Volume 1, Issue 2 , July - December 2025, Pg. 62- 73

Journal of Asian Law College ISSN: 3107-3859 (Online)

6

Cyber Violence Against Women in India: A Comparative Socio-Legal Study with International Conventions

Noyonika Gogoi,
Assistant Professor of Law,
Asian Law College, Noida,
Phd Research Scholar, Department of Law and Public Policy of Law, Sibsagarh University, Assam

Dr. Deepom Baruah
HOD, Department of Law and Public Policy of Law,
Sibsagarh University, Assam

ABSTRACT

The rapid growth of digital technology has advanced communication, education, and e-commerce, but it has also created avenues for new forms of gender-based violence. Women are particularly vulnerable to cyberstalking, online harassment, doxxing, deepfake exploitation, revenge pornography, and the circulation of non-consensual intimate images. These violations not only occur in cyberspace but also lead to severe consequences in the real world, including psychological trauma, reputational harm, and social exclusion, thereby threatening women's constitutional rights to dignity, equality, and privacy.

To address such crimes committed through technology, India has developed strong legal frameworks. Cyber gender violence is primarily governed by the Information Technology Act, 2000, and the Bharatiya Nyaya Sanhita, 2023 (BNS), which replaced the Indian Penal Code and recent laws related to cybercrimes. Judicial directives have further strengthened this framework by mandating measures to block and prevent the circulation of non-consensual intimate images and to curb such crimes effectively.

Despite these measures, significant gaps persist. The current laws remain largely reactive rather than preventive, lack gender-sensitive framing, and fail to adequately address technologically advanced crimes such as AI-generated deepfakes and persistent online hate speech. This paper critically examines the adequacy of the existing legal

Keywords
Gender Equality, Transparency, Governance, Accountability, Sustainable

Gupta, Priya, "Cyber Crime Against Women in Indian Context: An Overview," Journal of Humanities and Social Sciences, Vol. 8, Issue 1, 2025, pp. 175–179.

Sankhwar, S., "Cybercrime in India: An Analysis of Crime Against Women," Security and Privacy, Wiley Online Library, 2024.

Ibid.

Vidani, J., "Empowering Women in the Digital Sphere: Cyber Crime Combat Strategies in Indian Social Media," SSRN Electronic Journal, 2024.

framework and argues for reforms that incorporate gender-sensitive definitions, proactive intermediary accountability, trauma-informed policing, and digital literacy initiatives. This paper further studies the international conventions such as CEDAW, ICCPR, ICESCR and Budapest Convention to strengthen India's cyber laws by doing a comparative study. It is important to strengthen cyber laws to safeguard women's rights and ensuring substantive equality in the digital era.

INTRODUCTION

Cybercrime, often described as unlawful activity carried out with the help of technology, is not as modern a phenomenon as it is commonly assumed. Its roots can actually be traced back to the 18th century, with one of the earliest documented cases taking place in France in 1834. Over time, the arrival of the internet and later the World Wide Web fundamentally changed the way people communicate and do business, but it also provided fertile ground for new forms of criminal behaviour.

In India, the digital revolution has brought profound socioeconomic changes, opening doors for trade, education, and global connectivity. Yet, alongside these opportunities lies a troubling reality i.e. the rapid rise of cybercrimes, many of which disproportionately target women. Online harassment, cyberstalking, and abuse have increasingly escalated into serious crimes such as revenge pornography, identity theft, and defamation.

Technology is celebrated for enhancing access to knowledge and enabling instant communication, but its misuse has become one of the major reasons behind the alarming growth of cyber offenses. This dual nature of technology and its potential to empower and its capacity to harm makes it a complex challenge to regulate.

For women in particular, the internet initially symbolized empowerment and provided new avenues for education, employment, and self-expression. Digital platforms became essential to daily life, reshaping personal relationships and professional opportunities. However, this dependence also exposed women to fresh vulnerabilities. Over the years, harassment in online spaces has grown in both scale and intensity, with crimes like cyberstalking, impersonation, and circulation of intimate images becoming increasingly common.

A major contributing factor is the lack of awareness about how social media platforms and communication technologies such as WhatsApp, Skype, and Facebook actually operate. Limited digital literacy, coupled with insufficient knowledge of evolving technologies, has created fertile ground for abuse. Women often fall victim to perpetrators they know personally, as misplaced trust leads to the sharing of private information. In many cases, this trust is later exploited to commit online crimes.

Another barrier to tackling the problem is underreporting. Social stigma, fear of reputational damage, and the difficulty of collecting digital evidence often prevent women from lodging complaints. This silence allows offenders to act with impunity and further entrenches gendered violence in cyberspace. Studies show that such crimes are rising sharply worldwide, with the safety of women in the digital sphere remaining a pressing concern.

The present study highlights the nature and scope of cybercrimes against women in India, exposing gaps in both existing laws and their enforcement. Findings suggest that stalking, harassment, and the non-consensual circulation of intimate content are

"Cyber Crimes Against Women," ResearchGate, 2025, https://www.researchgate.net/publication/391409693_CYBER_CRIMES_AGAINST_WOMEN

"Cybercrime in India: An Analysis of Crime Against Women," Security and Privacy, Wiley Online Library, 2024, https://onlinelibrary.wiley.com/doi/full/10.1002/spy2.340

"Social Media and the Cyber Crimes Against Women: A Study," ResearchGate, 2025, https://www.researchgate.net/publication/364492160_Social_Media_and_the_Cyber_Crimes_Against_Women-A_Study

among the most widespread violations. Yet, a significant number of these cases remain unreported due to victims' lack of faith in the justice system and limited awareness of legal safeguards. The evidence indicates that the current legislative framework in India is not adequately equipped to address these issues. To improve the situation, stronger training for law enforcement officials, enhanced resources for cybercrime investigation, and nationwide campaigns promoting cyber literacy are urgently needed. These steps are essential to empower women, both by informing them of the risks and by making them aware of their rights and available remedies.

2. CLASSIFYING CYBERCRIMES

Cybercrime can be understood as unlawful activities carried out through technology, especially computers. In such cases, the computer itself may serve as the main target, be misused as an instrument for committing conventional crimes in new forms, or be employed to spread harmful software intended to damage or erase digital information.

Internet crimes are broadly classified into three categories. The first category covers those who break into computers but only get access. The second type consists of offenders who utilise technology to continue committing traditional crimes like theft or fraud. The third category includes persons who produce or distribute destructive programs, like as viruses, Trojan horses, or logic bombs, with the intent of causing information or network disruption.

Certain types of cybercrime resemble traditional offences but are aided by the internet. For example, the World Wide Web has become a platform for fraud, scamming, and cheating. Similarly, crimes committed via email can include extortion, cyberstalking, threats, defamation, email bombing, financial fraud, and the release of harmful code. Even platforms like Usenet newsgroups and Internet Relay Chat (IRC) have been used as gateways for illegal behaviour.

International organisations such as Interpol divide cybercrime into six broad categories. These include unauthorised access to systems, intercepting or modifying computer data, and engaging in computer-enabled fraud. Another method of categorising these crimes is to consider either the computer's participation in the offence or the sort of victim implicated. Cybercrimes can be directed at people, corporations, national security, or even the whole economy, depending on how the victims classify them. They can also be classified by content, the aim of the crime, or the identities of the perpetrators for example, distinguishing between insiders with privileged access and outsiders breaking systems from the outside.

3. OVERVIEW OF CYBER CRIMES AGAINST WOMEN

Crime has always adapted with time, reflecting changes in society, technology, and human interaction. Violence, abuse, and harassment against women are unfortunately not new, but the digital era has opened up new avenues for such exploitation. Cybercrimes against women are now one of the most pressing challenges of the modern age. These crimes make use of technology to inflict psychological and emotional harm, and at times, even physical danger,

Beliriya, N., "Cyber Crime Against Women in India: Legal Challenges and Solutions," International Journal of Law Management and Humanities, Vol. 3, Issue 5, 2020, pp. 1012–1022.

Ibid.

Uma, M. S., "Outlawing Cyber Crimes Against Women in India," Bharati Law Review, Vol. 3, Issue 2, 2017, pp. 103–116.

UN Women, "Technology and Violence Against Women Framework," 2014, <www.empowerwomen.org/ict4d

Kovacs, A., "Don't Let it Stand! An Exploratory Study of Women and Verbal Online Abuse in India," Internet Democracy Project, 2013,

thereby extending the inequalities women already face offline into the online world.

The roots of gendered violence in cyberspace began to emerge in the early 2000s, when internet access became more widespread. With the rise of social media, instant messaging, smartphones equipped with cameras, and cloud-based sharing systems, privacy in both real and digital spaces have been steadily eroded. Today, women across all backgrounds whether teenagers, homemakers, professionals, activists, celebrities, or even those with little to no digital literacy face the risk of online abuse. The Council of Europe has acknowledged that cyberviolence is a growing concern worldwide, and the COVID-19 pandemic only accelerated this trend. Since cyberviolence primarily targets women and girls, it undermines gender equality and directly violates women's rights.

Data from the International Telecommunication Union (ITU) in 2017 revealed that in nearly two-thirds of the world's countries, men access the internet more frequently than women. This digital divide highlights not only the exclusion of women from the benefits of technology but also their increased vulnerability when they are online. Many women are unaware of their legal rights in cyberspace and fear social stigma if they report incidents. This silence makes them "easier targets" for offenders. Social media platforms, messaging apps, and discussion forums are often weaponized against women through harassment, stalking, and abuse. Disturbing practices such as revenge pornography, doxing, and cyberstalking aim specifically to humiliate women and strip them of their dignity, with long-lasting impacts on their mental well-being.

A major reason cybercrime thrives is the anonymity that the internet provides. Unlike crimes in the physical world, which usually require presence or proximity, online offenses can be carried out from thousands of miles away. This anonymity emboldens perpetrators, allowing them to act without immediate fear of consequences. At the same time, gaps in digital literacy particularly a lack of awareness about privacy settings, cyber hygiene, and reporting mechanisms expose women to greater risks.

Women are disproportionately affected by certain categories of cyber offenses, including identity theft, phishing, extortion, defamation, impersonation through fake profiles, image morphing, circulation of explicit content, cyber pornography, online bullying, and persistent harassment. Whether motivated by a desire to intimidate, control, or shame, these acts violate not only privacy but also personal dignity. For many women, the effects are profound, creating fear and silencing their participation in online spaces.

This discussion sets the stage for examining different forms of cybercrimes committed against women, their prevalence, and the urgent need for stronger protective mechanisms.

• Cyberstalking

Cyberstalking is one of the most common forms of online abuse faced by women. It involves persistent and targeted harassment carried out through digital channels such as social media, emails, or instant messaging. The underlying purpose is often to intimidate, dominate, or control the woman. Typical behaviors include sending repeated unwanted messages, issuing threats, impersonating the victim, spreading degrading remarks, or exposing private

http://Internetdemocracy.in/wp-content/uploads/2013/12/Internet-Democracy-Project-Women-and-Online-Abuse.pdf
Ibid.
Supra, Note 1.
Nath, S. S., "Hear Her Fear: Data Sonification for Sensitizing Society on Crime Against Women in India," arXiv, 2020, https://arxiv.org/abs/2009.14182
Ibid.
Supra, note 2.

information. What makes cyberstalking particularly damaging is the gendered nature of the abuse, often accompanied by sexual threats or misogynistic comments. Victims are left feeling unsafe, anxious, and fearful, which forces them to restrict both their online presence and real-world interactions.

• Image-Based Sexual Abuse

Image-based sexual abuse occurs when intimate or sexually suggestive images of women are created, shared, or manipulated without their consent. This includes practices like "revenge porn," deepfake pornography, hidden-camera recordings (such as upskirting), and the non-consensual sharing of private photos. Sometimes these images are obtained through hacking, while in other cases, partners themselves distribute them after relationships sour. The aim is often to shame, blackmail, or control the victim, damaging her reputation or coercing her into submission. Since digital media can be endlessly circulated, the harm caused is profound and long-lasting.

• Doxing

Doxing refers to the deliberate exposure of someone's private details such as home addresses, phone numbers, workplace information, or even intimate data without consent. By making such information publicly available, offenders enable others to harass, stalk, or threaten the victim, both online and offline. For women, this practice carries particularly serious risks, as it often escalates into real-world violence or intimidation. Doxing strips women of their sense of security, making them vulnerable to unsolicited contact, abuse, or worse.

•Impersonation

Impersonation in cyberspace occurs when an offender pretends to be someone else, or even the woman herself, with the intent to deceive, harass, or damage reputations. In one form, the perpetrator may pose as a friend, colleague, or romantic interest to trick the woman into sharing personal information or intimate images (commonly known as "catfishing"). In another form, the offender may create a fake account using the woman's identity and post false or damaging content in her name. Both types of impersonation not only harm the victim's credibility but also facilitate related crimes such as blackmail or defamation.

• Online Defamation

Online defamation, or cyber libel, involves the publication of false statements, rumors, or accusations about women through digital platforms. These could appear on social media, blogs, comment sections, or even news sites. The defamatory content may allege immoral, criminal, or inappropriate conduct with the clear intent of damaging the woman's reputation. Unlike traditional defamation, the online medium magnifies the harm: once posted, defamatory material can be rapidly shared, stored, and searched, ensuring that the reputational damage persists long after the original content is taken down.

• Trolling

Trolling is a form of targeted harassment where offenders deliberately post inflammatory, abusive, or insulting comments directed at women online. Trolls often focus on women's personal attributes such as appearance, sexuality, or opinions, resorting to slurs, sexual harassment, or even threats of rape and violence. The attacks can take the form of memes, derogatory hashtags, or coordinated campaigns that flood a woman's online presence with abuse. Trolling

"Cyber Crime Against Women in India: A Critical Analysis," Law Journals, Vol. 5, Issue 2, 2019, pp. 1–6.
Ibid.
Ibid.
Vidani, J., "Empowering Women in the Digital Sphere: Cyber Crime Combat Strategies in Indian Social Media," SSRN Electronic Journal, 2024.
Id.
Supra, note 2.

not only humiliates victims but also attempts to silence their voices in digital spaces.

• Sextortion

Sextortion is a form of sexual blackmail that exploits technology. In such cases, a perpetrator threatens to release a woman's intimate photos or videos unless she complies with demands for money, sexual favors, or further explicit content. Sometimes the images are genuine, obtained from hacked devices or shared in trust, while at other times, fabricated materials such as deepfakes are used as leverage. Regardless of the method, the goal is to humiliate, control, or extort the victim. The fear of exposure forces women into silence, making sextortion a deeply coercive form of cybercrime.

‘

4. CRIMES AGAINST WOMEN: SOCIAL, PSYCHOLOGICAL & JURISPRUDENTIAL DIMENSIONS

Discrimination and violence against women have persisted across centuries, not only in India but in almost every part of the world. Rooted largely in patriarchal systems, where men occupy dominant positions of power, women are frequently relegated to subordinate roles, reinforcing inequality. In many societies, cultural traditions and religious interpretations assign women secondary status, emphasizing obedience, modesty, and domestic responsibilities. Such expectations restrict women's access to education and independence, discouraging their participation in public life.

Historically, limited access to education has been one of the most significant barriers to women's empowerment. Without education, opportunities for employment, financial independence, and leadership remain scarce. This lack of autonomy perpetuates economic dependence on male family members, reducing women's ability to make their own choices, leave abusive environments, or engage equally in society. Gender stereotypes that depict women as weak, overly emotional, or unfit for leadership roles further entrench these inequalities. As a result, daughters have often been perceived as burdens, leading to practices such as female infanticide and sex-selective abortion. Other harmful practices child marriage, dowry-related deaths, honor killings, domestic abuse, sexual harassment, female genital mutilation, and unequal wages reflect the continued subordination of women.

The roots of violence against women are not only social but also psychological. While social norms create structural inequality, individual behavior is shaped by personal insecurities, learned patterns, and distorted beliefs. Acts of violence often stem from a desire to dominate or control, which may arise from low self-esteem, poor impulse control, or childhood conditioning that normalized male superiority. In many situations, offenders are driven by ingrained misogynistic beliefs that view women as subordinate or as objects meant to satisfy male desires. Such perceptions strip women of their humanity, diminish empathy, and make it easier for perpetrators to rationalize acts of abuse. This mindset often manifests in crimes like sexual harassment, assault, stalking, exploitation, and blackmail. At the same time, many women continue to endure domestic violence, often because of economic dependence, fear of social judgment, or the persistence of rigid gender norms.

Justice K.S. Puttaswamy v. Union of India, (2017) 10 SCC 1.
Consumer Education and Research Centre v. Union of India, 1995 SCC (3) 42.

Crimes and discrimination against women are not isolated wrongs but reflect systemic inequalities and persistent violations of their legal and constitutional protections. These practices erode fundamental rights guaranteed by the Indian Constitution, including equality, dignity, liberty, and bodily autonomy under Articles 14, 15, and 21. Over the years, Indian courts have progressively broadened the interpretation of women's rights, aligning statutory provisions with constitutional values and India's commitments under international human rights frameworks such as the Convention on the Elimination of All Forms of Discrimination Against Women (CEDAW). Through purposive and transformative interpretations, the judiciary has sought to ensure that law serves as an instrument of social reform and gender justice.

Additionally, international human rights law emphasizes the "due diligence" principle, which imposes a responsibility on States to protect women from violence, regardless of whether the perpetrators are public authorities or private actors. A State's failure to establish, implement, or enforce effective legal protections not only undermines constitutional guarantees but also breaches international treaty obligations. In this light, India has introduced statutory measures designed to prevent, punish, and redress violations of women's dignity, autonomy, and bodily integrity.

5. INTERNATIONAL AND INDIAN LEGAL FRAMEWORK

The Constitution of India provides a strong framework to safeguard the interests of women. The Preamble, which is often regarded as a reflection of the vision of the Constitution's framers, sets out fundamental values such as dignity of the individual, liberty of thought, expression, faith, and belief, as well as equality of status and opportunity. It also upholds the principle of justice social, economic, and political thereby ensuring that discrimination of any kind, including gender-based, has no place in Indian democracy.

The Fundamental Rights enshrined in Part III apply equally to men and women, guaranteeing them protection against gender-based discrimination. A unique provision, however, exists in Article 15(3), which allows the State to enact laws specifically for the benefit of women and children. Such laws are not considered violations of the right to equality but rather tools for achieving substantive justice.

Another cornerstone is Article 21, which protects the right to life and personal liberty. Though brief in wording "No person shall be deprived of his life or personal liberty except according to procedure established by law" its scope has been significantly broadened by judicial interpretation. The Supreme Court has clarified that the right to life is not confined to mere survival or "animal existence." Instead, it extends to all elements essential for a life of dignity, including the rights to health, food, shelter, and even sleep.

In the digital age, cybercrimes against women directly threaten these constitutional guarantees. Acts such as cyberstalking, image morphing, and unauthorized circulation of private content violate a woman's right to privacy and dignity, both of which are recognized under Article 21. In the landmark judgment of Justice K.S. Puttaswamy v. Union of India , the Supreme Court explicitly recognized privacy as a fundamental right intrinsic to life and

liberty. Privacy, though undefined in the Constitution, essentially means freedom from unwarranted intrusion into personal life. This right is also reinforced under various international covenants like the Universal Declaration of Human Rights (UDHR) and the International Covenant on Civil and Political Rights (ICCPR).

Similarly, the right to health has been upheld as part of the right to life. In Consumer Education and Research Centre v. Union of India , the Court held that health and medical care are fundamental rights under Article 21. The World Health Organization also defines health not merely as the absence of disease but as complete physical, mental, and social well-being. Cybercrimes, especially those targeting women, often erode mental health and emotional security, thereby infringing this right.

Equally important is the right to dignity, which forms the foundation of all other human rights. A dignified life entails not only freedom from exploitation and abuse but also access to adequate living standards, safety, and respect. Cyber harassment, stalking, or circulation of obscene material directly undermines this core constitutional guarantee.

Apart from constitutional safeguards, the newly enacted Bharatiya Nyaya Sanhita (BNS), 2023, which replaces the Indian Penal Code, introduces several provisions to deal with technology-enabled crimes, including those against women.

• **Section 77** criminalizes voyeurism by penalizing the act of capturing or disseminating private images of women without consent.

• **Section 78** addresses stalking, including cyberstalking, covering repeated unwanted contact or monitoring through digital platforms.

• **Section 294** prohibits transmission of obscene content online.

• **Section 303** penalizes cyber theft involving devices, data, or software.

• **Section 336** deals with digital forgery aimed at damaging reputations.

• **Section 356** covers defamation, including defamatory online communications.

These inclusions highlight the legislature's intent to tackle emerging digital threats, particularly those that disproportionately affect women.

Additionally, the Information Technology Act, 2000 remains India's principal law on cybercrimes. Its provisions directly address online offenses against women. For instance:

• **Section 66E** penalizes non-consensual publication of private images.

• **Sections 67 and 67A** criminalize circulation of obscene or sexually explicit content, often invoked in cases of revenge porn.

• **Sections 66C and 66D** address identity theft and cheating by impersonation, commonly used in online blackmail.

• **Section 72** punishes breaches of confidentiality and privacy when personal data or images are misused.

Apart from criminal law, special legislations also

provide remedies in cyber contexts. The Protection of Women from Domestic Violence Act, 2005, for example, has been applied to digital abuse within households, such as surveillance through mobile apps or threats via social media. The Indecent Representation of Women (Prohibition) Act, 1986 also extends to the digital sphere, covering the online circulation of obscene or inappropriate depictions of women, whether in advertisements, websites, or social media platforms.

At the global level, international legal frameworks have increasingly acknowledged technology-driven violence against women. The Convention on the Elimination of All Forms of Discrimination Against Women (CEDAW, 1979), through its General Recommendation No. 35, broadened the understanding of gender-based violence to include forms of abuse such as cyberstalking and online harassment. Similarly, the Budapest Convention on Cybercrime—although not tailored specifically to gender issues—provides an important international framework for addressing offenses like data theft and unauthorized access, which often serve as the basis for online abuse. While India has yet to ratify this treaty, it continues to be regarded as a significant global instrument in combating cybercrime.

The Istanbul Convention (2011) explicitly addresses cyberstalking and digital sexual harassment, while the ICCPR (1966) guarantees privacy under Article 17, extending to non-consensual sharing of images or online surveillance.

Together, these constitutional protections, domestic laws, and international conventions form a robust but evolving framework aimed at addressing the growing menace of cybercrimes against women.

6. LACUNA IN THE EXISTING PROVISION OF LAW

Online verbal abuse that does not involve sexually explicit content often falls through the cracks of existing legal protections. For example, general sexist remarks or derogatory trolling are not adequately covered under Sections 499 and 507 of the IPC, which deal with criminal defamation and criminal intimidation. These provisions only address abuse of a personal nature, leaving out broader patterns of gendered harassment. Similarly, doxing the act of disclosing someone's personal information online remains unaddressed when it does not involve sexual content or intimidation. Although Section 66 of the IT Act penalizes hacking, it does not explicitly recognize doxing as a distinct offense, even when personal information is obtained through unauthorized access.

At present, trolling, verbal abuse, and doxing are treated as isolated personal crimes under provisions like Sections 499 and 507 of the IPC and Section 66 of the IT Act. However, the deeper issue is that such abuse is often directed at women precisely because of their gender. A review of past incidents shows that attacks frequently rely on stereotypes tied to a woman's sexuality, caste, or identity, making the harassment inherently gendered in nature.

While Section 66E of the IT Act and provisions such as Sections 354C and 354D of the Criminal Law (Amendment) Act, 2013 criminalize voyeurism and stalking, they are primarily limited to violations of physical privacy. These sections fail to address informational privacy, i.e., the misuse of personal

data in digital spaces. Similarly, Section 509 of the IPC, though it mentions privacy, restricts its scope to protecting women's "modesty." This reflects a broader problem in Indian law where sexual violence is conceptualized in terms of public morality and obscenity rather than being grounded in the principles of bodily integrity and personal autonomy. By framing such offenses as threats to modesty or public decency, the law reinforces patriarchal norms about controlling women's sexuality rather than ensuring protection of their inherent dignity and informational privacy.

Moreover, Sections 72, 43, and 66 of the IT Act approach privacy violations from an economic or property-based perspective, rather than treating them as gendered or social harms. This leaves a major gap in the legal framework, as women often face targeted psychological and informational violence online.

Equally concerning is the fact that psychological violence against women, when it occurs outside the family sphere, is not formally recognized in law. For example, the circulation of private information that is non-sexual in nature but still intended to humiliate or cause distress has not been classified as a form of gendered violence. Even progressive legislations such as the Protection of Women from Domestic Violence Act, 2005, which acknowledges psychological abuse within households and intimate relationships, do not extend to digital contexts or online harassment.

7. CHALLENGES IN ADDRESSING CYBER CRIMES AGAINST WOMEN

Cybercrimes targeting women in India have emerged as a pressing social and legal concern. Yet, despite increasing recognition of the issue, several systemic barriers continue to hinder effective prevention and redressal.

One of the foremost challenges lies in the limited resources available to law enforcement agencies. Cybercrimes are technologically complex and often demand specialized tools and expertise. However, many police units remain understaffed, underfunded, and inadequately equipped to deal with such cases. This resource gap frequently leads to delayed investigations, weak evidence collection, and ultimately low conviction rates.

Another obstacle is the low rate of reporting. Many women hesitate to approach authorities when subjected to online harassment or abuse due to fear of social stigma, victim-blaming, or retaliation. In other cases, the lack of awareness about their legal rights and remedies prevents victims from coming forward. Underreporting not only silences survivors but also makes it difficult for authorities to assess the actual scale of the problem and allocate resources effectively.

The legal framework itself poses challenges. Although the Indian Penal Code and the Information Technology Act, 2000, contain provisions addressing cyber offenses, gaps remain in their enforcement and interpretation. Inconsistencies in judicial application or a lack of clarity in certain provisions can result in unequal treatment of similar cases, weakening faith in the justice system.

Another pressing concern is the inadequate training of law enforcement agencies and members of the legal profession. Investigating cybercrimes requires

not only legal knowledge but also technical proficiency in areas such as digital forensics and cyber investigations. However, many police officers still lack the necessary expertise in handling electronic evidence, and a significant number of lawyers and judges remain unfamiliar with the complexities of cyber law. This gap in skills often results in procedural lapses and weak prosecutions, which in turn undermine justice and contribute to consistently low conviction rates.

In essence, crimes against women in cyberspace highlight not only the increasing risks to their security and dignity online but also expose the limitations of the legal system in effectively addressing such offenses. Without strengthening resources, improving reporting mechanisms, clarifying legal provisions, and ensuring specialized training, the problem will remain inadequately addressed.

8. GOVERNMENT INITIATIVES AND POLICIES

The Ministry of Home Affairs launched the National Cyber Crime Reporting Portal in 2018 as a centralized platform for citizens to lodge complaints related to cyber offenses. Through this portal, individuals can report incidents such as online fraud or crimes targeting women, while also accessing guidance on cyber safety and prevention. At the same time, it assists law enforcement agencies in taking quicker action on the cases reported.

That same year, the Ministry introduced the Cyber Crime Prevention against Women and Children (CCPWC) scheme, designed to support states and union territories with funds to set up specialized cyber cells. These units focus exclusively on crimes against women and children in the digital space. The scheme also includes the establishment of cyber forensic laboratories in every state and UT to strengthen the investigation process.

In addition to these focused schemes, the Indian government has adopted a number of broader policy measures to address online threats faced by women. The National Policy for the Empowerment of Women (2001) recognized early on the importance of safeguarding women's rights in the digital domain and stressed the need for gender-sensitive legislation to address online harassment and cyber violence. Building on this, the Digital India initiative of 2015 has played a significant role in expanding digital literacy and raising awareness about cyber safety, with a special focus on women and girls. By improving access to digital infrastructure and services, the program also aims to reduce the gendered digital divide and ensure that women benefit more fully from technological advancements.

On the legislative front, amendments to the Information Technology Act, 2000 introduced targeted provisions against offenses such as cyberstalking, voyeurism, and the non-consensual sharing of intimate content. These reforms also created mechanisms like the Cyber Appellate Tribunal, giving citizens a forum to appeal decisions under the Act.

Despite these notable developments, the overall response to cybercrimes against women remains hampered by persistent obstacles. Reporting through the National Cyber Crime Portal continues to be limited, often due to lack of awareness or fear of social repercussions. Similarly, initiatives like the CCPWC scheme face hurdles such as insufficiently trained personnel and inadequate infrastructure in several regions, which restrict their effectiveness in combating technology-enabled crimes against women.

CONCLUSION AND SUGGESTIONS

In the past decade, India has witnessed a sharp surge in cybercrimes directed at women, exposing them to varied forms of online harassment and abuse. The impact of such offenses often extends beyond the digital space, resulting in psychological trauma, reputational harm, and in some cases, even financial loss. Although the country has developed a fairly comprehensive legal framework to address cyber offenses, gaps in enforcement and implementation continue to undermine its effectiveness.

To counter this challenge, the government has launched several initiatives and reporting mechanisms aimed at safeguarding women in cyberspace. Yet, these measures alone cannot succeed unless the deeper causes of such crimes are addressed factors like entrenched patriarchy, systemic gender violence, and the lack of widespread awareness about cyber safety remain key enablers of abuse.

Emerging technologies such as artificial intelligence, blockchain, and machine learning hold significant potential in strengthening the fight against online crimes. These tools can help trace offenders, prevent digital violations, and facilitate faster responses by law enforcement agencies.

It is also essential to recognize that gender-based violence in the digital sphere is not a new phenomenon but an extension of traditional patterns of domination and control. Acts such as cyberstalking, image-based sexual abuse, doxing, or sextortion are not merely technical infractions; they reflect the continuation of long-standing gendered hierarchies in a new medium. These practices erode women's dignity, autonomy, and psychological well-being, thereby reproducing inequality in online spaces.

While Indian courts and international legal systems have taken steps to respond to such harms, the legal framework remains incomplete. Rights to privacy, dignity, and health interpreted as part of Article 21 of the Constitution offer some protection, but since they rest heavily on judicial interpretation, they remain vulnerable to re-interpretation or dilution by higher benches.

For example, Section 294 of the Bharatiya Nyaya Sanhita criminalizes the sale, distribution, or public display of obscene content, including material circulated online. However, the statute does not provide a precise definition of "obscenity." Courts have attempted to evolve tests for obscenity over time, but the absence of a fixed standard leaves considerable scope for subjective judgments.

Simultaneously, the rapid expansion of AI has increased the risks of digital exploitation, making it imperative to create a dedicated legal framework for its regulation and for assigning liability in cases of misuse. Alongside these reforms, there is a pressing need to promote digital literacy and cyber hygiene among women. Large-scale awareness campaigns especially in rural and marginalized communities could enable women to better understand their digital rights, protect their privacy, and seek timely remedies.

Despite ongoing policy and legal reforms, persistent challenges remain in reporting, investigating, and prosecuting cyber offenses. The overlap of entrenched patriarchal attitudes with technological misuse shows that stronger laws alone will not suffice; what is needed is a parallel cultural shift toward gender equality in both offline and online spaces.