 DOI: 10.5281/zenodo.18004484

CYBER HARASSMENT AGAINST WOMEN: A SILENT DIGITAL PANDEMIC

By V. ISWARIYALAKSHMI[1]

ABSTRACT

In India, the exponential growth of the internet, social media use, and the digital financial system has brought transformative opportunities for women across the globe. However, it has also given rise to a disturbing parallel reality. In recent cases, targeted cybercrime, especially against women, has increased. These offences, ranging from online harassment and stalking to morphing, deepfake abuse, financial fraud, and trafficking, have become a silent digital pandemic, spreading rapidly yet often remaining underreported. This silent digital pandemic not only causes psychological trauma and reputational damage but also restricts women's freedom of expression, digital participation, and economic opportunities. This article examines the nature, causes, impact, and legal responses to cybercrime against women, while arguing for stronger social, technological, legal, and psychological frameworks that can safeguard women's digital autonomy. To break this silent cycle, we need a powerful combination of legal enforcement, technological innovation, digital education, and awareness among women.

INTRODUCTION

As digital technology becomes inseparable from daily life, women increasingly use online platforms for education, entrepreneurship, social networking, and professional growth. However, the same digital spaces have become hostile environments where misogyny, violence, and discrimination thrive in new, technologically advanced forms. Cyber harassment against women is not merely an online inconvenience—it is a serious violation of fundamental rights, safety, and psychological well-being.

[1] Author is a law student at Government Law College Ramanathapuram.

What makes this issue a silent digital pandemic is its scale, speed, anonymity, and invisibility. While millions of cases occur globally, only a fraction are reported due to stigma, fear, and limited awareness. Unlike physical crimes, cybercrimes operate 24/7, without geographical boundaries, and allow perpetrators to remain anonymous. This anonymity emboldens offenders and intensifies the vulnerability of women. As a result, cybercrimes against women have quietly evolved into a persistent, pervasive threat—a digital pandemic affecting millions. Cyber harassment is not just a crime; it is a crisis of safety, dignity, and equality in the digital age, and it has also emerged as one of the most alarming social challenges of the 21st century. In recent years, India has witnessed an unprecedented spike in cybercrimes targeting women, fuelled by the explosive growth of smartphones, cheap data, and AI-powered tools capable of creating realistic deepfake images within seconds. From teenage girls to working professionals, influencers, activists, and homemakers, no woman is untouched by the risk of digital violence. This article explores the depth of the issue while offering insights into prevention, policy, and empowerment. It highlights the urgent need for stronger laws, faster cyber-cell responses, digital literacy, ethical tech development, and societal attitudes that refuse to blame victims.

FORMS OF CYBER HARASSMENT AGAINST WOMEN

Forms of cyber harassment against women refer to any intentional, repeated, harmful, or threatening behaviour carried out through digital technologies, including mobile phones, social media platforms, messaging apps, emails, and online forums. Unlike physical harassment, cyber harassment is boundaryless—it can occur anytime, reach a global audience instantly, and often remains anonymous. Women are disproportionately targeted due to social prejudices, gender stereotypes, and the rise of digital spaces where misogyny can spread without accountability. Cybercrimes targeting women take several distinct and evolving forms. The major categories include:

1. CYBER STALKING

Cyberstalking refers to persistent and unwanted monitoring of a woman's digital life. Offenders may repeatedly track her social media activity, scan her online status, follow her across platforms, or use spyware to gather information.

2. ONLINE SEXUAL HARASSMENT

Online sexual harassment against women includes any unwanted sexual content, messages, gestures, or approaches made online. Women face this routinely on platforms like Instagram, Facebook, WhatsApp, and gaming apps. Examples include sexualised comments on posts, unsolicited sexual messages, and the sending of obscene images or videos. Its impact includes fear of engaging online and damage to careers, especially in public-facing professions.

3. MORPHING & DEEPFAKE ABUSE

Morphing involves altering a woman's photo to create false or explicit imagery. Deepfake abuse uses AI to superimpose a woman's face onto sexual videos. Current trends show that deepfake cases have doubled in 2024–2025 due to easy-to-use apps like face-swap tools. Deepfakes ruin a woman's reputation instantly.

4. CYBERBULLYING & ONLINE TROLLING

Women—especially students, influencers, celebrities, journalists, and activists—face targeted online abuse meant to intimidate, silence, or shame them. Its forms include:

• Mass hate speech

• Body shaming, slut-shaming

• Threats of violence or rape

• Ridiculing appearance, profession, or opinions

5. DOXXING (PUBLISHING PERSONAL INFORMATION)

Doxxing is the deliberate public release of sensitive personal details such as home address, phone number, workplace, email ID, and family details. The dangerous risks include stalking, physical assault, and continuous harassment from strangers. Women are especially vulnerable as it compromises both digital and physical safety.

6. CYBER BLACKMAIL & EXTORTION

Women are threatened online with exposure of personal information, morphed photos, or fabricated content. For example: "Pay money or we will leak your photos." This is often done

through WhatsApp, Telegram, or unknown numbers. It involves threatening to release morphed or intimate images to force money transfers, sexual favours, silence, or compliance.

7. CYBER GROOMING

Adults manipulate underage girls online to exploit or sexually abuse them. This often occurs through gaming platforms, Instagram or Facebook, and WhatsApp or Telegram groups. Women and girls are manipulated into conversations or relationships that expose them to trafficking networks or sexual exploitation. This is one of the fastest-emerging online threats for school and college girls.

8. VOYEURISM & SPY-CAMERA CRIMES

Hidden cameras in changing rooms, PG hostels, washrooms, and hotels capture women without consent. For example, videos are uploaded on porn sites, shared on Telegram/WhatsApp groups, or sold for money. This form of cyber harassment is deeply traumatic and long-lasting.

9. REVENGE PORN / NON-CONSENSUAL INTIMATE IMAGE SHARING

This happens when intimate images shared privately, often within relationships, are leaked, posted, or used to humiliate women. Examples include an ex-partner posting photos after a breakup, threatening to leak videos for money, or circulating content among friends or online groups.

10. PHISHING, FRAUD & IDENTITY THEFT TARGETING WOMEN

Women are increasingly targeted by fraudsters using emotional manipulation or fake opportunities. For example: “Click this link to win a scholarship/job/gift.” This can lead to financial loss, emotional trauma, and data theft.

11. IMPERSONATION & FAKE PROFILES

Offenders create profiles using a woman’s name, photos, or identity. The purpose is to send abusive messages, mislead people about her character, lure victims while pretending to be her, or damage her reputation socially or professionally. For example, creating a fake account using a woman’s photos without consent.

12. MISOGYNISTIC ONLINE HATE SPEECH

Gender-based hate speech is used to degrade women collectively or individually. It includes remarks about "women belonging at home," slut-shaming, rape threats, and public humiliation. This affects women's participation in public discourse and democratic spaces.

CONSTITUTIONAL AND LEGAL FRAMEWORK FOR WOMEN AGAINST CYBERCRIME

Cyber harassment against women is not only a criminal offence but also a violation of fundamental constitutional rights. India's legal system provides multi-layered protection through the Constitution of India, the Information Technology Act, 2000, and the newly implemented Bharatiya Nyaya Sanhita (BNS), 2023, and the Bharatiya Sakshya Adhiniyam (BSA), 2023.

CONSTITUTIONAL SAFEGUARDS FOR WOMEN AGAINST CYBERCRIME[2]

The Constitution guarantees fundamental rights that cyber harassment directly violates:

• **Article 14 –** Right to Equality Guarantees equality before the law and equal protection of laws to all citizens. Women must be treated equally in physical and digital spaces. Any gender-based online harassment violates this equality.

• **Article 15 –** Prohibition of Discrimination Prohibits discrimination on grounds of sex, religion, caste, race, or place of birth.

• **Article 15(3)** – The State can make special laws for women's safety. Cybercrime provisions for women fall under this enabling clause.

• **Article 19(1)(a) –** Freedom of Speech and Expression Guarantees freedom of speech and expression, movement, and the right to practise any profession.

• **Article 19(2) –** These freedoms are subject to reasonable restrictions in the interests of public order, decency, morality, security of the State, etc. Women have the right to express themselves freely online. Cyberbullying, trolling, and online abuse restrict this freedom. It also allows the government to take action against abusive, obscene, defamatory, or threatening content under

[2] Constitution of India Art. 14,15,15(3),19(1)(a),19(2).

"reasonable restrictions." This ensures that freedom of speech cannot be used as a shield to justify cyberbullying or revenge porn.

• **Article 21 –** Right to Life and Personal Liberty Guarantees the right to life with dignity, privacy, safety, and personal liberty. It protects women from non-consensual sharing of images, cyberstalking, doxxing, blackmail, surveillance, and online sexual exploitation, and forms the constitutional basis for privacy protection and data protection in India.

LEGAL FRAMEWORK FOR WOMEN AGAINST CYBERCRIME

• INFORMATION TECHNOLOGY ACT, 2000[3]

The Information Technology Act, 2000, is India's primary cyber law. Several sections directly protect women from cyber harassment.

SECTION 66A – Offensive Messages Punishment for sending offensive messages through communication services, etc. The punishment includes imprisonment for a term which may extend to three years.

SECTION 66C – Identity Theft Punishes the fraudulent use of a woman's digital identity, passwords, photos, or electronic signatures. The punishment may extend to three years and shall also be liable to a fine which may extend to one lakh rupees.

SECTION 66D – Cheating by Personation Punishment for cheating by personation using a computer resource. It deals with creating fake online identities to deceive, harass, or defame women. The punishment may extend to three years and shall also be liable to a fine which may extend to one lakh rupees.

SECTION 66E – Violation of Privacy Punishment for violation of privacy. It protects women from unauthorised capturing, sharing, or publishing of private images. The punishment includes imprisonment which may extend to three years, or a fine not exceeding two lakh rupees, or both.

SECTION 67 – Publishing Obscene Material Online Punishment for publishing information which is obscene in electronic form. The punishment includes imprisonment which may extend to

[3] Information technology act 2000 sec 66A,66C,66D,66E,67,67A,67B

three years and a fine which may extend to five lakh rupees, and in the event of a second or subsequent conviction, imprisonment which may extend to five years and a fine which may extend to ten lakh rupees.

SECTION 67A – Publishing Sexual Content Punishment for publishing or transmitting material containing sexually explicit acts, etc., in electronic form.

SECTION 67B – Child Sexual Content Punishment for publishing or transmitting material depicting children in sexually explicit acts, etc., in electronic form.

CRIMINAL PROTECTION UNDER BHARATIYA NYAYA SANHITA (BNS), 2023[4]

SECTION 75 – Sexual Harassment Punishable for unwelcome sexual remarks; showing pornography against a woman's will; and suggestive or obscene communications. It also includes online sexual harassment.

SECTION 77 – Voyeurism Capturing or watching a woman in private acts without consent, and disseminating such images, even digitally.

SECTION 78 – Stalking Repeatedly following or contacting a woman despite her disinterest, or monitoring her internet, email, or digital communications. It also covers cyberstalking.

SECTION 79 – Offensive Words, Gestures, or Acts Punishable for using words, sounds, gestures, or exhibiting objects meant to insult a woman's modesty or privacy.

BHARATIYA SAKSHYA ADHINIYAM (BSA), 2023 – EVIDENCE IN CYBERCRIME CASES[5]

DIGITAL EVIDENCE IS FULLY ADMISSIBLE

Chats, screenshots, emails, CCTV footage, metadata, phone logs, and cloud data are legally valid.

SECTION 61 – Electronic or Digital Records This section declares that all electronic or digital records are admissible as evidence in court.

[4] Bharatiya Nyaya Sanhita, Sec. 75, 77, 78, 79.
[5] Bharatiya Sakshya Adhiniyam, 2023, Sec. 61, 62, 63.

SECTION 62 – Content of Electronic Records This section links Section 61 to Section 63, clarifying that the content of electronic records must be proved in accordance with the conditions laid down in Section 63.

SECTION 63 – Admissibility of Electronic Records This is the key "computer output as document" provision. It provides that any information stored, recorded, or copied in electronic form—on magnetic media, optical media, semiconductor memory, or produced by a computer or communication device—is deemed a "document." Such data can be admitted in court proceedings as evidence without needing the original paper, provided certain conditions are satisfied, such as lawful custody and regular use of the device.

CAUSES BEHIND RISING CYBER HARASSMENT AGAINST WOMEN

• ANONYMITY & FAKE IDENTITIES

The ability to hide behind fake profiles, anonymous accounts, VPNs, and temporary numbers makes offenders feel safe. This anonymity encourages bold, aggressive, and abusive behaviour because they believe they cannot be traced.

• DEEP-ROOTED GENDER BIAS & MISOGYNY

Patriarchal attitudes and sexist mindsets spill into the digital world. Women are more frequently targeted with sexualised abuse, body-shaming, moral policing, threats, and blackmail. Gender-based hostility is one of the strongest drivers of cyber harassment.

• MISUSE OF SOCIAL MEDIA PLATFORMS

Social media gives offenders direct and unrestricted access to women. Common abuses include morphing photos, spreading fake news, revenge porn, stalking through DMs, and abusive comments. The fast, viral nature of social apps makes harassment easier and more frequent.

• LACK OF DIGITAL AWARENESS & CYBER SAFETY SKILLS

Many women are unaware of privacy settings, safe password practices, how to block or report offenders, legal protections, and the risks of sharing personal details. This digital knowledge gap increases vulnerability.

• WEAK LAW ENFORCEMENT & LOW REPORTING

Many incidents go unreported due to fear, shame, or lack of trust in the system. Even when complaints are filed, slow investigations, limited cyber-police resources, and low conviction rates embolden offenders. When criminals see that "nothing will happen," crimes increase.

• MISUSE OF AI TECHNOLOGY

Deepfake tools and AI-powered image manipulators allow offenders to commit sophisticated crimes.

STRATEGIES TO COMBAT THE DIGITAL PANDEMIC OF CYBER HARASSMENT AGAINST WOMEN

The rise in cyber harassment demands a multi-level response involving individuals, families, institutions, government agencies, technology platforms, and society. The following strategies address prevention, protection, enforcement, and empowerment.

• STRENGTHENING DIGITAL LITERACY & CYBER AWARENESS

Conduct awareness programmes in schools, colleges, workplaces, and communities, and teach every woman how to:

1. Set privacy controls
2. Identify fake profiles
3. Use strong passwords
4. Recognise phishing, stalking, and extortion
5. Secure bank and UPI accounts

Encouraging safe digital habits, such as not oversharing personal details, creates a great impact by empowering women to protect themselves and reducing vulnerability.

• LEGAL LITERACY & ENCOURAGING REPORTING

Spread awareness about laws such as the IT Act, 2000 (Sections 66E, 67, 67A, 67B) and provisions under the Bharatiya Nyaya Sanhita relating to stalking, sexual harassment, and identity theft. Promote the use of the NCCRP (National Cyber Crime Reporting Portal) and the 1930 cyber-fraud helpline. This creates a great impact by helping women report crimes confidently and ensuring faster action.

• STRENGTHENING CYBER LAW ENFORCEMENT

Increase specialised cyber police stations in all districts. Train police in digital forensics, cyber psychology, and victim-sensitive handling. Establish fast-track cyber courts to avoid delays. Improve tools for tracking anonymous and VPN-based offenders. This creates a great impact by ensuring quicker investigations and higher conviction rates.

• SOCIAL MEDIA ACCOUNTABILITY & PLATFORM-LEVEL SAFEGUARDS

Platforms must enforce:

1. AI-based detection of harassment
2. Quick takedown of obscene or harassing content
3. Stricter identity verification
4. Better reporting tools
5. Blocking mechanisms

Mandatory 24/7 content removal teams for sensitive cases like morphing and deepfakes reduce the spread of harmful content and protect victims.

• EDUCATION CURRICULUM INTEGRATION

Mandatory digital safety chapters in school curricula and college modules on cyber ethics, cyber law, and responsible social media behaviour create long-term digital responsibility.

• FAMILY & COMMUNITY SENSITISATION

Encourage families to support victims instead of blaming them, and educate parents about:

1. Monitoring online risks for teenagers
2. Teaching healthy digital behaviour
3. Recognising early warning signs of cyberstalking

This creates a supportive ecosystem that encourages reporting.

• MENTAL HEALTH & VICTIM SUPPORT SYSTEMS

Provide counselling centres and psychological support for victims. Establish safe spaces in schools and colleges for reporting without stigma. Create peer-support networks and helplines. This creates a great impact by helping victims recover emotionally and preventing long-term trauma.

• COLLABORATION WITH COMPANIES & NGOs

NGOs can conduct awareness workshops in rural and urban areas. Collaboration with platforms such as:

1. Meta (Facebook, Instagram)
2. Google
3. YouTube

helps strengthen safety features and creates a united and technologically strong defence system.

CASE LAWS ON CYBER CRIME AGAINST WOMEN

STATE OF TAMIL NADU v. SUHAS KATTI (2004)

This was the first conviction in India for online harassment involving obscene and defamatory messages under the Information Technology Act, 2000. In this case, the accused sent obscene and defamatory messages in a Yahoo message group using a fake email account (impersonation) and forwarded sexual and defamatory emails in the victim's name. This resulted in harassment, and the victim received phone calls from strangers who believed she was soliciting sex work. The accused was convicted under Section 67 of the IT Act (for obscene content) and IPC Sections 509 (outraging modesty) and 469 (forgery). The court awarded imprisonment and a fine.

RITU KOHLI v. MANISH KATHURIA (2001)

(First cyber-stalking case in India)

In 2001, a woman (Ritu Kohli) reported that someone was using her identity on a chat platform, giving out her phone number and address, and using obscene language through the website (www.mirc.com), which led to her receiving dozens of harassing phone calls from strangers at odd hours. The accused (Manish Kathuria) was charged under IPC Section 509 (outraging the modesty of a woman), as at that time the IT Act was not fully equipped to deal with cyberstalking.

STATE OF WEST BENGAL v. ANIMESH BOXI (2017–2018)

In this case, the accused (Animesh Boxi) had a relationship with the victim and obtained intimate photos and videos under the promise of marriage. After the breakup, he uploaded them on pornographic websites and social media without her consent, exposing her identity. He was convicted under multiple IPC sections, including 354A (sexual harassment), 354 (voyeurism), 354D (stalking), and 509 (outraging modesty), and under IT Act sections such as 66, 66E, and 67/67A. The court sentenced him to five years' imprisonment and a fine of ₹9,000. The court also recognised that harm to the victim's reputation and dignity, even without physical violence, constitutes "injury."

CONCLUSION

Cyber harassment against women is not just a technological wrongdoing; it is a violation of dignity, identity, and freedom. In a world where screens have become spaces of expression and

empowerment, no woman should ever fear logging in, speaking up, or simply being visible online. The rising tide of cyber misuse is a reminder that misuse of technology is never a failure of women—it is a failure of society to protect them.

Every law enacted, every case fought, and every voice raised brings us one step closer to a safer digital space. When women protect themselves, they strengthen the future of our democracy, our humanity, and our shared online world. Let us commit to a culture where respect travels faster than hate, where empathy overpowers anonymity, and where safety is not a privilege but a right. A society that protects its women both online and offline is a society that protects its future.

To break this silent cycle, we need a powerful combination of legal enforcement, technological innovation, digital education, and cultural change. When women feel safe online, they thrive offline as well, shaping stronger opportunities and a more inclusive future.

“Your voice is your power. Your safety is your right. Your digital freedom is non-negotiable.”