Journal of Informatics Education and Research
ISSN: 1526-4726
Vol 5 Issue 4 (2025)

Cyber Violence Against Women in Haryana: A Socio-Legal Dimension

Ms. Richa Sharma[1*]
[1]Research Scholar, School of Law, Sushant University Sector-55, Golf Course Road, Gurugram, Haryana- 122011, India
*Corresponding Email Id: richasharma.phd20@sushantuniversity.edu.in

Dr. Anil Dawra[2]
[2]Professor, School of Law, Sushant University Sector-55, Golf Course Road, Gurugram, Haryana- 122011, India
Email Id: anildawra@sushantuniversity.edu.in

Dr. Anjali Sehrawat[3]
[3]Associate Professor, School of Law, Sushant University Sector-55, Golf Course Road, Gurugram, Haryana- 122011, India
Email Id: anjalidabas@sushantuniversity.edu.in

ABSTRACT

The rise of digital communication has dramatically reshaped social and economic interactions globally, facilitating connectivity and knowledge exchange across unprecedented scales. However, this digital revolution has simultaneously given rise to new forms of gendered violence, which disproportionately target women. Cyber Violence Against Women (CVAW) encompasses a spectrum of abuses, including online harassment, cyberstalking, non-consensual dissemination of intimate images, identity theft, and other forms of technology-enabled abuse. This study focuses on CVAW in India, examining both doctrinal and socio-legal frameworks, with particular attention to Haryana—a state marked by rapid urbanization and digitization yet steeped in entrenched patriarchal norms. The paper critically evaluates the interaction between constitutional guarantees, statutory provisions, and judicial interpretations, including the newly enacted Bharatiya Nyaya Sanhita (BNS) alongside Information Technology laws. Further, it situates India's approach within the global legal landscape, comparing institutional responses in Kerala and Telangana, and identifies systemic gaps in enforcement. Empirical evidence, including case studies and National Crime Records Bureau (NCRB) cyber-crime data, demonstrates that legal reforms alone are insufficient; effective mitigation of CVAW requires complementary socio-cultural and institutional interventions. The paper proposes a comprehensive approach, integrating legislative clarity, institutional capacity building, digital literacy initiatives, and broader societal transformation.

Keywords: *Cyber Violence Against Women (CVAW), Haryana, Legal and Institutional Framework, Digital Gendered Harms*

INTRODUCTION

Digital technologies have revolutionized the way individuals communicate, access information, and participate in public life. While the proliferation of smartphones, social media platforms, and online communities has facilitated social and economic empowerment, it has also exposed women to a range of risks unique to cyberspace. Women face harassment that can range from persistent messaging and stalking to severe reputational damage through manipulated images and non-consensual disclosures. Concepts such as "revenge porn," "deepfake abuse," and "cyberstalking" reflect the novel forms of harm emerging in digital environments. Unlike traditional physical violence, CVAW transcends spatial boundaries, enabling perpetrators to inflict psychological, social, and even economic harm from remote locations.

India, home to over 850 million internet users, presents a complex picture. Digital penetration offers transformative opportunities for women's education, employment, and social participation, yet it also magnifies vulnerabilities. NCRB statistics indicate a steady increase in cybercrimes against women, particularly on social media platforms, where anonymity and ease of access embolden perpetrators. According to NCRB-linked data**,** cybercrime cases reported via the National Cyber Crime Reporting Portal rose from 22,188 in 2020 to 48,475 in 2024, while online and social media-related crime

grew from 56,283 to 1,56,938 in the same period[1]. Haryana, despite significant strides in urban development and technology adoption, illustrates the paradox of progress: deeply rooted patriarchal norms, gender imbalances, and low female labor force participation amplify women's exposure to cybercrime.

This study seeks to answer a critical question: How adequate is India's legal and institutional framework in addressing cyber violence against women, particularly in Haryana, and what reforms are necessary to strengthen protection and redress? By combining doctrinal legal analysis, socio-legal insights, and comparative state-level perspectives, the research provides a holistic understanding of the dynamics of CVAW and its regulatory challenges.

LITERATURE REVIEW

Academic engagement with CVAW has evolved in tandem with the expansion of digital spaces. Early Indian scholarship primarily addressed issues of data protection, e-commerce fraud, and hacking, often neglecting the gendered dimensions of cybercrime. In the past decade, however, scholars, NGOs, and policy institutions have increasingly recognized online gender violence as a significant human rights concern.

Danielle Citron, in her seminal work Cyber Civil Rights, emphasizes the societal harm caused when women are silenced or threatened online, highlighting the democratic consequences of digital harassment[2]. Martha Nussbaum situates cyber abuse within broader frameworks of dignity, equality, and autonomy, arguing that online harassment undermines women's substantive freedoms in ways comparable to physical violence[3].Indian scholars such as Banerjee and Rao contextualize cyber harassment as an extension of offline patriarchal structures, necessitating interventions that are simultaneously legal, social, and technological[4].

Empirical studies further illuminate the lived realities of Indian women in cyberspace. Reports by the Internet Democracy Project (IDP) and Centre for Internet and Society (CIS) document persistent harassment, limited awareness of redressal mechanisms, and the chilling effect of online abuse on women's public participation[5]. NCRB data indicate that a significant proportion of offenders are known to victims, challenging conventional assumptions that online harm primarily originates from strangers.

While India has introduced statutory protections under the Information Technology Act, 2000[6] and Bhartiya Nyaya Sanhita[7], implementation gaps remain substantial. Scholars argue that ambiguity in legislative language, inadequate cyber police infrastructure, and gender-insensitive law enforcement hinder effective mitigation. Comparative studies suggest that states such as Kerala, through digital literacy programs and community interventions, and Telangana, via dedicated cyber police units, offer models for systemic improvement. Yet, literature specific to Haryana remains sparse, highlighting a critical research gap addressed by this study.

A review of existing scholarship reveals that most studies adopt a national or pan-Indian perspective, without delving into state-specific dynamics. For instance, Neha and Seema's study in Envision: Apeejay's Commerce & Management Journal provides an analytical overview of cybercrime against women in India, focusing on typologies such as cyberstalking, morphing, and financial frauds[8]. While insightful, the study does not disaggregate data at the state level, nor does it examine localized cultural or enforcement challenges, which are critical in patriarchal contexts like Haryana.

---

[1] Cybercrime Cases Reported via National Cyber Crime Reporting Portal Rise from 22,188 in 2020 to 48,475 in 2024, Medianama (3 Mar. 2025), available at https://www.medianama.com/2025/03/223-funding-for-women-focused-cybercrime-scheme-drops-89/, last seen on 27 Aug. 2025.

[2] Danielle Keats Citron, Cyber Civil Rights (Harvard University Press 2014).

[3] Martha C. Nussbaum, Women and Human Development: The Capabilities Approach (Cambridge University Press 2000).

[4] Banerjee S and Rao N, 'Cyber Violence Against Women in India: Legal and Policy Perspectives' (2019) 61 Journal of Indian Law and Society 112.

[5] Internet Democracy Project, Online Gender-Based Violence in India: Case Studies and Policy Analysis (2021).

[6] The Information Technology Act, 2000, No. 21 of 2000, Acts of Parliament, 2000 (India).

[7] The Bhartiya Nyaya Sanhita, 2023, No. 45 of 2023, Acts of Parliament, 2023 (India).

[8] Neha & Seema, Cybercrime against Women in India: An Analytical Study, Envision: Apeejay's Commerce & Management Journal, Vol. 14 (2020), available at https://acfa.apeejay.edu/docs/volumes/envision-2020/envision-paper-01-vol-14-2020.pdf, last seen on 27 Aug. 2025.

Similarly, Raghav's paper in the International Journal of Humanities and Social Science Invention examines the social impact of cybercrime, emphasizing its psychological and societal ramifications[9]. Although it highlights broad legal frameworks and societal consequences, it remains generic, lacking empirical engagement with regional variations, particularly in states with contrasting gender dynamics.

Further, Garg and Chauhan's IEEE paper presents a comprehensive analysis of cybercrime trends and cybersecurity strategies in India, integrating statistical data and policy recommendations[10]. However, its orientation is technological and infrastructure-driven, with minimal consideration of gendered vulnerabilities or state-specific implementation issues.

Collectively, these studies underscore the prevalence and severity of cybercrime but fail to address Haryana's unique socio-cultural fabric—marked by deep-rooted patriarchy, low female workforce participation, and urban-rural digital divides—which significantly shape the nature and reporting of cyber offences. This omission creates a clear research gap, as Haryana's rapidly increasing internet penetration juxtaposed with gender imbalances amplifies the risks of cyber victimization among women. This study seeks to fill that gap by providing a targeted analysis of Haryana's cybercrime landscape, evaluating enforcement mechanisms, and proposing gender-sensitive strategies for mitigation.

THEORETICAL & METHODOLOGICAL FRAMEWORK

This study adopts a doctrinal-analytical methodology, complemented by socio-legal insights. Doctrinally, the paper examines constitutional provisions under Articles 14, 15, 19, and 21, statutory provisions under the IT Act (2000, amended), the Indian Penal Code (now BNS), and relevant judicial interpretations, including landmark cases such as Puttaswamy v. Union of India.

Socio-legal analysis incorporates NCRB data, Haryana-specific case studies, and institutional assessments, situating legal provisions within the lived realities of women facing cyber harassment. The research also draws upon feminist legal theory, emphasizing how legal frameworks can reflect, reinforce, or challenge patriarchal norms.

International human rights frameworks provide normative guidance, including the Convention on the Elimination of All Forms of Discrimination Against Women (CEDAW) and UN General Recommendation No. 35 on gender-based violence. These instruments underscore the obligation of states to prevent, investigate, and remedy gender-based harm, including online abuse.

Methodologically, the research is qualitative, relying on secondary sources such as statutory texts, academic commentary, judicial judgments, policy reports, and comparative state practices. Case studies from Haryana provide depth and context, while comparisons with Kerala and Telangana illustrate the impact of institutional and policy interventions on mitigating CVAW.

Typologies of Cyber Violence Against Women

CVAW manifests in multiple, often overlapping forms. The most common categories in India include:

Cyberstalking is one of the most prevalent forms of cyber violence against women (CVAW) in India. It involves continuous online harassment through persistent monitoring of social media profiles, sending unwanted messages, or issuing threats. Such behavior often escalates into offline violence, making it a serious concern for women's safety in the digital space.

Another critical category is Non-Consensual Image Sharing (NCII), commonly referred to as "revenge porn." This form of abuse occurs when intimate images or videos of women are disseminated without their consent. The psychological and social impact of NCII is devastating, often leading to public shaming, mental health issues, and in extreme cases, suicidal tendencies.

Morphing and Deepfakes represent a technologically advanced form of CVAW. In this typology, perpetrators manipulate photographs or videos of women to create sexually explicit or derogatory content. With the rise of AI-driven tools, deepfake pornography has emerged as a major threat, making detection and legal redress increasingly challenging.

---

[9] A. Raghav, Cybercrime and Its Impact on Society, International Journal of Humanities and Social Science Invention, Vol. 4, Issue 11 (2015), available at https://www.ijhssi.org/papers/v4(11)/D04011016024.pdf, last seen on 27 Aug. 2025.

[10] A. Garg & M. Chauhan, A Comprehensive Study on Cybercrime and Cybersecurity in India, IEEE (2020), available at https://ieeexplore.ieee.org/document/9197788/authors#authors, last seen on 27 Aug. 2025.

Cyberbullying and Trolling are rampant on social media platforms. Women frequently face gendered abuse, including derogatory language, threats of physical harm, and character assassination. Often, such attacks are intersectional, combining misogyny with communal, caste-based, or political slurs, which intensifies the harm.
Identity Theft and Impersonation involve creating fake social media accounts or using stolen personal information to impersonate victims. Such acts are typically aimed at damaging a woman's reputation, soliciting money, or engaging in fraudulent activities in her name, which can have severe legal and social consequences for the victim.
Lastly, Financial Exploitation is another significant concern. Fraudsters often target women by luring them into scams, phishing attempts, or extortion schemes through digital means. This not only results in monetary loss but also exposes women to further blackmail and harassment.

Doctrinal & Legal Analysis

International Norms

Cyber violence against women is increasingly recognized as a violation of fundamental human rights. At the international level, Convention on Elimination of All forms of Discrimination against Women (CEDAW) (1979) obliges states to eliminate discrimination against women in both public and private spheres, explicitly extending to new forms of violence facilitated by technology. United Nations resolutions in 2018 and 2021 on online gender-based violence reaffirm the responsibility of states to regulate cyberspace while protecting women's rights to privacy, safety, and dignity[11]. The Istanbul Convention (2011) is particularly instructive, as it mandates criminalization of cyber harassment and obliges signatory states to adopt protective and preventive measures.
Despite India being a signatory to CEDAW, its domestic framework for CVAW remains piecemeal. There is a lack of comprehensive legislation explicitly recognizing online abuse as a distinct category of gendered violence, resulting in fragmented enforcement and limited remedies. Comparative global experiences indicate that countries with integrated approaches—combining legal provisions, digital literacy campaigns, and institutional capacity—achieve higher effectiveness in mitigating cyber violence.

Indian Constitutional and Statutory Framework

The Indian Constitution provides multiple avenues to address CVAW. Article 14 guarantees equality before the law, while Article 15 prohibits gender discrimination. Article 19 protects freedom of expression, which must be balanced against the need to restrict harmful online content. Article 21, interpreted expansively in Puttaswamy v. Union of India, encompasses the right to privacy, personal autonomy, and dignity—all directly relevant to CVAW. These provisions collectively establish a constitutional mandate to protect women from online harassment[12].
Statutorily, the Information Technology Act, 2000 (as amended) criminalizes several forms of cyber abuse. Section 66E addresses violations of privacy, Section 67 covers the publication of obscene material, and Section 67A focuses on sexually explicit content. Provisions under the Indian Penal Code (IPC), now consolidated under the Bharatiya Nyaya Sanhita (BNS), such as Sections 354C (voyeurism), 354D (stalking), and 509 (insulting modesty), extend traditional concepts of sexual harassment into cyberspace. However, ambiguity persists regarding emerging digital forms like deepfakes and cyber-extortion.

Bharatiya Nyaya Sanhita (BNS) & IT Laws

The Bharatiya Nyaya Sanhita (BNS), 2023, under Section 74, criminalizes stalking, including online stalking, while Section 77 addresses voyeurism, and Section 79 covers harassment and intimidation, explicitly extending their application to digital spaces. While this codification marks significant progress, critics argue that the statute provides limited clarity on nuanced digital-specific offences such as deepfakes or non-consensual image sharing, leaving gaps in prosecutorial practice.

[11] Convention on the Elimination of All Forms of Discrimination Against Women (CEDAW) 1979.
[12] Justice K.S. Puttaswamy v. Union of India (2017) 10 SCC 1.

Similarly, the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021, framed under Section 79 of the IT Act, 2000, mandate social media intermediaries to remove or disable access to flagged content within 36 hours of receiving a complaint. However, concerns remain regarding potential over-regulation, the risk of censorship, and the delicate balance with free speech and privacy rights.

Institutional Enforcement Gaps

Despite a robust legal framework, enforcement in India remains weak. NCRB data reveal low conviction rates in cybercrime cases, reflecting gaps in police capacity, victim hesitation, and delays in judicial processes. Haryana illustrates these challenges acutely: districts often lack dedicated cyber units, forensic infrastructure is underdeveloped, and police personnel frequently lack gender-sensitive training. Victims report reluctance to file FIRs due to fear of social stigma, bureaucratic hurdles, and lack of confidence in effective redress. NGOs and civil society organizations often serve as crucial intermediaries, highlighting the need for systemic reform beyond statutory measures.

Cyber-Crime Data

According to the NCRB's Crime in India report, cybercrime cases in India rose notably: from 2,334 cases in 2020 to 2,597 in 2021, and further to 2,940 in 2022, reflecting a near 13% increase from 2021 to 2022[13]. Although NCRB does not directly provide a national percentage increase—or a women-specific victim percentage—in the cybercrime section, a related analysis indicates that cybercrime cases nearly doubled in the national capital (Delhi) in 2022, signaling a disturbing acceleration in digital offences[14].

At the national level, overall crimes against women also increased from 428,278 in 2021 to 445,256 in 2022, marking a 4% rise[15]. These numbers include diverse offence categories—not limited to cybercrimes—ranging from kidnapping and abduction to assault.

In Haryana, NCRB data reveals that cases of crimes against women rose from 13,000 in 2020 to 16,658 in 2021, a substantial 28% increase[16]. Although cybercrime-specific counts for women victims in Haryana aren't broken out in the 2022 report, the overall uptrend underscores heightened digital and physical vulnerabilities.

Common offences faced by women, as reported across NCRB data, include:

1. Cyberstalking: Persistent harassment via digital channels.
2. Non-consensual image sharing and sextortion: Violating women's privacy and dignity.
3. Financial exploitation: Scams, phishing, or digital extortion targeting women.

However, these figures likely underestimate the true prevalence of cybercrimes against women. Underreporting remains a critical challenge, driven by social stigma, fear of victim-blaming, and inadequate institutional support—even when infrastructure exists.

Table 1. Case Studies: Haryana

S. No.	Case	Year	Description	Key Issues Highlighted
1	Revenge Porn in Gurugram	2019	A 24-year-old woman became the victim of revenge porn when an ex-partner uploaded intimate images on social media.	Delayed FIR registration, systemic insensitivity, lack of specialized cybercrime training, psychological harm.

[13] Cybercrime/Information Technology Act cases registered in India: 2,334 in 2020; 2,597 in 2021; 2,940 in 2022, NCRB, Crime in India 2022, Annexure-II (Government of India, Ministry of Home Affairs, 2025).

[14] Cybercrime cases nearly doubled in the national capital in 2022, Finology Blog summarizing NCRB data (2022).

[15] Overall crimes against women in India rose from 428,278 in 2021 to 445,256 in 2022 (4 % increase), NCRB, Crime in India 2022 (Government of India, Ministry of Home Affairs, 2025).

[16] In Haryana, crimes against women rose from 13,000 in 2020 to 16,658 in 2021 (27–28 % increase), Indian Express, "Punjab, Haryana sees rise in crime against women in 2021-22: NCRB," 30 August 2022.

2	Cyberstalking in Rohtak	2021	A female college student faced persistent harassment from a known acquaintance through messages, calls, and fake social media profiles.	Police inaction, need for NGO intervention, institutional gaps.
3	Sextortion Racket in Faridabad	2022	Women were targeted by an organized group manipulating intimate images to demand money.	Lack of trained cyber forensic units, infrastructural deficits, delayed investigation.

Socio-Cultural & Institutional Barriers

Haryana's deeply patriarchal social fabric significantly exacerbates cyber violence against women. Structural inequalities, cultural norms, and traditional gender hierarchies interplay with digital vulnerabilities to limit women's freedom and safety online.

Victim-Blaming and Stigma: Women are often blamed for online harassment, particularly in cases of non-consensual image sharing or interactions with strangers on social media. Fear of social ostracism discourages reporting, contributing to severe underreporting. Families may pressure victims to settle cases privately rather than engage legal mechanisms, reinforcing a culture of silence.

Gender Imbalances: Haryana has one of the lowest female-to-male sex ratios in India, which reflects broader socio-cultural biases. This imbalance often translates into a skewed perception of women's rights, limiting their agency both offline and online.

Low Digital Literacy among Women: While urban areas show higher internet penetration, rural women frequently lack awareness about digital safety, privacy controls, and reporting mechanisms. Predators exploit these knowledge gaps to perpetrate harassment.

Institutional Barriers: Law enforcement agencies often mirror societal biases. Police personnel may dismiss complaints as trivial or assume women are at fault. Additionally, many districts lack cybercrime cells or trained personnel in digital forensics, resulting in delayed investigations and low conviction rates. Victim support services, including counseling and legal aid, remain limited.

These socio-cultural and institutional barriers compound the risk of cyber violence, demonstrating that legal provisions alone cannot ensure safety without societal and administrative reforms.

Comparative Insights: Kerala & Telangana

Comparative analysis of other Indian states provides insight into potential solutions:

Kerala: Known for its high literacy rates and gender-sensitive governance, Kerala has pioneered digital literacy programs targeting women. Initiatives like the Kudumbashree women's collectives integrate online safety education into broader empowerment frameworks. The state has also introduced school curricula incorporating cyber awareness, fostering early digital literacy. These measures have led to higher reporting rates and lower incidences of online harassment relative to other states.

Telangana: Telangana emphasizes institutional capacity, with dedicated cyber police stations, 24/7 women helplines, and trained forensic units. Police officers receive gender-sensitivity training, and swift action is mandated under state guidelines. The use of technology, such as online complaint portals and rapid content takedown protocols, ensures timely response.

These examples suggest that Haryana could benefit from a combination of educational initiatives (to raise awareness), institutional strengthening (to improve enforcement), and community engagement (to challenge patriarchal attitudes).

Proposed Reforms

Legal Reforms: Addressing cyber violence against women requires clear and robust legal frameworks. The Bharatiya Nyaya Sanhita (BNS) should explicitly recognize CVAW, including emerging digital harms such as deepfakes, sextortion, and online impersonation. Victim-centric amendments to data protection laws are essential to ensure privacy, rapid redress,

and protection from further harm. Additionally, simplified reporting mechanisms and streamlined legal processes can reduce barriers for victims, making it easier to seek justice and support.

Institutional Reforms: Strengthening institutional capacity is equally critical. Dedicated cybercrime cells should be established in all districts, staffed with trained personnel capable of handling digital forensic investigations. Continuous gender-sensitivity training for police officers will enhance victim support and ensure empathetic handling of cases. Furthermore, integrating NGOs and civil society organizations into investigative and support roles can bridge gaps in institutional response and provide much-needed assistance to survivors.

Societal Reforms: Societal attitudes must also evolve to mitigate CVAW. Public awareness campaigns can challenge patriarchal mindsets while educating communities about online safety and consent. Community programs aimed at promoting digital literacy among women, especially in rural areas, will empower them to navigate cyberspace safely. Media campaigns highlighting the consequences of cyber harassment can further act as a deterrent, fostering a culture of respect and accountability online.

Policy-Driven Measures: Finally, policy interventions should complement legal and institutional strategies. Collaboration with social media platforms is crucial to monitor content and ensure rapid takedown of abusive material. Establishing victim compensation schemes can provide redress for psychological, legal, and financial damages suffered by survivors. Additionally, incorporating CVAW awareness modules into school curricula will educate young citizens about responsible online behavior, cultivating a safer digital environment for future generations.

CONCLUSION & POLICY IMPLICATIONS

Cyber violence against women in Haryana—and India more broadly—is both a technological and socio-legal challenge, deeply rooted in gender inequalities. Legal frameworks like the BNS and IT Act provide necessary tools for protection, yet their effectiveness is limited by institutional weaknesses, socio-cultural biases, and technological gaps.

Haryana's experience demonstrates the compounded effects of entrenched patriarchy and inadequate institutional preparedness. Low digital literacy, victim-blaming, and weak enforcement mechanisms create a hostile environment for women in cyberspace. Case studies, including revenge porn, cyberstalking, and sextortion, illustrate these challenges, while NCRB data confirm rising trends of online abuse.

Comparative insights from Kerala and Telangana highlight actionable strategies: digital literacy campaigns, gender-sensitive policing, dedicated cyber units, and proactive policy interventions.

Policy Implications:

1. Lawmakers must clarify and expand definitions of cyber offences to include emerging technologies and forms of harassment.
2. State governments must invest in institutional capacity-building, particularly in cyber forensics and victim support.
3. Societal attitudes must be addressed through awareness campaigns, education, and community engagement.
4. Collaboration with technology platforms and NGOs is essential for rapid intervention, monitoring, and prevention.

Ultimately, an integrated approach—combining legal, institutional, technological, and societal measures—is imperative for ensuring women's safety and dignity in the digital age. Legislative reform alone is insufficient; cultural transformation and robust enforcement mechanisms are equally critical to mitigating cyber violence and empowering women to participate safely in the digital sphere.

REFERENCES

Books

1. Jane Bailey and Valerie Steeves, *eGirls, eCitizens: Putting Technology, Theory and Policy into Dialogue with Girls' and Young Women's Voices* (University of Ottawa Press 2015).
2. Danielle Keats Citron, *Cyber Civil Rights* (Harvard University Press 2014).
3. Martha C Nussbaum, *Women and Human Development: The Capabilities Approach* (Cambridge University Press 2000).

Journal Articles

1. S Banerjee and N Rao, 'Cyber Violence Against Women in India: Legal and Policy Perspectives' (2019) 61 *Journal of Indian Law and Society* 112.
2. Neha and Seema, 'Cybercrime against Women in India: An Analytical Study' (2020) 14 *Envision: Apeejay's Commerce & Management Journal* https://acfa.apeejay.edu/docs/volumes/envision-2020/envision-paper-01-vol-14-2020.pdf accessed 27 August 2025.
3. A Raghav, 'Cybercrime and Its Impact on Society' (2015) 4(11) *International Journal of Humanities and Social Science Invention* https://www.ijhssi.org/papers/v4(11)/D04011016024.pdf accessed 27 August 2025.
4. A Garg and M Chauhan, 'A Comprehensive Study on Cybercrime and Cybersecurity in India' (2020) IEEE https://ieeexplore.ieee.org/document/9197788/authors#authors accessed 27 August 2025.

Reports and Policy Documents

1. Internet Democracy Project, *Online Gender-Based Violence in India: Case Studies and Policy Analysis* (2021).
2. NCRB, *Crime in India 2022*, Annexure-II (Government of India, Ministry of Home Affairs 2025).

Statutes

1. The Information Technology Act 2000, No 21 of 2000, Acts of Parliament, 2000 (India).
2. The Bhartiya Nyaya Sanhita 2023, No 45 of 2023, Acts of Parliament, 2023 (India).

Case Law

Justice KS Puttaswamy v Union of India (2017) 10 SCC 1.

International Instruments

Convention on the Elimination of All Forms of Discrimination Against Women (CEDAW) 1979.

Online News and Web Sources

1. 'Cybercrime Cases Reported via National Cyber Crime Reporting Portal Rise from 22,188 in 2020 to 48,475 in 2024' *Medianama* (3 March 2025) https://www.medianama.com/2025/03/223-funding-for-women-focused-cybercrime-scheme-drops-89/ accessed 27 August 2025.
2. 'Cybercrime cases nearly doubled in the national capital in 2022' *Finology Blog* summarizing NCRB data (2022).
3. 'Punjab, Haryana sees rise in crime against women in 2021-22: NCRB' *Indian Express* (30 August 2022).

Additional NCRB Data

Overall crimes against women in India rose from 428,278 in 2021 to 445,256 in 2022 (4% increase), NCRB, *Crime in India 2022* (Government of India, Ministry of Home Affairs 2025).