Research Ambition
An International Multidisciplinary e-Journal
(Peer-reviewed & Open Access) **Journal home page:** www.researchambition.com
ISSN: 2456-0146, Vol. 10, Issue-III, Nov. 2025

LEGAL AWARENESS AND UNDERREPORTING OF CYBER VIOLENCE AGAINST WOMEN: A SOCIO-LEGAL ANALYSIS IN THE INDIAN CONTEXT

Ayush Gautam,[a*] **Dr. Sanjay Kulshreshtha,**[b**]

[a]*Research Scholar, Institute of Law, Jiwaji University, Gwalior (M.P), India.*
[b]*Professor & Head, Institute of Law, Jiwaji University, Gwalior (M.P), India.*

KEYWORDS

Cyber Violence Against Women, Underreporting of Cyber Crimes, Socio-Legal Analysis, Gender and Cyberspace, Legal Awareness, Indian Cyber Law.

ABSTRACT

Cyber violence against women has emerged as a pervasive yet underreported form of gender-based harm in the digital age. Despite the existence of legal frameworks and increasing public discourse around cyber laws in India, a significant number of women refrain from reporting online abuse such as cyberstalking, harassment, non-consensual dissemination of intimate content, and digital intimidation. This paper undertakes a socio-legal analysis of the relationship between legal awareness and the persistent underreporting of cyber violence against women in the Indian context. It critically examines whether legal awareness alone is sufficient to empower victims to seek legal redress or whether deeper socio-cultural and institutional barriers continue to silence survivors. Through a doctrinal analysis of statutory provisions under the Information Technology Act, 2000 and relevant sections of the Indian Penal Code, along with an examination of judicial responses and enforcement mechanisms, the study highlights the limitations of law when confronted with patriarchal norms, social stigma, fear of reputational harm, and lack of trust in institutional responses. The paper argues that legal awareness, while necessary, is not a standalone solution to address underreporting. Instead, a holistic approach that integrates legal reform, gender-sensitive enforcement, institutional accountability, and socio-cultural transformation is essential to ensure meaningful access to justice for women facing cyber violence in India.

1. INTRODUCTION

1.1 Concept of Cyber Violence Against Women

Cyber violence against women refers to gender-based acts of harm committed through or facilitated by digital technologies that violate a woman's dignity, privacy, autonomy, and psychological well-being. It is a contemporary manifestation of violence that operates within cyberspace but is rooted in long-standing social structures of gender inequality. Unlike traditional physical violence, cyber violence is characterised by its capacity for anonymity, permanence, and wide dissemination, allowing perpetrators to exert control and inflict harm without physical proximity. The concept therefore demands a broader understanding of violence one that extends beyond bodily injury to include emotional, reputational, and psychological harm inflicted through digital means.[1]

From a socio-legal perspective, cyber violence is not an isolated technological phenomenon but an

>Corresponding author
***E-mail:** ayush_gautam93@yahoo.com (Ayush Gautam).
https://orcid.org/0009-0002-3576-7116
DOI: https://doi.org/10.53724/ambition/v10n3.08
Received 18th Sep. 2025; Accepted 15th Oct. 2025
Available online 30th Nov. 2025

extension of gender-based violence that mirrors and reinforces offline power relations. Digital platforms often reproduce existing hierarchies of dominance, where women's visibility and participation are met with disproportionate hostility. Acts such as online harassment, intimidation, invasion of privacy, and digital surveillance are frequently employed as tools to silence women, restrict their agency, and punish perceived transgressions of socially prescribed gender norms. The harm caused by such acts is compounded by the continuous nature of digital access, making escape or disengagement from abuse particularly difficult.

The conceptual framework of cyber violence against women has gained recognition in international human rights discourse, which increasingly acknowledges that violence can occur in virtual environments with consequences as severe as offline abuse. Cyber violence undermines women's fundamental rights, including the right to equality, freedom of expression, privacy, and personal liberty. In the Indian context, these rights are constitutionally protected under Articles 14, 19, and 21 of the Constitution of India. When cyber violence interferes with a woman's ability to participate freely in digital spaces, it effectively curtails her access to education, employment, social engagement, and democratic participation, thereby deepening gender-based exclusion.[2]

Legally, the concept of cyber violence against women in India is addressed through a combination of technology-specific legislation and general criminal law. While the Information Technology Act, 2000 provides the primary statutory framework for regulating digital conduct, several provisions of the Indian Penal Code, such as those relating to criminal intimidation, insult to modesty, stalking, and defamation, are invoked to address gendered harms occurring online. However, the absence of a singular, comprehensive statutory definition of cyber violence against women has led to fragmented legal responses. As a result, the conceptual understanding of cyber violence remains largely interpretive, shaped by judicial reasoning, enforcement practices, and socio-cultural perceptions rather than a unified legislative vision.

Importantly, cyber violence must also be understood as a continuum of harm rather than a single event. Digital abuse often escalates over time, beginning with seemingly minor acts and progressing into more severe forms of coercion or intimidation. The impact of such violence is not limited to immediate distress but can result in long-term psychological trauma, self-censorship, withdrawal from public life, and erosion of trust in legal institutions. The fear of reputational damage and social judgment further intensifies the harm, particularly in societies where women's honour and morality are closely scrutinised.

Thus, conceptualising cyber violence against women requires an integrated approach that recognises its technological dimensions, legal implications, and socio-cultural foundations. It is a form of structural violence that operates at the intersection of gender, power, and technology, demanding responses that go beyond punitive legal

measures. A nuanced understanding of the concept is essential for analysing why, despite legal recognition of cyber offences, women continue to remain hesitant to report such violations. This conceptual grounding forms the basis for examining the limitations of legal awareness and the persistent underreporting of cyber violence against women in India.

1.2 Nature and Forms of Cyber Violence

The nature of cyber violence against women is shaped by the distinctive characteristics of digital technologies, which alter both the mode and impact of harmful conduct. Cyber violence is typically non-physical, yet its consequences are deeply invasive, persistent, and far-reaching. Unlike conventional forms of violence, digital abuse transcends geographical boundaries and time constraints, enabling perpetrators to target victims continuously and anonymously. The permanence of online content, combined with its potential for rapid dissemination, amplifies the severity of harm and often renders victims powerless to control the spread or recurrence of abusive material. These features make cyber violence uniquely coercive and psychologically damaging.

Cyber violence against women manifests in multiple forms, each exploiting the structural vulnerabilities of digital platforms. One of the most common forms is online harassment, which includes the repeated sending of abusive, threatening, or sexually explicit messages through social media, email, or messaging applications. Such conduct often aims to intimidate or silence women, particularly those who are vocal or visible in public or professional spaces. Closely related is cyberstalking, characterised by persistent monitoring, unsolicited communication, and digital surveillance, which creates a climate of fear and intrusion into a woman's personal life.[3]

Another significant form of cyber violence is the non-consensual dissemination of intimate images or personal data, commonly referred to as image-based abuse. This includes the sharing of private photographs, videos, or personal information without consent, often with the intent to shame, humiliate, or exert control. The irreversible nature of online dissemination magnifies the harm caused by such acts, frequently leading to severe emotional distress, social withdrawal, and reputational damage. Digital platforms also facilitate impersonation and identity misuse, where fake profiles are created in a woman's name to post offensive content or engage in deceptive communication, thereby damaging her credibility and social standing.

Cyber violence further includes acts of digital intimidation and threats, where women are subjected to threats of physical harm, sexual violence, or exposure of private information. These threats, even when not acted upon, exert significant psychological pressure and can restrict women's freedom of expression and participation in digital spaces. Additionally, online defamation and character assassination are commonly employed to police women's behaviour, particularly by invoking moral judgments or questioning their character, sexuality, or credibility.[4]

The nature of cyber violence is often cumulative

rather than isolated. Victims frequently experience multiple forms of abuse simultaneously or sequentially, creating a cycle of harassment that intensifies over time. What may begin as casual online hostility can escalate into sustained campaigns of abuse, involving coordinated attacks, repeated threats, or the mobilisation of online communities against a single individual. This cumulative dimension distinguishes cyber violence from sporadic online misconduct and underscores its classification as a serious form of gender-based harm.

Importantly, cyber violence disproportionately affects women who challenge traditional gender norms, including students, professionals, activists, journalists, and public figures. The digital environment enables perpetrators to enforce conformity through harassment and intimidation, thereby reinforcing existing social hierarchies. While cyber violence may appear technologically driven, its forms are deeply influenced by gendered expectations and power relations that shape both the choice of tactics and the intensity of abuse.

In essence, the nature and forms of cyber violence against women reflect a convergence of technological capability and social intent. The digital medium serves as a facilitator rather than the root cause of violence, enabling familiar patterns of gender-based abuse to assume new and more pervasive forms. Understanding these manifestations is crucial for analysing the broader socio-cultural and legal challenges associated with addressing cyber violence and forms the foundation for evaluating the adequacy of legal awareness and protective mechanisms in the Indian context.

1.3 Socio-Cultural Dimensions of Cyber Violence

Cyber violence against women cannot be understood solely through a technological or legal lens; it is deeply embedded within broader socio-cultural structures that shape gender relations in society. Digital spaces do not exist in isolation from social realities but function as extensions of offline norms, attitudes, and power hierarchies. Consequently, cyber violence reflects and reinforces entrenched patriarchal values, gender stereotypes, and moral expectations imposed upon women. The persistence of such socio-cultural factors plays a critical role in both the prevalence of cyber violence and the reluctance of women to seek redress.

Patriarchy remains a defining influence on how women's presence in digital spaces is perceived and regulated. Women who express opinions, assert autonomy, or challenge dominant narratives online often face disproportionate backlash, including harassment and abuse aimed at disciplining their behaviour. Cyber violence is frequently employed as a mechanism of social control, designed to silence women and restrict their participation in public discourse. The targeting of women for visibility rather than invisibility reveals the discomfort with female agency in both online and offline environments.[5]

A significant socio-cultural factor contributing to cyber violence is the pervasive culture of victim-blaming. Women subjected to online abuse are often questioned about their conduct, online

presence, clothing, or choice of expression, rather than the actions of the perpetrator being scrutinised. These narrative shifts responsibility from the offender to the victim and normalises abusive behaviour as an inevitable consequence of women's engagement with digital platforms. Such attitudes discourage women from reporting cyber violence, as disclosure is frequently met with judgment, trivialisation, or moral policing.

Social stigma and fear of reputational harm further exacerbate the impact of cyber violence. In many communities, particularly within conservative social settings, a woman's honour and family reputation are closely linked to perceptions of morality and modesty. The public and permanent nature of digital content intensifies these fears, as online abuse can be accessed, shared, and resurrected indefinitely. The potential for social ostracisation, familial pressure, and damage to personal relationships often compels women to remain silent, even when the abuse is severe.

Cultural norms surrounding gender roles also influence the way cyber violence is perceived and addressed. Women are often socialised to endure harassment quietly and to avoid confrontation, while assertive responses are discouraged or penalised. This conditioning reinforces silence and normalises abuse as an unfortunate but acceptable aspect of digital participation. The expectation that women must adapt their behaviour to avoid victimisation places an unfair burden on them and obscures the need for systemic accountability.

Additionally, digital inequality intersects with socio-cultural constraints to intensify vulnerability. Limited access to digital literacy, particularly among women from marginalised or rural backgrounds, reduces awareness of online safety practices and support mechanisms. Even where awareness exists, socio-cultural pressures often override the perceived benefits of reporting, creating a gap between knowledge and action. The absence of supportive community environments further isolates victims, reinforcing feelings of helplessness and resignation.[6]

In essence, the socio-cultural dimensions of cyber violence reveal that technology serves as a medium through which existing gendered power structures are reproduced rather than dismantled. Cyber violence is sustained not merely by digital anonymity but by social attitudes that tolerate, excuse, or trivialise abuse against women. Any meaningful response to cyber violence must therefore address these underlying cultural norms alongside legal and institutional reforms. Recognising the socio-cultural context is essential to understanding why legal awareness alone fails to translate into reporting and protection for women in cyberspace.

1.4 Legal Framework Governing Cyber Violence in India

The legal framework governing cyber violence against women in India is primarily derived from a combination of technology-specific legislation and general criminal law. Unlike certain jurisdictions that have enacted specialised statutes addressing digital gender-based violence, India relies on the Information Technology Act, 2000 supplemented by relevant provisions of the Indian Penal Code to

address offences committed in cyberspace. While this framework provides multiple avenues for redress, its fragmented nature often limits its effectiveness in responding to the complex and gendered realities of cyber violence.

The Information Technology Act, 2000 serves as the foundational statute regulating conduct in digital environments. Section 66E of the Act addresses the violation of privacy through the intentional capture, publication, or transmission of images of a person's private areas without consent, thereby offering protection against certain forms of image-based abuse. Section 67 and Section 67A criminalise the publication or transmission of obscene and sexually explicit material in electronic form, provisions that are frequently invoked in cases involving the circulation of non-consensual intimate content. Additionally, Section 72 penalises the breach of confidentiality and privacy by individuals entrusted with access to electronic records. Although these provisions provide important safeguards, they are not gender-specific and often fail to fully capture the power dynamics and psychological harm associated with cyber violence against women.

Alongside the IT Act, the Indian Penal Code, 1860/ Bhartiya Nyaya Sanhita, 2023 plays a significant role in addressing cyber violence by extending traditional criminal offences to digital contexts. Section 354D/78 criminalises stalking, including monitoring or contacting a woman through electronic communication despite clear indications of disinterest. Section 509/79 penalises acts intended to insult the modesty of a woman through words, gestures, or electronic communication. Provisions relating to criminal intimidation under Section 503/ 351(1), defamation under Section 499/ 356(1), and intentional insult under Section 504/ 352 are also commonly applied in cases of online abuse and harassment. The application of these provisions reflects judicial recognition that offences committed through digital means are no less harmful than those occurring offline.

Judicial interpretation has been instrumental in bridging the gap between statutory language and evolving digital realities. Indian courts have acknowledged that cyber offences can cause serious psychological and reputational harm and have emphasised the need for a purposive interpretation of existing laws to address online abuse. Courts have also underscored the importance of protecting women's dignity and privacy in cyberspace, viewing such protection as an extension of constitutional guarantees under Article 21. However, judicial intervention remains largely case-specific and reactive, offering limited structural guidance for addressing the broader issue of underreporting.

Institutional mechanisms such as cyber-crime cells, online reporting portals, and helplines have been established to facilitate the reporting and investigation of cyber offences. The Ministry of Home Affairs' cyber-crime reporting portal represents an important step toward accessibility. Nevertheless, procedural complexities, lack of specialised training, jurisdictional ambiguities, and limited victim-centric approaches continue to undermine the effectiveness of these mechanisms.

Women frequently encounter delays, insensitivity, or uncertainty when navigating the reporting process, which discourages engagement with the legal system.

Despite the presence of multiple legal provisions, the Indian framework remains largely reactive rather than preventive and lacks a cohesive policy addressing cyber violence as a form of gender-based harm. The absence of a comprehensive definition of cyber violence against women and the reliance on dispersed statutory provisions contribute to inconsistent enforcement and legal uncertainty. As a result, while the law formally recognises various cyber offences, its practical capacity to encourage reporting and provide meaningful protection remains constrained.

Thus, the legal framework governing cyber violence in India reflects a paradoxical situation: legal remedies exist, yet their fragmented structure, procedural limitations, and institutional shortcomings hinder effective access to justice for women. This gap between legal availability and practical usability sets the stage for examining why legal awareness alone is insufficient as a protective tool against cyber violence.

1.5 Limitations of Legal Awareness as a Protective Tool

Legal awareness is often viewed as a foundational strategy for empowering individuals to assert their rights and seek redress against violations. In the context of cyber violence against women, awareness of legal provisions governing online abuse is widely promoted as a preventive and remedial measure. However, the persistence of underreporting despite the existence of legal knowledge reveals the inherent limitations of legal awareness when it operates in isolation. Awareness of the law, while necessary, does not automatically translate into the ability or willingness to invoke legal remedies.

One of the primary limitations of legal awareness lies in the disconnect between knowledge and accessibility. Awareness of statutory provisions does not ensure familiarity with procedural mechanisms such as jurisdiction, evidence preservation, or reporting channels. The complexity of cyber laws, combined with overlapping provisions under multiple statutes, often creates confusion rather than clarity for victims. This procedural opacity discourages women from approaching legal institutions, particularly when the anticipated process appears lengthy, technical, or emotionally taxing.[7]

Another significant constraint is the absence of institutional trust. Women may be aware of their legal rights yet remain reluctant to engage with enforcement agencies due to concerns regarding insensitivity, secondary victimisation, or lack of confidentiality. Fear of being questioned, judged, or dismissed by authorities often outweighs the perceived benefits of legal action. In such circumstances, legal awareness exists in theory but fails to function as a practical protective tool.

Socio-cultural pressures further undermine the effectiveness of legal awareness. In societies where stigma, moral scrutiny, and reputational concerns dominate responses to gender-based harm, awareness of the law does not neutralise the fear of

social consequences. Women are frequently compelled to prioritise familial harmony, social acceptance, and personal safety over legal accountability. This dynamic illustrates that legal consciousness operates within cultural boundaries that shape decision-making and limit the exercise of rights.

Additionally, legal awareness campaigns often adopt a formalistic approach, focusing on statutory provisions without addressing the lived realities of victims. Such approaches overlook the emotional, psychological, and social dimensions of cyber violence, reducing awareness to mere information dissemination. Without parallel efforts to create supportive environments, sensitise enforcement agencies, and ensure victim-centric processes, legal awareness remains insufficient as a standalone solution.

The digital nature of cyber violence also complicates the protective role of legal awareness. The rapid pace of online abuse, difficulties in identifying perpetrators, and challenges in preserving digital evidence frequently render legal remedies reactive rather than preventive. Even informed victims may perceive legal intervention as ineffective in providing immediate relief or preventing further harm.

Thus, the limitations of legal awareness highlight a critical paradox within the existing legal response to cyber violence against women. While awareness is an essential component of empowerment, it cannot function effectively without institutional accountability, procedural accessibility, and socio-cultural support. Addressing underreporting therefore requires a shift from awareness-centric strategies to integrated approaches that combine legal education with systemic reform and cultural transformation. This understanding provides the conceptual foundation for examining existing scholarship and identifying gaps in the current discourse, which the subsequent section on literature review seeks to address.

2. Literature Review

Scholarship on cyber violence against women in India and globally underscores the rapid rise of digital abuse and highlights its complex socio-legal implications. A recent study by Ahlawat and Sharma (2024) examines the growth of technology and internet usage in India and notes that women face a disproportionate share of cybercrimes, including harassment, cyberstalking, and non-consensual dissemination of private content, which have far-reaching impacts on mental health and freedom of expression. Their analysis also points to weaknesses in existing regulations and calls for legal reforms tailored to address these emerging threats.

Dar and Nagrath's work on whether women are a "soft target" for cybercrime situates the issue within structural inequalities. They argue that the increased accessibility of ICTs like the internet and mobile devices has made women particularly vulnerable to a range of abuses such as cyberstalking, online sexual harassment, and phishing, noting that these forms of violence carry serious social and psychological consequences. This perspective helps frame cyber violence as not only a technological problem but also a social one,

driven by patterns of gendered behaviour in digital spaces.

A closer lens on specific manifestations of online abuse is found in research that highlights the emotional and psychological severity of digital threats. Semwal's article on "digital death and rape threats" shows how threats delivered via online platforms including coordinated trolling and messages with rape or acid attack metaphors produce real trauma that the current legal system tends to under-recognise or under-respond to. Such work contributes to understanding the severity and personal nature of cyber violence beyond mere inconvenience or offensive speech.

Studies that focus on particular regions, such as Sharma, Dawra, and Sehrawat's socio-legal study of cyber violence in Haryana, demonstrate how digitisation coexists with entrenched patriarchal norms, creating environments where online abuse persists despite constitutional protections. Their work highlights how legal frameworks like the IT Act and the Bharatiya Nyaya Sanhita interact with socio-cultural attitudes in shaping victims' willingness to pursue legal recourse, pointing to the limitations of law in isolation.

Research reports analysing cybercrime broadly, such as the work on online crimes against women and children, categorise common cyber offences including stalking, bullying, morphing, and blackmail while emphasising that awareness remains low and victims often lack knowledge of legal options. These findings echo concerns about gaps in legal literacy and the need for sustained public education on cyber rights and remedies.

Kolekar's "Virtual Violence**:** Understanding Cybercrime against Women" further extends this discourse by framing cyber-crime as a form of virtual gendered violence that exploits anonymity and reach of technology. The article points to a broad range of offences from online defamation to identity theft and suggests that legal recognition under the IT Act and recent amendments is still insufficient to fully capture the lived experiences of victims.

Vaishnav and Dewan's international perspective on cybercrime against women reinforces that while India shares global patterns of online abuse, there are unique national challenges related to legal implementation and social attitudes. Their evolutionary account of cybercrime demonstrates that technology alone does not explain the phenomenon, and stresses that outdated legal frameworks struggle to keep pace with both technological change and the sophistication of abusive conduct.

Khan's study on protection and empowerment highlights how cyberspace can be both an empowering and a threatening domain for women. While women's access to information and participation in public discourse has increased, the same platforms are misused for sexual harassment, unsolicited messaging, and email misrepresentation, which undermines the empowering potential of digital tools. The research underscores the dual nature of digital technologies as both enabling and harmful.

Legal assessments examining the effectiveness of India's statutory framework, such as the evaluation

of cyber-crimes and harassment of women, point to gaps in enforcement, public awareness, and technical capacity. These evaluations emphasise that although provisions under the Information Technology Act and IPC exist for online offences, limitations in enforcement and lack of specialised training for law enforcement result in under-utilisation of legal remedies and contribute to persistent underreporting.

Complementing doctrinal analysis, several critical reviews note that cyber violence disproportionately affects women because of gendered power structures and societal norms that facilitate harassment. The recurring theme across these works is that socio-cultural contexts including stigma and moral policing play a central role in shaping both the prevalence of cyber abuse and the reluctance to seek legal redress.

Some literature also points to the evolving judicial and policy responses, though not always in a positive light. For instance, recommendations for reviewing cyber laws linked to women's digital rights, as advocated by national commissions, demonstrate acknowledgment of systemic gaps but also reflect ongoing uncertainty about how to tailor laws to address gendered harm disproportionately.

Taken together, existing scholarship reveals a multi-layered understanding of cyber violence: as a social phenomenon influenced by technology and gendered norms; as a legal problem with fragmented responses; and as an issue where awareness does not necessarily lead to reporting or justice. However, much of this literature tends to address either socio-cultural impediments, the nature of cyber offences, or the adequacy of law in isolation. There remains limited integrated analysis on how legal awareness interacts with social realities to influence reporting behaviour the precise gap this research paper aims to fill.

3. **Research Gap**

The existing body of literature on cyber violence against women has substantially contributed to identifying the nature, forms, and socio-cultural impact of digital abuse, as well as analysing the adequacy of legal frameworks governing cyber offences. However, a critical gap persists in the integrated examination of legal awareness and underreporting from a socio-legal perspective. While several studies emphasise the importance of legal awareness and digital literacy as tools for empowerment, they often operate on the assumption that awareness naturally leads to reporting and legal action.

Most socio-cultural analyses highlight stigma, patriarchal norms, and victim-blaming as barriers to reporting but tend to underexplore how these factors interact with legal consciousness and institutional mechanisms. Conversely, doctrinal legal studies frequently focus on statutory provisions and judicial interpretations without sufficiently accounting for the lived realities that shape women's engagement with the legal system. As a result, the relationship between legal awareness and reporting behaviour remains inadequately theorised.

This paper seeks to bridge this gap by offering a socio-legal analysis that situates legal awareness within its broader cultural, institutional, and

structural context. By examining the limitations of legal awareness in isolation, the study aims to move beyond awareness-centric narratives and contribute to a more nuanced understanding of underreporting of cyber violence against women in the Indian context.

4. **Objectives of the Study**

The present study aims to examine cyber violence against women through a socio-legal lens, with particular emphasis on the role and limitations of legal awareness in addressing underreporting. The specific objectives of the study are as follows:

i. To conceptualise cyber violence against women as a form of gender-based harm within digital spaces and examine its distinctive characteristics.
ii. To analyse the existing legal framework in India governing cyber violence against women, including relevant statutory provisions and institutional mechanisms.
iii. To critically assess the extent to which legal awareness functions as an effective protective tool for women facing cyber violence.
iv. To examine the socio-cultural and institutional factors that influence women's reporting behaviour despite the availability of legal remedies.
v. To identify structural limitations within the legal and enforcement framework that contribute to the persistent underreporting of cyber violence against women in India.

5. **Hypothesis**

The study proceeds on the hypothesis that legal awareness alone is insufficient to address the problem of cyber violence against women, and that socio-cultural barriers, institutional limitations, and lack of trust in enforcement mechanisms significantly contribute to the underreporting of such offences in India.

6. **Data Analysis**

Although this study is primarily doctrinal in nature, limited illustrative data has been drawn from secondary sources, policy reports, and region-specific observations to contextualise the issue of underreporting of cyber violence against women. The Chambal region, encompassing parts of Madhya Pradesh and adjoining areas, is used illustratively to reflect broader socio-legal patterns prevalent in semi-urban and rural India. The analysis does not seek to establish statistical prevalence but rather to interpret how legal awareness operates in practice within a specific socio-cultural setting.

Available reports and regional observations indicate that awareness of cyber-crimes and relevant legal provisions among women in the Chambal region has gradually increased due to digital penetration, educational initiatives, and media coverage of cyber offences. Women, particularly students and young professionals, are increasingly conscious of the existence of cyber laws and the illegality of online harassment, stalking, and image-based abuse. However, this awareness has not resulted in a corresponding increase in formal reporting to law enforcement agencies.

The gap between awareness and reporting is

evident in the manner cyber violence is informally managed or ignored. Many women prefer to block perpetrators, deactivate accounts, or rely on familial intervention rather than approach legal institutions. This tendency reflects a perception that legal remedies are either inaccessible or ineffective in providing timely and meaningful relief. Even when women are aware of cyber-crime reporting portals or cyber cells, uncertainty regarding procedural steps, jurisdiction, and evidentiary requirements discourages formal complaints.

Socio-cultural pressures play a decisive role in shaping these responses. In the Chambal region, as in many parts of India, concerns related to family honour, social reputation, and moral scrutiny strongly influence women's decision-making. Reporting cyber violence is often perceived as inviting unwanted attention, questioning of character, or prolonged engagement with the criminal justice system. These apprehensions persist regardless of a woman's educational background or basic legal awareness, indicating that knowledge of the law does not neutralise the social costs associated with reporting.

Institutional factors further reinforce underreporting. Anecdotal accounts and secondary studies suggest that women often anticipate dismissive or insensitive responses from authorities, particularly in cases involving online harassment that do not result in immediate physical harm. The lack of visible victim-centric procedures, gender-sensitive handling, and consistent follow-up contributes to a broader trust deficit. Consequently, legal awareness exists in a vacuum, unsupported by institutional confidence or cultural acceptance.

This interpretive analysis demonstrates that underreporting of cyber violence cannot be attributed to ignorance of the law alone. Instead, it emerges from the intersection of partial legal awareness, socio-cultural constraints, and institutional limitations. The Chambal region thus serves as an illustrative context highlighting a national pattern: legal awareness, while present to varying degrees, fails to function as an effective protective tool in the absence of supportive social and enforcement structures.

7. **Findings**

Based on the doctrinal examination of cyber violence against women, the existing legal framework, and the interpretive analysis of reporting behaviour, the study arrives at the following key findings:

First, the study finds that legal awareness, while necessary, is not sufficient as a standalone protective mechanism against cyber violence. Awareness of laws governing online abuse does not automatically empower women to seek legal remedies, particularly when procedural complexities and uncertainty regarding enforcement persist.

Second, socio-cultural barriers exert a stronger influence on reporting behaviour than legal knowledge. Fear of stigma, reputational harm, moral judgment, and familial pressure consistently outweigh the perceived benefits of formal legal action. These factors remain deeply embedded in social structures and continue to silence victims,

irrespective of their educational or legal awareness levels.

Third, the study reveals a significant trust deficit between victims and institutional mechanisms. Women often anticipate insensitivity, delay, or dismissal by law enforcement agencies, which discourages engagement with cyber cells or reporting portals. This lack of confidence undermines the practical utility of existing legal provisions.

Fourth, the absence of a cohesive and gender-specific legal approach to cyber violence contributes to fragmented enforcement. The reliance on dispersed provisions under different statutes creates confusion and inconsistency, limiting the law's capacity to address the unique nature of gendered digital harm.

Fifth, the analysis highlights that underreporting is not merely a result of ignorance but a rational response to structural constraints. Women frequently adopt self-protective strategies such as disengagement from digital platforms or informal resolution, reflecting a perception that the legal system offers limited relief.

Collectively, these findings demonstrate that the persistence of underreporting of cyber violence against women in India is rooted in a complex interplay of legal, social, and institutional factors. Addressing this issue therefore requires a shift from awareness-centric interventions toward more holistic, trust-based, and gender-sensitive approaches.

8. Conclusion

Cyber violence against women represents a complex and evolving form of gender-based harm that extends beyond technological misuse into the deeper terrain of social power, cultural norms, and institutional functioning. This study has demonstrated that while India possesses a legal framework capable of addressing various manifestations of cyber violence, the mere existence of laws and increasing levels of legal awareness have not been sufficient to ensure reporting or access to justice for women.

The analysis reveals that legal awareness operates within a constrained socio-cultural and institutional environment. Patriarchal attitudes, victim-blaming narratives, fear of reputational damage, and familial pressures significantly shape women's responses to cyber violence, often discouraging formal complaints. These social realities diminish the practical effectiveness of legal knowledge, rendering awareness a limited protective tool when unsupported by trust, sensitivity, and accessibility within the justice delivery system.

The study underscores the need to reorient policy and legal responses away from awareness-centric strategies toward more integrated approaches that prioritise institutional accountability, gender-sensitive enforcement, and socio-cultural transformation. Strengthening reporting mechanisms, ensuring confidentiality, building trust through sensitisation of law enforcement agencies, and fostering supportive community environments are essential to translating legal awareness into meaningful access to justice.

In conclusion, addressing the underreporting of cyber violence against women in India requires

recognising that law alone cannot dismantle deeply embedded social hierarchies. Legal awareness must be accompanied by structural reform and cultural change to create an environment in which women can assert their rights without fear or hesitation. Only through such a holistic socio-legal approach can cyberspace evolve into a safer and more inclusive space for women.

9. References:

[1]Aparna Chandra, *Gender Justice and the Digital Space*, Oxford University Press, New Delhi (2021).

[2]UN Women, *Online and ICT-Facilitated Violence Against Women and Girls* (United Nations 2020).

[3]Madhu Mehra, 'Online Violence Against Women in India' (2017) 26(4) *Journal of Gender Studies* 420.

[4]Nandita Bhatla et al., 'Digital Abuse and Women's Safety in India' (2018) 12(1) *International Journal of Cyber Criminology* 1.

[5]Flavia Agnes, 'Law, Gender and Cyber Space' (2018) 53(17) *Economic and Political Weekly* 45.

[6]Pratiksha Baxi, 'Justice, Dignity and Gender Violence in India' (2016) *Journal of Indian Law and Society* 67.

[7]Bina Agarwal, 'Gender and Legal Consciousness in India' (2019) 10(2) *Indian Journal of Law and Society* 123.

Other work cited:

1. Aparna Chandra, *Gender Justice and the Digital Space*, Oxford University Press, New Delhi (2021).
2. Bina Agarwal, "Gender and Legal Consciousness in India," *Indian Journal of Law and Society*, Vol. 10, No. 2 (2019).
3. Danielle Keats Citron, *Hate Crimes in Cyberspace*, Harvard University Press, Cambridge (2014).
4. Flavia Agnes, "Law, Gender and Cyber Space," *Economic and Political Weekly*, Vol. 53, No. 17 (2018).
5. Government of India, *Information Technology Act, 2000* (as amended).
6. Government of India, *Indian Penal Code, 1860* (as amended).
7. Justice J.S. Verma Committee, *Report on Amendments to Criminal Law*, Ministry of Home Affairs, New Delhi (2013).
8. Law Commission of India, *Consultation Paper on Cyber Crimes*, Government of India (2017).
9. MadhuMehra, "Online Violence Against Women in India," *Journal of Gender Studies*, Vol. 26, No. 4 (2017).
10. Ministry of Home Affairs, Government of India, *National Cyber Crime Reporting Portal: Guidelines and Framework* (2020).
11. NanditaBhatla et al., "Digital Abuse and Women's Safety in India," *International Journal of Cyber Criminology*, Vol. 12, No. 1 (2018).
12. Pratiksha Baxi, "Justice, Dignity and Gender Violence in India," *Journal of Indian Law and Society*, Vol. 7 (2016).
13. UN Women, *Online and ICT-Facilitated Violence Against Women and Girls*, United Nations, New York (2020).
14. United Nations General Assembly, *Declaration on the Elimination of Violence Against Women*, 1993.
15. Vrinda Grover, "Privacy, Dignity and Cyber Crimes Against Women," *National Law School of India Review*, Vol. 31 (2019).
16. Yogesh Pratap Singh, *Cyber Laws in India*, LexisNexis, New Delhi (2020).
17. Zubeda Hamid, "Patriarchy, Technology and Gender Violence," *Sociological Bulletin*, Vol. 68, No. 3 (2019).

****