



CYBER HARASSMENT AND GENDER-BASED CRIME IN INDIA: A CRITICAL STUDY OF SEXTORTION, CYBERSTALKING AND DOXXING

Rekha Rani^a

^aAssistant Professor, School of Legal Studies, NIILM University, Kaithal, Haryana (136027), India

ABSTRACT :

Cyber harassment threatens equal participation in India's digital public sphere through coercion, persistent surveillance and exposure of personal information. This paper examines sextortion, cyberstalking and doxxing using descriptive secondary-data analysis and a critical reading of Indian law. The quantitative core comprises registered cybercrimes against women across all thirty-six States and Union Territories during 2021–2023, supplemented by national cybercrime totals and published studies of online abuse. Registered cases against women increased from 10,730 to 19,510, an 81.8 per cent rise. Karnataka accounted for 35.9 per cent of 2023 total and 54.2 per cent of national increase across period. These findings indicate substantial growth and concentration in recorded cases, without establishing population prevalence or identifying contribution of each harassment subtype. Evidence from Amnesty International and Plan International illustrates how platform abuse and self-reported consequences capture dimensions that police statistics cannot measure. The legal analysis identifies uneven coverage of sexual coercion, gender-specific stalking and harmful disclosure, alongside February 2026 acceleration of intimate-image complaint responses. The paper recommends separate behavioural indicators, linked complaint and case tracking, confidential evidence preservation and independently evaluated survivor services. Effective protection requires measuring safety and continued digital participation alongside criminal justice outcomes.

Keywords: cyber harassment; gender-based violence; sextortion; cyberstalking; doxxing; India; secondary-data analysis.

Introduction

Digital communication creates opportunities for education, employment, intimate relationships and political expression. It also enables an offender to reach a person repeatedly, reproduce intimate material and assemble information about her residence, workplace or social network. Harassment therefore affects more than an isolated message: it can restrict a person's ability to communicate, move safely and maintain relationships. UNFPA places sextortion, cyberstalking and doxxing within technology-facilitated gender-based violence, recognising connection between digital conduct and offline harm (UNFPA, 2025).

The three practices require distinct analysis. Sextortion exploits threatened sexual exposure to obtain compliance; cyberstalking involves persistent unwanted pursuit or monitoring; doxxing makes identifying information available in ways that facilitate targeting. They may occur together, but combining them under a single label obscures different evidence and remedies each requires. An intimate-image threat needs rapid containment and secure preservation. Repeated monitoring requires evidence of conduct over time. Disclosure of an address may require immediate physical protection even when disclosed information is accurate.

This study asks three questions. How did registered cybercrimes against women change nationally and geographically during 2021–2023? What additional dimensions emerge from published platform and survey research? How adequately do Indian legal provisions address behaviours constituting three practices? Its contribution is a transparent connection between observable administrative patterns, limits of available evidence and specific proposals for legal and institutional reform. It does not infer that rising registrations necessarily represent an equivalent rise in victimisation.

The central argument is that criminal recognition, statistical visibility and practical protection must be examined together. A conduct category can be punishable through several provisions yet remain invisible in national tables. Conversely, a recorded increase can reflect improved reporting rather than deteriorating safety. Policy evaluation consequently needs a clear account of what each dataset counts and which aspects of survivors' experiences it excludes.

An empirical approach is especially useful where public discussion moves quickly from disturbing examples to general claims. Individual episodes can reveal mechanisms and institutional failures, but they cannot establish how common a practice is. National tables offer wider coverage but less detail. Bringing two levels into conversation requires resisting both generalisation of exceptional examples and dismissal of harms absent from administrative categories. This paper treats distinction as a substantive research problem, because design of an indicator can influence which injuries receive public attention.

Research Design and Methodology

The study uses descriptive analysis of published aggregate data, rather than a newly administered survey. Its principal dataset is Annexure I of Ministry of Home Affairs parliamentary answer dated 24 March 2026, reproducing NCRB registrations and rates for cybercrimes against women during 2021–2023 (MHA, 2026). The extraction covers thirty-six jurisdictions and three years, producing 108 jurisdiction-year observations. National totals are treated as summaries and are not added as independent observations. General cybercrime totals are obtained from government's March 2026 parliamentary release (PIB, 2026).

Variables are jurisdiction, year, registered cases and published crime rate. Counts are transcribed with their category labels and checked against State, Union Territory and national totals. Calculations include annual growth, cumulative growth, compound annual growth, national shares and contribution to national increase. Annual growth equals difference from previous year's count divided by that previous count, multiplied by one hundred. Compound annual growth across 2021–2023 uses two intervals. Jurisdictions with a zero initial count receive no percentage-growth estimate.

The six jurisdictions with highest 2023 counts are selected only for comparative display; calculations of totals and concentration use complete dataset. This distinction prevents a convenience selection from being presented as nationally representative. Charts separate registered-case trends, geographic concentration and survey consequences. Percentages from different sources are not pooled, because they refer to different populations, denominators and observation periods. Rate comparisons use published rounded values and therefore remain approximate.

Amnesty International's study of Indian women politicians provides platform-based evidence, while Plan International's multinational survey provides self-reported experiences and consequences. These are purposively selected complementary sources, not an exhaustive literature review. Their results are discussed within their original scope. The analysis does not download individual posts, contact participants or republish identifying disclosures. The study uses published aggregates rather than individual communication records.

The legal component reads statutory elements relevant to coercion, monitoring, image dissemination and disclosure. It distinguishes historical IPC setting of dataset from current BNS framework and separately considers IT Rules as amended in February 2026. Findings are descriptive and interpretive. Three annual observations cannot support a reliable causal model, forecast or evaluation of newer legislation. The reproducibility material records data, formulas and sources underlying every quantitative exhibit.

Quality checks distinguish a numerical zero from missing information. For extracted counts, a reported zero remains a zero and is not replaced with an assumed positive value. Rates are retained as published rather than reconstructed from rounded figures. Percentage results are rounded only after calculation and year attached to a value denotes year of registration rather than later release date. These choices prevent artificial precision and make tables auditable. Another researcher can reproduce results without access to confidential complaints or proprietary platform records.

Concepts and Gendered Mechanisms

For this analysis, sextortion means a threat to reveal sexual information or imagery used to demand money, additional images, sexual activity or other compliance. Cyberstalking means repeated unwanted digital pursuit or monitoring, interpreted more broadly for research than any particular statutory definition. Doxxing means exposing identifying or private information to facilitate harassment or place someone at risk. These operational categories draw on international descriptions but are not asserted to be separate Indian statutory offences (UNFPA, 2025).

Gender enters analysis through substance of threats, social consequences of disclosure and unequal costs of withdrawing from digital spaces. A threatened disclosure can exert pressure because an offender anticipates family sanctions, workplace hostility or sexual stigma. These are plausible mechanisms requiring direct investigation; administrative totals cannot measure their frequency. The analysis therefore avoids portraying every cybercrime involving a woman as necessarily motivated by gender.

Overlap is equally important. An offender may monitor accounts, identify relatives and threaten to send them intimate material. Coding only financial demand would lose stalking and exposure components. A behaviour-based research design should allow multiple flags for one episode while maintaining a separate count of unique episodes. This would permit analysis of combinations without artificially inflating total number of affected persons or registered cases.

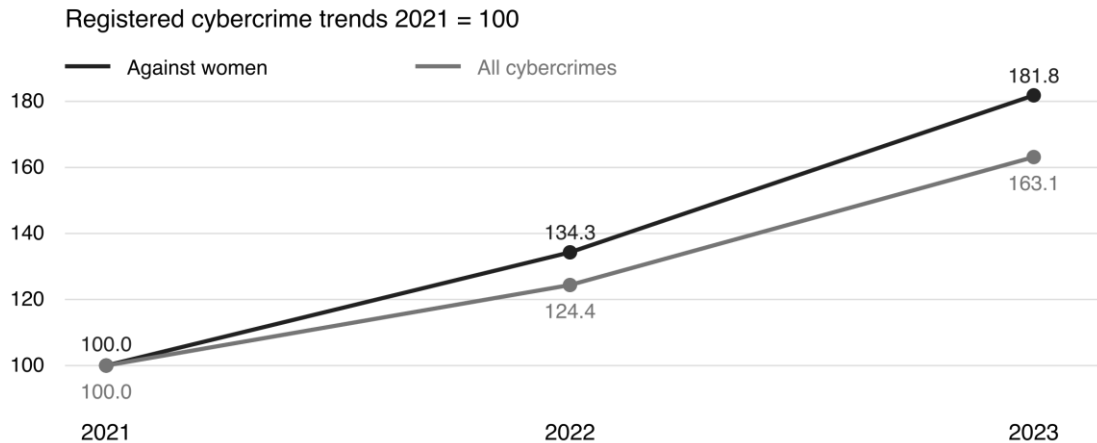
Empirical Findings

Table 1 presents national series. Registered cybercrimes against women increased by 3,679 in 2022 and 5,101 in 2023. The corresponding annual increases were 34.3 and 35.4 per cent. The cumulative increase was 8,780 cases or 81.8 per cent and compound annual growth rate was 34.8 per cent. General cybercrime registrations rose by 63.1 per cent across same period. These are calculations from published counts, rather than estimates of changes in actual exposure (MHA, 2026; PIB, 2026).

Table 1. National registered cybercrime series and calculated comparisons

Year	All cybercrime cases	Cases against women	Annual growth (%)	Ratio of series (%)
2021	52,974	10,730	—	20.3
2022	65,893	14,409	34.3	21.9
2023	86,420	19,510	35.4	22.6

Sources: MHA (2026); PIB (2026). Ratio = women-specific cases / all cybercrime cases × 100; it is not a reconciled distribution of individual victims by gender.

Figure 1. Indexed growth in registered cybercrime series, 2021–2023

Sources: MHA (2026), Annexure I; PIB (2026), Annexure I. Calculated index; 2021 = 100. This chart measures registrations, not victimisation prevalence.

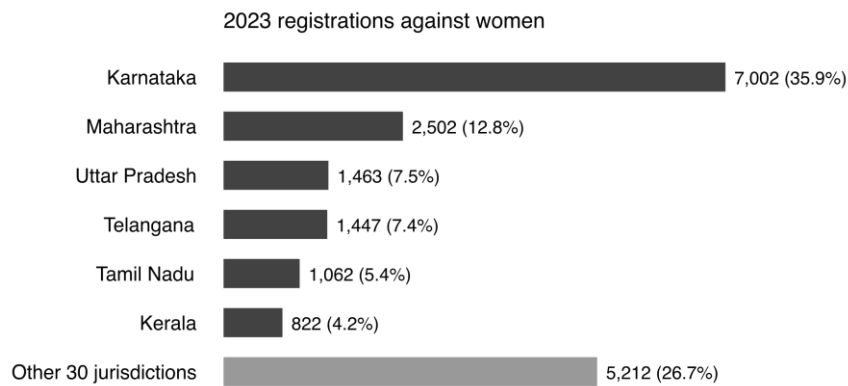
The ratio of women-specific series to all cybercrime registrations increased from 20.3 per cent in 2021 to 21.9 per cent in 2022 and 22.6 per cent in 2023. This comparison describes published series; it should not be interpreted as a fully reconciled distribution of all victims by gender. Without case-level linkage and classification rules, it cannot establish share of individual victims who were women or proportion of cybercrime that involved sexual harassment.

Geographic concentration is substantial. The six largest 2023 counts sum to 14,298 cases, representing 73.3 per cent of national total. Karnataka alone contributes 7,002 cases or 35.9 per cent. Its increase from 2,243 in 2021 contributes 4,759 of national increase of 8,780, equivalent to 54.2 per cent. After excluding Karnataka from both endpoints, remaining jurisdictions show growth of 47.4 per cent. National growth is consequently broad enough to persist under this sensitivity check, but its magnitude depends heavily on one jurisdiction.

Table 2. Six jurisdictions with highest registered counts in 2023

Jurisdiction	2021 cases	2022 cases	2023 cases	2023 share (%)	2023 rate
Karnataka	2,243	3,904	7,002	35.9	21.0
Maharashtra	1,697	2,530	2,502	12.8	4.1
Uttar Pradesh	958	1,101	1,463	7.5	1.3
Telangana	883	1,262	1,447	7.4	7.6
Tamil Nadu	248	401	1,062	5.4	2.8
Kerala	353	381	822	4.2	4.4

Source: MHA (2026), Annexure I. Share calculated against national total; rate reproduced as published, per lakh population in source category. Selection is based on 2023 counts.

Figure 2. Geographic concentration of registered cybercrimes against women, 2023

Source: MHA (2026), Annexure I. Percentages use 19,510 national registrations. Other jurisdictions are aggregated, not an individual State.

Counts and published rates answer different questions. Uttar Pradesh's 2023 count exceeds Telangana's, while its published rate is lower. Comparing two solely through counts would therefore obscure population size. However, even population-adjusted rates remain registration measures: they do not adjust for internet access, time online, awareness or police recording practices. A rate per internet user would require a compatible denominator unavailable in this dataset.

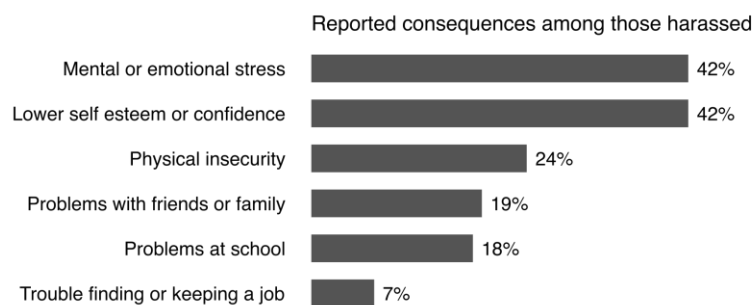
Variation within leading group also cautions against a uniform national narrative. Maharashtra's count falls slightly between 2022 and 2023, while Tamil Nadu's rises sharply. Neither movement demonstrates success or failure of a particular intervention. A credible explanation would require investigating changes in recording, reporting access and case composition. The practical implication is to examine jurisdictions individually before translating national trends into resource allocations or institutional performance rankings.

The concentration calculation also suggests an evaluation strategy. Researchers could compare how complaints are received and coded in jurisdictions with large and small registered totals, using a common protocol. The purpose would be to identify differences in institutional access and classification before attributing differences to offending. Such work should include ordinary police stations and support organisations as well as specialist cyber units. Otherwise, a study may overlook complaints handled outside specialist system and mistakenly equate visibility of one agency with performance of entire response network.

Evidence Beyond Police Registrations

Amnesty International analysed more than 114,000 tweets mentioning ninety-five Indian women politicians during 2019 election period. It reported that 13.8 per cent were problematic or abusive. The organisation distinguished hostile content from narrower abuse category and described targeting associated with gender, religion, caste and other identities (Amnesty International, 2020). This is evidence about a particular platform and politically visible group, not a prevalence estimate for all Indian women or any of three offences.

Plan International's quantitative study involved 14,071 interviews with girls and young women aged fifteen to twenty-five across twenty-two countries, including India. Its global findings reported online harassment among 58 per cent of respondents. Among those harassed, 42 per cent reported mental or emotional stress, 42 per cent lower self-esteem or confidence and 24 per cent physical insecurity (Plan International, 2020a, 2020b). Figure 3 retains this conditional denominator and does not present global values as Indian statistics.

Figure 3. Self-reported consequences of online harassment in a multinational survey

Global survey results multiple responses possible

Sources: Plan International (2020a), p. 28; Plan International (2020b). Denominator: respondents who experienced harassment. Global findings, not India-specific estimates; categories overlap.

These sources measure different levels of harm: posts, reported experiences and registered cases. Their value lies in complementarity rather than numerical equivalence. A single survivor may receive many abusive posts, experience one prolonged episode and have no registered case. Future Indian research should connect these levels through consent-based designs. Until then, differences between their percentages should not be used to calculate reporting gaps, multiply national victim counts or claim that one data source validates another's prevalence estimate.

Sextortion and Sexual Coercion

Sextortion requires attention to both threatened exposure and demanded benefit. A financial demand accompanied by a threat to publish intimate material raises different legal questions from a demand for further sexual images. Completed extortion under BNS section 308 involves dishonest inducement to deliver property or valuable security; criminal intimidation under section 351 addresses qualifying threats intended to alarm or compel conduct. A sexual demand does not automatically satisfy property element of completed extortion (NCRB, n.d.).

The critical empirical gap is absence of a clean sextortion variable in extracted women-specific totals. Broad motive categories such as extortion or sexual exploitation would also be imperfect substitutes. They may include different behaviours, genders and factual settings. Consequently, this paper cannot calculate sextortion's national share, growth or conviction rate. Presenting entire increase as sextortion would make an unsupported inference.

A better record would distinguish money, sexual activity, imagery and other demanded compliance, together with whether threat was attempted, executed or repeated. Researchers should also distinguish genuine intimate material from impersonated or synthetic material. These fields would clarify coercion without requiring publication of images. Protection should begin with threat and its likely consequences, rather than depend exclusively on proof that money was transferred or an image was already disseminated.

Cyberstalking and Persistent Monitoring

BNS section 78 addresses a man's repeated pursuit of a woman despite disinterest and, separately, monitoring her internet or electronic communications. The electronic-monitoring limb should not be collapsed into repeated-contact limb. Its gendered wording also means that this specific provision does not provide universal coverage of every perpetrator–victim configuration (NCRB, n.d.). Research definitions should capture conduct outside that statutory pairing while acknowledging distinction.

The evidentiary problem is temporal. A complaint containing one screenshot may conceal months of contact across multiple accounts. Blocking may stop one channel while pursuit continues elsewhere. Recording each message independently can overcount episodes, while reducing everything to one isolated exchange can understate persistence. An episode-based timeline should therefore retain dates, channels, account changes, expressed disinterest and any connection to offline contact.

Institutional assessment should measure recurrence after intervention, rather than only initial complaint outcome. A closed complaint does not demonstrate that monitoring ended. With consent and confidentiality safeguards, follow-up could examine whether unwanted contact resumed, whether protective measures helped and whether person remained able to use digital services. These questions translate concept of safety into observable outcomes while avoiding assumptions that police registrations alone can answer them.

Doxxing and Informational Exposure

Doxxing directs attention to relationship between information and risk. A residence, telephone number or workplace can be used to mobilise others against an individual. Even information once available publicly may become more harmful when aggregated and distributed to a hostile audience. The analytical question is therefore not confined to whether information is secret; it includes targeting, context, consent and foreseeable consequences.

India's criminal framework does not make every unwanted disclosure punishable merely because it is called doxxing. Applicable provisions depend on accompanying conduct, such as qualifying intimidation, unlawful access or misuse of identity credentials. IT Act section 66E concerns images of private bodily areas and is not a general prohibition on exposing addresses or phone numbers (Government of India, 2000). This distinction prevents a privacy provision from being stretched beyond its statutory elements.

The available registrations do not identify doxxing episodes separately. Statistical silence is therefore not evidence that practice is rare. A research instrument should record information disclosed, its original accessibility, intended audience, associated threats and whether offline targeting followed. Public outputs must remove identifying details: reproducing a hostile disclosure in an academic appendix can repeat harm. Aggregated coding and confidential source storage provide a more proportionate evidentiary approach.

Constitutional and Statutory Assessment

The recognition of privacy in *Justice K.S. Puttaswamy v. Union of India* connects informational and bodily autonomy with constitutional dignity (Supreme Court of India, 2017). It provides a framework for scrutinising state responses, while criminal liability still requires an applicable offence and proven elements. Privacy protection cannot substitute for careful charging decisions or justify unrestricted surveillance of everyone using digital services.

Table 3. Behaviour-based comparison of legal routes

Behaviour	Relevant legal route	Limit requiring attention
Sextortion	BNS ss. 308, 351; IT Act ss. 66E, 67A where applicable	Completed extortion requires delivery of specified property; sexual demands need fact-specific analysis.
Cyberstalking	BNS s. 78; other applicable offences	Section 78 uses a man–woman pairing; research coverage should be broader.
Doxxing	Qualifying intimidation under BNS s. 351; IT Act s. 66 for dishonest/fraudulent unauthorised access, where proved	No universal offence of unwanted disclosure; s. 66E concerns private bodily images.

Sources: NCRB (n.d.), statutory text; Government of India (2000). Routes are conditional, not an exhaustive charge list. The BNS framework is distinguished from IPC period of dataset.

The IT Act offers relevant but bounded tools: sections 66C and 66D address specified identity misuse and cheating by personation; sections 67 and 67A concern qualifying obscene or sexually explicit electronic material (Government of India, 2000). Their application turns on conduct and content proved. These provisions do not create a single comprehensive offence covering all unwanted digital behaviour.

Under consolidated IT Rules updated in February 2026, rule 3(2)(b) requires reasonable and practicable removal or disabling measures within two hours after receipt of qualifying complaints involving intimate exposure or electronic impersonation, including morphed images (MeitY, 2026). This channel is distinct from criminal prosecution and does not automatically apply to every doxxing disclosure. Short deadlines require evaluation through actual response records, not an assumption of effective implementation.

Reform must also respect expression. *Shreya Singhal v. Union of India* invalidated IT Act section 66A; it cannot be proposed as a current remedy for offensive messages (Supreme Court of India, 2015). Any new offence should define prohibited conduct, mental elements and legitimate exceptions precisely. Protection from coercion and targeting should coexist with lawful criticism, public-interest reporting and proportionate investigation.

Discussion and Limitations

The findings support a limited but consequential conclusion: women's cybercrime registrations grew considerably and unevenly across observed period. They do not identify which harassment practice drove increase. Geographic concentration creates a priority for investigation, rather than proof of geographic differences in underlying propensity to offend. The same high count can coexist with better complaint access, more victimisation or changes in classification.

Several limitations follow. Police data omit unreported experiences and can reflect inconsistent recording. Aggregate series cannot identify repeat victims, overlapping behaviours, offender relationships or case trajectories. Published platform research concerns a selected group and historical period; survey indicators are global and age-specific. Source definitions are not interchangeable. The legal analysis considers newer provisions, while quantitative window predates their operation, preventing evaluation of their impact.

These constraints make a causal interpretation inappropriate. No regression is attempted because three years of aggregate registrations and missing exposure variables would produce weak explanatory claims. Descriptive calculations remain useful because they reveal concentration, document scale and specify questions for subsequent inquiry. An empirical paper gains credibility by reporting these boundaries alongside its results, rather than supplying apparently precise estimates for quantities its sources cannot observe.

A further limitation concerns whose experiences are visible. The women-specific administrative category cannot represent every person exposed to gendered digital harm. Neither can it reveal differences by disability, caste, sexuality, age or offender relationship without additional disaggregation. Future collection should allow voluntary disclosure and avoid making sensitive identity information a condition of receiving assistance. Researchers must also assess participation bias: people who can safely discuss harassment may differ from those whose family circumstances, dependence on an offender or fear of disclosure prevent participation in a study.

These considerations support cautious interpretation and stronger future measurement. The evidence presented here establishes a baseline for further inquiry, with its scope stated explicitly so that subsequent studies can extend analysis without treating descriptive findings as causal proof.

Future evaluation should predefine outcomes and follow-up periods before examining results. This would reduce selective reporting and allow interventions to be compared on consistent terms, including recurrence, response time, access to assistance and survivors' ability to continue their digital activities.

Conclusion and Suggestions

India needs a coordinated approach that identifies behaviour, preserves evidence and assesses survivors' safety. First, NCRB and complaint systems should develop separately defined flags for sextortion, persistent digital monitoring and harmful identifying disclosures. The flags should permit overlap, while maintaining distinct totals for episodes, victims and cases. Published tables should explain exclusions and changes in definitions so researchers can distinguish genuine trends from statistical discontinuities.

Second, institutions should link complaint receipt, registration, investigation and disposal through confidential identifiers. Aggregate releases should report elapsed time and reasons for closure, without exposing complainants. This would permit assessment of movement through system rather than

comparison of incompatible totals. It would also clarify whether rapid platform containment and criminal investigation operate together or leave survivors navigating disconnected processes.

Third, police and platform procedures should preserve relevant evidence securely while restricting public access to harmful content. Investigators need timelines and contextual records, not unnecessary copies of intimate material circulated among officials. Access controls, retention schedules and documented handling should accompany digital collection. The same principle applies to doxxing: evidence of disclosure should be preserved without repeating identifying information in publicly accessible records.

Fourth, statutory review should examine sexual coercion beyond property demands and stalking beyond present gender pairing. Any proposed doxxing provision should require defined harmful conduct and safeguards for lawful publication. Drafting should be informed by anonymised case analysis identifying where existing provisions actually fail. A broad prohibition on material described as offensive would create uncertainty and risk restrictions on legitimate expression.

Finally, independent evaluation should examine recurrent harassment, physical insecurity and continued access to education, employment and public discussion. Survivor interviews and an ethically recruited Indian survey could supply evidence absent from registrations. The present study establishes a reproducible administrative baseline and exposes limits of that baseline. Its principal finding is that growth in recorded cases warrants action, while effective action requires evidence specific to each behaviour and to outcome of protection

REFERENCES

- Amnesty International. (2020, January 23). India: Women politicians face shocking scale of abuse on Twitter—new research. <https://www.amnesty.org.uk/knowledge-hub/all-resources/india-women-politicians-face-shocking-scale-abuse-twitter-new-research/>
- Government of India. (2000). The Information Technology Act, 2000 (Act No. 21 of 2000), as amended. India Code. https://www.indiacode.nic.in/bitstream/123456789/13116/1/it_act_2000_updated.pdf
- Ministry of Electronics and Information Technology [MeitY]. (2026). The Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021, updated as on 10 February 2026. <https://www.meity.gov.in/static/uploads/2026/02/550681ab908f8afb135b0ad42816a1c9.pdf>
- Ministry of Home Affairs [MHA]. (2026, March 24). Cyber crime against women (Lok Sabha Unstarred Question No. 5108, Annexure I). Government of India. Data source: NCRB, Crime in India 2021–2023. <https://www.mha.gov.in/MHA1/Par2017/pdfs/par2026-pdfs/LS24032026/5108.pdf>
- National Crime Records Bureau [NCRB]. (n.d.). Bharatiya Nyaya Sanhita, 2023: Chapters and statutory text. CyTrain. Retrieved September 15, 2026, from https://cytrain.ncrb.gov.in/staticpage/web_pages/ChaptersBNS.html
- Plan International. (2020a). Free to be online? Girls' and young women's experiences of online harassment. The State of World's Girls 2020. https://www.plan.org.hk/wp-content/uploads/2020/10/Plan_International_FULL-Comms-Report_IDG2020_FreedomOnline_Freetobeonline_EN.pdf
- Plan International. (2020b). Free to be online? Executive summary. The State of World's Girls 2020. <https://plan-international.org/uploads/2022/02/sotwgr2020-execsummary-en-3.pdf>
- Press Information Bureau [PIB]. (2026, March 17). Cyber crime cases (Annexure I, cybercrime registrations 2021–2023). Government of India. <https://www.pib.gov.in/PressReleasePage.aspx?PRID=2241339&lang=2®=3>
- Supreme Court of India. (2015). Shreya Singhal v. Union of India, (2015) 5 SCC 1; [2015] 5 SCR 963. https://cdnbbsr.s3.waas.gov.in/s3ec0490f1f4972d133619a60c30f3559e/documents/aor_notice_circular/35.pdf
- Supreme Court of India. (2017, August 24). Justice K.S. Puttaswamy (Retd.) v. Union of India, (2017) 10 SCC 1. https://api.sci.gov.in/supremecourt/2012/35071/35071_2012_Judgement_24-Aug-2017.pdf
- United Nations Population Fund [UNFPA]. (2025, November 26). Technology-facilitated gender-based violence: A growing threat. <https://www.unfpa.org/TFGBV>