Legal House Law Journal
ISSN : 3048-779X Volume II Issue III (2025)

CYBER CRIMES AGAINST WOMEN IN INDIA: NEED FOR GENDER-SENSITIVE LEGAL REFORMS IN THE DIGITAL ERA

(Author - Adv. Mrunmayee Mahesh Pawaskar[1], Co-Author - Ms Ananya Yadav[2])

ABSTRACT

Rapid digitalisation in India, accelerated by the Digital India Mission, has exposed women to a growing spectrum of technology-facilitated gender-based violence. From cyberstalking and non-consensual intimate imagery to AI-generated deepfakes and identity theft, cyber crimes against women have emerged as a systemic challenge that existing legal frameworks address only partially. Drawing on doctrinal analysis, comparative law, and judicial precedents, the paper argues that India's legal framework, while markedly improved since 2021, remains structurally deficient in addressing the gendered dimensions of cyber harm. The paper proposes specific gender-sensitive reforms including a standalone law against non-consensual intimate imagery, mandatory gender-disaggregated cybercrime data collection, dedicated cyber courts for gender-based digital violence, and constitutional grounding of digital personhood under Article 21.

Keywords: Cyber crimes, women, BNS 2023, IT Act 2000, deepfakes, NCRB, gender-sensitive law, non-consensual intimate imagery, DPDP Act 2023, IT Rules 2026.

INTRODUCTION

By 2024, India had over 900 million internet users, the second-highest in the world. However, this online growth has not been a gender level playing field. Women who form some share of the Indian population on internet are particularly targeted by the cyber criminals and they

[1] Author, Student LL.M., Chhatrapati Shivaji Maharaj University (Panvel)
[2] Co-Author, Assistant Professor, Chhatrapati Shivaji Maharaj University (Panvel)

experience a different kind of violence which abuses technology and social structures, which are deeply rooted. In 2022, the cases of cybercrime in India increased by 24.4% and there were 65,893 registered cases of cybercrime cases, according to the National Crime Records Bureau (NCRB).[3] More alarmingly, the National Cyber Crime Reporting Portal (NCRP) recorded 76,657 complaints involving women in particular in 2025 an increase of 58% of 48,335 complaints in 2024. These data are just the tip of the iceberg because underreporting is caused by the social stigma, digital illiteracy, and distrust of the enforcement agencies is still prevalent.[4]

Women cyber crimes cover a continuum of cyberstalking, online sexual harassment, voyeurism, identity theft, morphing of images, sextortion, financial fraud, doxxing, and the ever-growing menace of AI-generated deepfake pornography. In contrast to the conventional type of gender-related violence, the purpose of these types of crimes is not only material but also virtual, and is able to impose psychological distress as much as or more difficult to cure. It is further complicated by the legal dimension of the litigation, which is more dynamic than the law, establishing consistent gaps between the damage done to women and the remedies directed on them.

The process of lawmaking by the legislature of India against such menaces has taken three different stages. The former was the Information Technology Act, 2000 and its amendment in 2008 a technology-neutral approach that criminalised cyber offences, but without gender-specificity. The latter included the Criminal Law Amendment Act, 2013, which replicated and improved the convictions against voyeurism, stalking, and sexual harassment and made them

[3]NCRB, "Crime in India 2022" (Ministry of Home Affairs, Government of India, 2023), available at: https://ncrb.gov.in (last visited on Mar. 27, 2026).

[4]Government of India, Ministry of Home Affairs, "Lok Sabha Unstarred Question No. 452" (Dec. 2, 2025), available at: https://www.mha.gov.in/MHA1/Par2017/pdfs/par2025-pdfs/LS02122025/452.pdf (last visited on Mar. 27, 2026). According to government data, 76,657 cases involving women were reported on the NCRP in 2025.

easier to find in Sections 75-79 of the Bharatiya Nyaya Sanhita, 2023.[5] The third and latest stage includes the Digital Personal Data Protection Act, 2023 and the IT (Intermediary Guidelines and Digital Media Ethics Code) Amendment Rules, 2026 which are the first legal expanding expressly on synthetic/AI-generated content such as deepfakes. The paper reviews the issue of this cumulative framework on whether it goes a sufficient distance to capture the gendered reality of cyber crime in India.[6]

OBJECTIVES OF THE STUDY

- To examine the nature, typology, and empirical trends of cyber crimes against women in India from 2019 to 2025.
- To critically analyse the adequacy of existing legal provisions under the BNS 2023, IT Act 2000, DPDP Act 2023, and IT Rules 2026 in addressing gender-based cyber violence.
- To study significant judicial decisions shaping the law on cyber crimes against women in India.
- To assess the structural and institutional deficiencies in the enforcement of cyber crime laws against women.
- To propose evidence-based, gender-sensitive legislative and institutional reforms for India.

METHODOLOGY

[5]The Bharatiya Nyaya Sanhita, 2023 (Act 45 of 2023), ss. 75, 77, 78, 79, 111, 112 (India) (effective July 1, 2024).
[6]The Digital Personal Data Protection Act, 2023 (Act 22 of 2023), ss. 4, 5, 6, 8, 9.

In this paper, the doctrinal-analytical approach is applied. The primary sources are legislation BNS 2023, IT Act 2000, DPDP Act 2023, POCSO Act 2012, PWDVA 2005), subordinate legislation IT Rules 2021 as amended in 2026), court cases, Supreme Court and a range of HCs as well as the official government data and statistics published by NCRB, NCRP, parliamentary debates etc. The sources of secondary data encompass peer reviewed journal articles, reports by statutory agencies (NCW, NITI Aayog, Law Commission of India), policy analysis of civil society organisations. The regulatory frameworks in the UK (Online Safety Act 2023) and in the United States (TAKE IT DOWN Act 2025) are analyzed using the comparative approach. India law Institute (ILI) form of citation is used, and the footnotes are on each page.

EMPIRICAL TRENDS

Classification of Cyber Crimes Against Women

There are six main categories in which cyber crimes against women may be classified into. First online sexual harassment and obscenity including unsolicited sexually explicit messages, revenge pornography, and distribution of obscene material fall under the provisions of 66E and 67 and 67A of the IT act.[7] Second, cyberstalking and cyber-harassment the continuous due to electronic means following, monitoring, or threatening of women, which is outlawed by the Section 78 of the BNS.[8] Third, identity theft and impersonation the opening of a fake social network account, posing as another person, and the unauthorized use of a woman: the punishment may be provided in accordance with 66C and 66D of the IT Act.[9] Fourth, voyeurism and non-consensual intimate images (NCII) the act of recording and sharing intimate images without authorization, which is covered by The Law on Computer-aided

[7]The Information Technology Act, 2000 (Act 21 of 2000), s. 66E, s. 67 and s. 67A.
[8]The Bharatiya Nyaya Sanhita, 2023 (Act 45 of 2023), s. 78.
[9]The Information Technology Act, 2000 (Act 21 of 2000), ss. 66C, 66D.

offences 1977 BNS and Section 66 E IT Act. Fifth, deepfake and AI-generated abuse The development of artificial non-consensual broadcasting images with AI software, now forcibly addressed by the IT Amendment Rules 2026. Sixth, women as victims of online financial frauds as well as matrimonial frauds, investment scams targeting housewives, and account preying.

Year	Total Cybercrime Cases	Cases Involving Women/Children	Increase Over Previous Year
2019	44,546	Data not disaggregated	+12.3%
2020	50,035	Data not disaggregated	
2021	52,974	Data not disaggregated	+5.9%
2022	65,893	Approx. 3,400 (sexual exploitation)	+24.4%
2024	(NCRB pending)	48,335 (NCRP complaints)	
2025	(NCRB pending)	76,657 (NCRP complaints)	+58.5%

Table 1: Cybercrime Trends in India (2019–2025) Source: NCRB, "Crime in India" (2022); MHA Parliamentary Replies (2024, 2025).

Category of Complaint (NCRP 2025)	Number of Complaints
Obscene content / online harassment	37,743
Sexually explicit acts / content	19,703
Rape-related abusive content	8,780
Child sexual abuse material (CSAM)	10,431
Total cases involving women	76,657

Table 2: Category-wise Cybercrime Complaints Against Women/Children NCRP 2025 Source: Government of India, MHA Lok Sabha Unstarred Q. No. 452 (Dec. 2, 2025).

The information provided in Tables 1 and 2 demonstrates an alarming trend. Although overall registered cybercrimes increased at an average rate of 24.4 in 2022, those targeted at women on the NCRP increased by 58.5 percent between 2024 and 2025. Out of the 76, 657 complaints in 2025, the massive majority are having to do with obscene or sexually explicit material

category that mostly harmed women. Most importantly, given that the EPW has identified, of all four individuals who fall prey to cybercrime in India, one of them is a woman but women constitute a tiny percentage of those who report the crime. [10] This paradox of high victimisation but low formal reporting points to a structural failure of gender-sensitive access to justice. [11]

State	Cybercrime Cases 2022 (NCRB)	Crimes Against Women 2022 (NCRB)
Uttar Pradesh	10,117	65,743
Telangana	15,297	18,456
Maharashtra	7,152	45,331
Rajasthan	4,978	45,058
Karnataka	7,118	22,194
Delhi (UT)	2,913	14,247

Table 3: State-wise Cybercrime and Crimes Against Women 2022 Source: NCRB, "Crime in India 2022", Chapter 3A & Chapter 4.

LEGAL FRAMEWORK: A CRITICAL ANALYSIS

The Bharatiya Nyaya Sanhita, 2023

The BNS, which came into effect on 1 July 2024, is the main penal code that will serve in lieu of the colonial criminal code 1860, IPC. An example of cyber crimes against women is that the BNS provides some specific provisions in Chapter V (Offences Against Woman and Child). Section 75 (substituting Section 354A IPC) criminalises sexual harassment such the display of pornography without a women consent or sexually coloured comments by use of electronic media. Section 77 (which replaces the previous Section 354C IPC) covers voyeurism in both its forms of unauthorised recording and internet distribution of intimate photographs, often

[10]The420.in, "Cybercrime Against Women Surges in India, NCRP Data Shows" (Mar. 20, 2026), available at: https://the420.in/india-cybercrime-against-women-ncrp-2025-online-harassment-surge/ (last visited on Mar. 27, 2026).

[11]EPW Research, "Cyber Police Stations and Cybercrime Against Women in India" 59(31) Economic and Political Weekly (Aug. 3, 2024), available at: https://www.epw.in/journal/2024/31/commentary/cyber-police-stations-and-cybercrime-against-women.html (last visited on Mar. 27, 2026).

referred to as revenge porn. Subsection 78 (substituting Subsection 354D IPC), makes crimes of spying on the activities of a woman over the internet or internet email, or contacting her electronically several times without her expressed disdain. Section 79 (to substitute Section 509 IPC) criminalises words, gestures, or objects of any type such as electronic form which is intended to offend the modesty of a woman or intrude to her privacy.

Noteworthy is Section 111 BNS that categorises organised crime to explicitly encompass cyber offences, including cyber extortion, identity theft, phishing, ransomware and botnet activity a clause that has no direct IPC antecedent. Nevertheless, there is a crucial gap: there is no particular provision of the BNS regarding the AI-generated deepfake intimate imagery, or a separate offence of a non-consensual sharing of intimate images (comparable to the UK specific NCII offence designed by the Online Safety Act 2023). It is also in the BNS, which has retained the gendered framing of stalking and voyeurism provisions so that it only applies to female victims, falls into a structural gap to which no non-binary or male victims are appropriate.

Offence	IPC Section	BNS Section	Punishment
Sexual harassment (incl. electronic)	354A	75	3 years / 1 year + fine
Voyeurism / NCII	354C	77	1–3 years + fine
Cyberstalking	354D	78	First: 3 yrs; Subsequent: 5 yrs + fine
Insult to modesty (online)	509	79	1 year simple imprisonment + fine
Organised cybercrime	No equivalent	111	5–10 years + fine (or death)

Table 4: Cyber Offences Against Women IPC to BNS Transition Source: The Bharatiya Nyaya Sanhita, 2023 (Act 45 of 2023); The Indian Penal Code, 1860 (Act 45 of 1860).

The Information Technology Act, 2000 and the 2026 Amendment Rules

The provision that primarily provides statutory armour to combat technology facilitated cyber crimes is the IT Act 2000, as amended in 2008. Its key provisions for crimes against women are Section 66E (violation of privacy through intimate images imprisonment till three years and fine till 2 lakh), Section 67 (obscene electronic material up to three years), Section 67A (sexually explicit material up to five years), and Section 66C-66D (identity theft and impersonation).

The most consequential development in the recent past is the IT (Intermediary Guidelines and Digital Media Ethics Code) Amendment Rules, 2026 which were notified on 10th February 2026 by MeitY and will be effective effective from 20th February 2026. These rules the most comprehensive update to the intermediary liability framework in India bring an explicit definition of "Synthetically Generated Information" (SGI) for the first time under Rule 2(1)(wa), that covers deepfakes and Artificial Intelligence (AI) generated content. The rules require platforms to implement automated means for preventing SGI from constituting non-consensual intimate imagery (NCII), child sexual exploitation material (CSEM) and obscene/sexually explicit content.[12] Critically, the reduction of the takedown timeline for intimate content and NCII related complaints to 36 hours (from 72 hours under the 2021 Rules) and three hours for content adjudged lawful by government order or direction of court is a substantial change. Failure to comply entails loss of the "safe harbour' from liability under Section 79 of the IT Act, i.e. it will be exposed to direct criminal liability.

Complementing the IT Rules 2026, MeitY also issued in November 2025, a Standard Operating Procedure (SOP) on Non-Consensual Intimate Imagery (NCII) to make a structured response mechanism available for victims, intermediaries and the law enforcement agencies. Additionally, a government advisory of 16 March 2026 reiterated platform responsibility in

[12] Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Amendment Rules, 2026, Rule 2(1)(wa), Rule 3(3).

particular when it comes to abusive, defamatory, misleading, and AI generated content. These developments cumulatively refer to the shift from reactive to proactive digital governance in India by no standalone NCII legislation.

The Digital Personal Data Protection Act, 2023

Data protection guarantees data protection duties particularly applicable for the cyber crimes against women according to DPDP Act 2023. Its mandate that data fiduciaries get free, specific and informed consent before they process personal data directly affects platforms that deal with intimate images, location data, and communication metadata which are all typically used as weapons in gender-based cyber crimes. Section 9 of the DPDP Act contains some specific protections of data of children and requires verifiable parental consent, which is of fundamental importance to fight online grooming and CSAM. However, the DPDP Act does not provide for any criminal offences which would mean the direct applicability of the act to perpetrators of cyber crimes against women; the Act plays with the role of data fiduciaries as opposed to individual perpetrators. This institutional gap results in cyber crimes against women's primary criminal liability to date remaining on the IT Act and BNS with the DPDP Act playing a complementary regulatory role.

Allied Legislation

Beyond the main framework, a number of allied statutes will offer a degree of further protection. Protection of women from domestic violence Act, 2005 (PWDVA) has been covered in various ways by the judiciary to extend protection to digital forms of abuse such as cyber stalking and online monitoring in the context of intimate partner relationships.[13] The POCSO Act, 2012 targets online sexual grooming, solicitation and cyberpornography against

[13]The Protection of Women from Domestic Violence Act, 2005 (Act 43 of 2005), s. 3.

minors being another important protection for the ever growing digital nexus of child exploitation.[14] The Indecent Representation of Women (Prohibition) Act, 1986 has been interpreted to cover internet-based indecent representations of women, but the enforcement of this law in the digital world is limited.[15] The Bharatiya Sakshya Adhiniyam, 2023 (BSA) replaces the Indian Evidence Act, 1872 and increases weightage on provisions relating to electronic records and authentication of digital evidence and expert testimony all of which are critical for successful prosecution of cyber crimes.[16]

JUDICIAL DEVELOPMENTS

Indian courts have gradually been dealing with cyber crimes against women, though there are fundamental issues of inconsistency on the way towards dealing with it. The landmark decision of the Supreme Court in Shreya Singhal v. Union of India (2015)[17] struck down Section 66A of IT Act as unconstitutional in utmost terms (vague and overbroad) and emphasized that criminal prohibition on online speech required to be built on narrow basis. While hailed for its free speech implications the decision left a lacuna in prosecuting online harassment and threats a lacuna that has been in part filled by provisions of the BNS (Sections 75, 78, 79).

The right to privacy recognised in *K.S. Puttaswamy v. Union of India* (2017)[18] has been a strong constitutional yardstick for claims of victims of digital intimate violence. The affirmation by the nine-judge Constitution Bench that privacy is an integral part of Article 21 has been cited by the High Courts in suggesting to platforms to remove non-consensual intimate content, identifying with the victim's 'digital personhood.' The Delhi High Court in *X v. Union of India*

[14] The Protection of Children from Sexual Offences Act, 2012 (Act 32 of 2012), ss. 11, 12, 13, 14, 15.
[15] The Indecent Representation of Women (Prohibition) Act, 1986 (Act 60 of 1986), ss. 3, 4, 5, 6.
[16] The Bharatiya Sakshya Adhiniyam, 2023 (Act 47 of 2023), ss. 39, 57, 58, 63.
[17] (2015) 5 SCC 1.
[18] (2017) 10 SCC 1.

(2024)[19] directed the social media platforms to immediately take down AI-generated deepfake content involving women, grounding the order in both the Articles 21 as well as 14 of the constitution. Significantly, the Punjab and Haryana High Court on 5th March 2026 issued the notice of Union ministries on urgent regulatory intervention against deepfakes on following notification of IT Rules, 2026 acknowledging that even the new regulatory framework may not be sufficient.[20]

The Addl. Sessions Court in West Bengal *State of West Bengal v. Animesh Boxi* (2019)[21] delivered first conviction in India for sharing intimate images of a woman without consent using sections 354A, 354C, 509 IPC in conjunction with sections 66E and 67 of the IT Act, The ‘comprehensive approach" by the court, including the combination of criminal punishment, mandatory takedown of materials from platforms and instructions on how to report to them anonymously, has been called by scholars a model for future adjudication of cyber crimes.

The Orissa High Court in *Kalandi Charan Lenka v. State of Orissa* (2017)[22] affirmed the relevance of Section 354D IPC (presently Section 78 BNS) in cases of cyberstalking and denied bail to an accused who had sent obscene messages and had changed his/her fake social media id to stalk a female victim. The court ruled that cyberstalking, though done via electronic means, is no less severe than stalking through physical conduct, and deserves to be punished by the same level of severity under the law.

GAPS AND CRITICAL DEFICIENCIES

[19] W.P. (C) No. 1206/2024 (Delhi High Court, decided Aug. 2024).

[20]Tech Law Forum @ NALSAR, "Rethinking Judicial Approaches to Sexually-Explicit Deepfakes: The Case for Article 21-Based Relief Against Nudifying Websites" (NALSAR University of Law, Mar. 2026), available at: https://techlawforum.nalsar.ac.in (last visited on Mar. 27, 2026).

[21] Sessions Case No. 2 of 2018, Judgment dated Feb. 18, 2019 (Addl. Sessions Court, Tamluk, West Bengal).

[22] 2017 SCC OnLine Ori 81.

Absence of a Standalone Non-Consensual Intimate Imagery Law

India does not have any specific legislation that criminalises non-consensual intimate imagery (NCII) as a term that means the sharing via authentic or AI-generated private sexual images without the consent of the person shared with. While the conduct touched in Section 66E of the IT Act and Section 77 BNS deal with NCII, they do not address all forms of NCII, especially when it comes to AI-generated synthetic intimate imagery of non-celebrities. The UK's Online Safety Act 2023 and the US TAKE IT DOWN Act 2025 show that the combination of legally achievable and operationally required NCII statute is attainable. The IT Rules 2026 take a roundabout to cover this gap through the platform-level obligations, but without a direct criminal offence against the perpetrators, this response on the legal front is incomplete.[23]

Gender-Neutral but Gendered-Reality Framework

While most provisions of the IT Act and the BSA are gender Neutral, the ones in the BNS pertaining to women specifically against stalking, voyeurism and sexual harassment (Sections 75-79) apply to female victims. This gender-specific framing alludes to a reality of empiricism, however, because it leaves out non-binary persons and transgender women. Simultaneously, the gender-neutrality of the IT Act does not ensure gender disaggregated collection of data, which has led to sociological visibility of data pertaining to cyber crimes against women being poor. As the EPW pointed out, there is no systematic data on the gender of victims of cybercrime in NCRB reports there exists a fundamental gap in evidence-based policy formulation. [24]

[23]Vivekananda International Foundation, "Bharatiya Laws Against Deepfake Cybercrime: Opportunities and Challenges" (VIF, Apr. 28, 2025), available at: https://www.vifindia.org/article/2025/april/28/Bharatiya-Laws-Against-Deepfake-Cybercrime-Opportunities-and-Challenges (last visited on Mar. 27, 2026).

[24]SPRF India, "Crimes Against Women in India: Trends, Challenges, and Policy Responses" (SPRF, 2024), available at: https://sprf.in/crimes-against-women-in-india-trends-challenges-and-policy-responses/ (last visited on Mar. 27, 2026).

Low Conviction Rates and Institutional Deficiencies

Despite the massive increase in the legal framework, the conviction rates in cyber crime cases in India still are abysmistly low at less than 15% according to various civil society assessments owing to lack of proper digital forensics infrastructure, under-trained investigating officers, delayed FIR registration especially in the case of online harassment, and lack of understanding of digital evidence by the judiciary as per BS A 2023. The NCRB says that the charge-sheeting rate for cybercrimes in 2022 was 52.8% located and the conviction rate was only 12.3%. Women complainants are also further subject to secondary victimisation of questioning about online behaviour, [25] being dissuaded from filing complaints, and having their cases registered under lesser offences.[26]

The Deepfake Crisis and Regulatory Lag

The deepfake crisis is the most acute emerging crisis. A study conducted in 2023 found that there were 95820 deepfake videos online in the entire world a 550% increase over 2019 with around 98% of them being of women with non-consensual sexual content.[27] In India, deepfake-related High Court cases surged 375% from 2024 to 2025, from 4 to 19 reported cases.[28] While IT Rules 2026 bring in the concept of SGI labelling and platform accountability, the constitutional foundation for take down orders either of Article 21 privacy rights or personality/publicity rights are yet to be able to deal with cases of takedown prospect litigation matter, as non-celebrity women are still subjugated from accessing judicial law right remedy.

[25]Law Commission of India, "Report No. 273 Implementation of United Nations Convention against Cybercrime: New Challenges of Cyberspace" (Law Commission of India, 2024), available at: https://lawcommissionofindia.nic.in (last visited on Mar. 27, 2026).

[26]National Commission for Women, "Cybercrime Against Women: Analysis of Complaints Received, 2022-23" (NCW, 2023).

[27]Data Security Council of India, "India Cyber Threat Report 2025" (DSCI, New Delhi, 2025), available at: https://www.dsci.in/resource/content/india-cyber-threat-report-2025 (last visited on Mar. 27, 2026).

The lack of any dedicated Digital Safety Commissioner, or authority of its sort, leads to an enforcement void.

CONCLUSION

India has taken a significant step towards making legislative gains on cyber crimes against women from the gender blind IT Act 2000 to the specific provisions of the BNS 2023 and the seminal IT Amendment Rules 2026. But the empirical data is clear: 76,657 NCRP complaints in 2025, a 58% increase from the previous year, deepfake cases increasing 375% in one year and conviction rates decrepit below 15% together reveal that something is amiss with the current substantive. The law is running to catch up with technology, whilst women as a disproportionate victim wait for justice.

The basic reform required is a change of philosophy: from viewing cyber-crimes against women as a subset of the general field of cybercrime law, to recognising them as a form of gender-based violence that is deserving of a separate, gender sensitive architectural legal right. This calls for a separate NCII law, mandatory gender-disaggregated data, Digital Safety Authority with powers of enforcement, dedicated-fast track cyber courts, Article 21 constitutional grounding of digital personhood and BNS amendments that extends protection to all gender identities. The IT Rules 2026 is a necessary but not a sufficient step. India needs to legislate on the realities of the digital world in which gender-based violence has found its most scalable and invisible form.