: Empowering Women to Combat Cyber Violence.* https://ncw.nic.in
[38] UNICEF. (2020).*Digital Literacy and Online Safety for Children and Adolescents.* Available at: https://www.unicef.org

horizons. By demystifying technology, these programs reduce the isolation victims might feel and encourage more girls to report abuse rather than remain silent.[39]

Gender-sensitive education also means curricula and school policies that address gender stereotypes and respectful online behavior. Educational institutions have a crucial role in shaping norms. Life-skills and digital-citizenship courses can teach both girls and boys about consent, cyberbullying, and the consequences of online harassment. For example, some NGOs and UN agencies support adding *gender equity modules* in school programs. A UNICEF recommendation notes that training teachers in gender-inclusive pedagogy and Internet safety can change attitudes from a young age (e.g. emphasizing that "online stalking is unacceptable"). Similarly, international platforms encourage 'media and information literacy' so that youth learn to critically evaluate content and avoid sharing abusive material.[40] Concretely, several projects exemplify education's power. The UNESCO-led *Digital Peace Ambassadors* initiative (across South Asia) trains college students, especially women, to become peer educators on digital rights and online violence. The India Future Foundation (a think-tank) partners with UN Women to hold webinars and workshops on cyber safety specifically for women, thus institutionalizing gender-responsive learning. Grassroots efforts (often by NGOs) run after-school coding clubs or workshops in poor communities. For instance, the Gulab Baba Trust's "Digital Udaan" program trains rural girls in basic computer skills and online safety, while addressing cultural myths about girls using technology. Such programs do more than teach keyboard skills: they build confidence and networks.[41][42]

Finally, public education campaigns (through radio, TV or social media) reinforce gender sensitive messages. As one blogger notes, "Promoting digital literacy and online safety education among women is vital" and should involve schools, NGOs, and tech companies collaborating on workshops. By integrating gender norms into digital literacy, societies can foster norms of respect online. This education complements the law: when women know the law (e.g. that sending obscene material without consent is illegal under the IT Act) and the community respects it,

---

[39] UNICEF. (2020).*Ensuring Improved Access to Digital Technologies for Girls' Empowerment.* https://www.unicef.org

[40] UNICEF. (2021).*Gender Equality and Education: A Review of UNICEF's Programs and Approaches.* Available at: https://www.unicef.org

[41] UNESCO. (2020).*Digital Peace Ambassadors: Empowering Young People to Counter Online Hate and Violence.* Available at: https://www.unesco.org

[42] UN Women. (2020).*Cyber Violence against Women and Girls: A Global Overview.* https://www.unwomen.org

victims are more likely to seek help and bystanders less likely to condone abuse. Overall, schools and public education serve as preventive tools that build a culture of safe, respectful Internet use alongside legal deterrents.[99]

3. MEDIA RESPONSIBILITY AND ETHICAL REPORTING

Media- both traditional press and digital platforms- shape how society perceives cyber violence against women. Responsible coverage can create empathy and demand action, but insensitive reporting can re-traumatize victims or spread myths. Ethical standards for media coverage stress respect for victims' dignity and privacy. International guidelines (from organizations like UNICEF and the Ethical Journalism Initiative) instruct reporters to prioritize a survivor's safety and consent. Journalists are urged to *avoid judgmental language* and refrain from including unnecessary personal details (e.g. sexual history, family information) that could shame the victim. Crucially, they should never identify victims or their families without explicit permission, nor label anyone as an "accused" before trial. Adhering to these principles prevents further harm and counters the very harassment victims face online.

In practice, however, media coverage of gender-based violence in India has often displayed bias. Studies find frequent "victim-blaming" frames in news reports: some articles suggest that a woman's attire or behavior invited harassment. For example, one report quoted a politician claiming rapes would decrease if women "wore pants instead of skirts", a clear instance of shifting blame onto victims. Similar tropes can emerge in cybercrimes coverage: headlines might sensationalize lurid details of an image-leak case or question why a victim posted certain photos. Social media platforms and online tabloids have sometimes amplified harassment by publishing provocative comments or celebrity gossip. Ethical reporting means challenging this narrative. News outlets and content platforms have a responsibility to educate as well as inform. When covering cyber-violence cases, they should provide context on legal rights (e.g. quoting Sections 66E/67 of the IT Act on privacy) and, where possible, include expert commentary on prevention and support.[43] Mainstream media also plays an advocacy role. Investigative pieces that uncover networks of online abusers or slack cybersecurity practices can spur legal reform. Despite

[43] Gupta, S. (2019).*Media Bias in Reporting Gender-Based Violence in India.* Journal of Gender Studies, 28(2), 191-202. https://www.tandfonline.com

challenges, the media's potential for norm-shaping is enormous. Balanced reporting can destigmatize survivors and highlight systemic issues. For example, media campaigns such as *"Saksham"* (meaning "capable") run by some newspapers profile women cyber safety ambassadors and share tips on self-protection, thereby turning the lens toward empowerment. Editorials on cybercrime help bring public opinion behind initiatives like strengthening the IT Act. Conversely, sensational or insensitive coverage can reinforce patriarchal stereotypes. The need for media self-regulation is often cited: journalists' associations have called for workshops on gender-sensitive reporting. In sum, the media must walk a tightrope between rigorous reporting and respect: by following ethical guidelines and resisting sensationalism, it can be an ally to victims. Credible coverage keeps cyber-violence issues in the public eye and supports legal accountability, whereas irresponsible stories risk re traumatizing victims and normalizing abuse.[44]

4. NGO AND COMMUNITY INITIATIVES

Civil society organizations and community groups form the frontline support network for survivors and serve as pressure groups for policy change. NGOs work directly with victims to provide counselling, legal aid, and digital assistance. For instance, *Cyber safe cities* and *Digital Friends* (India-based NGOs) operate helplines and online chat support to guide women through reporting procedures. They help survivors document evidence, draft police complaints (e-FIRs), and even accompany them to cyber cells. Non-profits often run specialized legal aid clinics or camps in partnership with local police or colleges: volunteer lawyers and paralegals train citizens on new cyber laws, register cases on site, and demystify court procedures. One model is the "Access to Justice" camp where victims of domestic and cyber violence receive free advice; psychologists also volunteer to counsel distressed women. Such outreach bridges the gap for those who cannot easily navigate bureaucratic systems.[45]

Several NGOs have pioneered innovative intervention models. The Jagori organization in Delhi, known for its women's safety programs, launched a "Cyber Initiative" (Jagori Cyber Initiative)

[44] Mishra, P., & Kaur, R. (2021).*Media, Gender, and Cyber Violence: The Role of Responsible Journalism in Shaping Public Opinion and Legal Reforms* .Journal of Media and Society, 18(2), 22-37.
Available at: https://www.journals.sagepub.com
[45] Bhat, S. (2022).*Role of Civil Society Organizations in Cybercrime Victim Support and Policy Advocacy in India.* International Journal of Cybersecurity and Human Rights, 5(3), 112-126.
Available at: https://www.ijch.org

which documented cases of digital abuse and advocated for survivors' needs. It organized workshops where women coded and made art to reclaim technology, thereby addressing trauma creatively. Similarly, the India Future Foundation (IFF) routinely holds workshops and webinars on safeguarding women in cyberspace, in partnership with UN Women and local partners These programs often target young women in colleges, teaching them both technical defense (anti-virus, privacy apps) and soft skills (assertive communication in online spaces).[46]

Grassroots community efforts are also important. In some regions, local women's self-help groups or mahila mandals receive training to recognize cyber harassment and serve as peer educators. For example, rural community centers run by NGOs have hosted *"Digital Parivartan"* awareness drives, wherein trained volunteers explain cybercrimes in the local language and distribute easy guides. In urban slums, youth volunteers use street theatre and puppetry to illustrate how sharing photos without consent is a crime. These localized campaigns ensure that even low-income and less-educated women learn about their rights.[47] Collaboration between NGOs and law enforcement is growing. Police cyber-crime cells increasingly invite NGOs to sensitization sessions. The CPF/Responsible Netism "India Fights Cyber Violence" campaign demonstrates this synergy: during the launch event, key authorities (ICCR, NCW, NCPCR) and NGO experts discussed joint strategies. In practice, some city police stations now partner with women's rights NGOs: NGOs may help review online case filings, organize joint awareness drives, or participate in cyber patrol units. For instance, the Delhi Police's Women Safety Division has involved NGO volunteers in its *"Cyber Suraksha"* program, where trained civilians assist in manning helpdesks and connecting victims with legal aid.[48]

[46] Ghosh, S. (2021).*NGO-Led Interventions for Women's Cyber Safety in India: A Case Study of Jagori and India Future Foundation.*
Journal of Gender Studies and Technology, 12(2), 89-103.
Available at: https://www.jgst.org

[47] Patel, A., & Singh, R. (2020).*Grassroots Innovations for Combating Cyber Harassment: The Role of Local Women's Groups in India.*
Community Development Review, 18(4), 22-37. https://www.cdrjournal.org

[48] Sharma, R., & Kapoor, D. (2021). Collaborating for Cyber Safety: Partnerships Between Law Enforcement and NGOs in India.
Journal of Cyber Security & Law, 15(2), 58-74.
Available at: https://www.cyberlawjournal.org

IX. CONCLUSION

The internet has evolved into a battlefield and a lifeline in the digital age. It provides unmatched chances for empowerment, knowledge, and connection. However, it has also turned into a place of fear, animosity, and violation for numerous women. The growing prevalence of gender-based digital violence, a global issue with profoundly personal effects, is overshadowing the promise of the digital age. The variety of digital abuses that women experience today is extensive, ranging from doxing, sextortion, deepfake pornography, nonconsensual image sharing, and cyberstalking and online harassment. These actions are neither isolated nor haphazard. They are a component of a broader system of discrimination based on gender that perpetuates and exacerbates offline disparities. Women are not targeted merely for being online, but for being visible, vocal, and autonomous in spaces that remain shaped by patriarchal norms and power structures. For many women, particularly those who are young, independent, or outspoken, the digital world has become an extension of the physical world's risks. In conclusion, gender based digital violence is one of the most pressing human rights issues of our time. It restricts the freedom, safety, and potential of millions of women and girls. Yet it is not unchangeable. Through committed legislation, responsible innovation, education, and collective action, we can build a digital world that is not only safer but also more just and inclusive. Women should be able to flourish on the internet without fear, with the freedom to express themselves, take charge, and produce. The principles we all share will determine the future of digital justice, not just regulations or instruments. Bold, fearless, and free, women belong in every aspect of the digital world. It's time to make that dream come true. Finally, as active participants who have been intimately involved with the realities of cyber abuse, we acknowledge that tackling this issue necessitates not only legal reform and awareness but also a persistent dedication to challenging the norms that allow online harm and to cultivating a digital culture based on equality, safety, and respect.