CYBERSECURITY AND CYBERSTALKING IN INDIA: CURRENT STATUS, FUTURE PROSPECTS, LIMITATIONS AND CHALLENGES - A REVIEW

Mukesh Shukla, Pt. Parmeshwar Deen Law College, Atrauli, Hardoi, Uttar Pradesh, India.

ABSTRACT

India's digital expansion has been among the fastest in recorded history, and its exposure to cyber harm has expanded with it. This review synthesises official statistics, legal instruments, parliamentary documents, industry telemetry and peer-reviewed scholarship to assess two interlocking problems: the state of national cybersecurity and the specific, gendered problem of cyberstalking. Reported cybercrime cases rose from 27,248 in 2018 to 86,420 in 2023, while incidents handled by the national computer emergency response team crossed two million in 2024. Financial losses reported through the national reporting portal rose from about ₹7,465 crore in 2023 to about ₹22,846 crore in 2024. Against this, the country secured Tier 1 status in the International Telecommunication Union's Global Cybersecurity Index 2024, operationalised its data protection statute through subordinate rules in November 2025, and became the first jurisdiction to mandate provenance metadata for synthetic media in February 2026. Cyberstalking sits awkwardly inside this architecture. It is under-counted, narrowly defined in gender-specific terms under Section 78 of the Bharatiya Nyaya Sanhita, 2023, poorly served by conviction data, and inadequately studied through Indian victimisation surveys. The review argues that India's cyber governance has advanced substantially at the level of institutions and statutes, but remains constrained by an enforcement deficit, a federal division of policing responsibility, a severe skills shortage, and an evidence base too thin to support precise policy design. Directions for future research and policy are set out.

Keywords: cybersecurity, cyberstalking, cybercrime, India, Bharatiya Nyaya Sanhita, digital personal data protection, technology-facilitated abuse, victimisation

1. Introduction

India crossed 886 million active internet users in 2024, growing roughly eight per cent year on year, with rural users (488 million) accounting for 55 per cent of the total (IAMAI & Kantar, 2025). Much of this growth comes from first-generation users accessing the internet on shared devices, in Indic languages, with limited exposure to formal digital-safety education. The same infrastructure that delivers welfare payments, identity verification and instant retail payments also delivers phishing messages, investment scams, non-consensual intimate imagery and persistent unwanted pursuit.

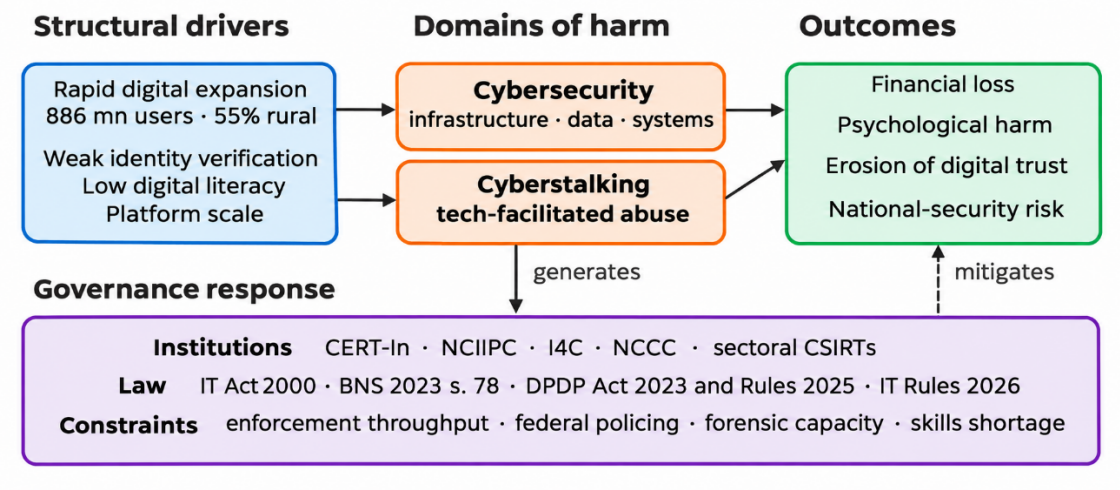
Two problems are examined here. The first is cybersecurity understood broadly - the protection of information systems, critical infrastructure and personal data from unauthorised access, disruption or exploitation. The second is cyberstalking, understood as the repeated use of electronic communication to pursue, monitor, threaten or harass an identified individual in a manner that would cause a reasonable person fear or substantial distress (Reyns et al., 2011; Spitzberg & Hoobler, 2002). The two are usually treated separately: cybersecurity as a technical and national-security domain, cyberstalking as an interpersonal or criminological one. Treating them together is analytically useful for India, because the same weaknesses - weak identity verification, thin enforcement capacity, low digital literacy, and platforms that operate at a scale regulators cannot match - produce both a vulnerable critical infrastructure and a permissive environment for technology-facilitated abuse (Kshetri, 2016; Sambasivan et al., 2019).

This review addresses four questions. What is the current status of cybersecurity and cyberstalking in India? What are the realistic future prospects, given current policy trajectories? What are the limitations of the available evidence? And what challenges obstruct effective response?

Figure 1 sets out the framework organising the review: structural drivers of exposure, the two domains of harm they produce, the outcomes that follow, and the governance response that is meant to interrupt the sequence.

Figure 1

Conceptual framework of the review: drivers, domains of harm, outcomes and governance response



Note: Constructed by the author. User figures from IAMAI and Kantar (2025); institutional and legal elements as described in Sections 4.3 and 4.4.

2. Method

This is a narrative review conducted in the tradition of integrative synthesis rather than a formal systematic review, because the relevant material spans legal instruments, administrative statistics, parliamentary records and empirical scholarship that cannot be pooled quantitatively (Holt & Bossler, 2014). Four categories of sources were consulted. First, official Indian sources: National Crime Records Bureau reports, parliamentary questions and committee reports, gazette notifications, judgments, and press releases of the Ministry of Home Affairs and the Ministry of Electronics and Information Technology. Second, multilateral and standard-setting sources, including the International Telecommunication Union and the United Nations Office on Drugs and Crime. Third, peer-reviewed literature on cyberstalking, cyber victimisation and cyber governance, drawn from criminology, cyberpsychology, information systems and human–computer interaction. Fourth, industry and civil-society telemetry, used cautiously and only where methodology is disclosed.

Because official statistics and industry telemetry measure different things and rest on different denominators, figures from different sources are reported separately and not aggregated. Where

a claim rests on a single commercial source, that provenance is stated in the text.

3. Conceptual and Theoretical Foundations

3.1 Defining the terms

Cybercrime resists stable definition. Wall (2007) distinguishes computer-integrity crimes, computer-assisted crimes and computer-content crimes, a taxonomy that maps reasonably onto Indian statutory practice, where offences are split across the Information Technology Act, 2000 and the general penal code. Yar (2005) argued that much cybercrime is not novel in its motivation but is transformed in its opportunity structure, a point that anticipates the Indian pattern in which the dominant reported motive remains ordinary fraud (National Crime Records Bureau [NCRB], 2025).

Cyberstalking has an even less settled definition. Bocij and McFarlane (2003) treated it as a course of conduct involving repeated threats or harassment through electronic means; Spitzberg and Hoobler (2002) operationalised it through obsessive relational intrusion; Sheridan and Grant (2007) questioned whether it is qualitatively distinct from offline stalking at all, finding substantial overlap. Pittaro (2007) emphasised the offender's intent to intimidate, while Basu and Jones (2007) argued that the regulatory difficulty lies in capturing a course of conduct made up of individually lawful acts. Parallel confusion affects cyberbullying, where Tokunaga (2010) and Kowalski et al. (2014) documented prevalence estimates varying by an order of magnitude across studies as a direct consequence of measurement inconsistency. Kaur et al. (2021), in a systematic review of 49 empirical studies, concluded that inconsistent conceptualisation and measurement is the field's central methodological weakness. This matters for India, because the statutory definition in Section 78 of the Bharatiya Nyaya Sanhita, 2023 is narrower than any of the scholarly definitions and shapes what gets recorded.

Table 1 compares the principal definitions against the Indian statutory formulation and shows why the two diverge.

Table 1: *Competing definitions of cyberstalking and their measurement implications*

Source	**Defining emphasis**	**Implication for measurement**

Spitzberg and Hoobler (2002)	Obsessive relational intrusion carried into computer-mediated channels	Captures low-level persistence that criminal law ignores
Bocij and McFarlane (2003)	Course of conduct of repeated threats or harassment by electronic means	Requires repetition; a single severe act falls outside
Pittaro (2007)	Offender intent to intimidate, threaten or instil fear	Intent is difficult to evidence from platform records
Reyns et al. (2011)	Repeated unwanted pursuit online producing fear or distress in a reasonable person	Victim-centred; supports survey measurement
Kaur et al. (2021)	Synthesis of 49 studies; no convergent operational definition	Cross-study and cross-country comparison unreliable
Bharatiya Nyaya Sanhita, 2023, s. 78	A man following or repeatedly contacting a woman despite disinterest, or monitoring her electronic communication	Gender-specific and conduct-limited; narrowest of the six

3.2 Theoretical frames

Routine activity theory, originally formulated to explain direct-contact predatory crime (Cohen & Felson, 1979), has been adapted for online environments. Reyns et al. (2011) proposed a cyberlifestyle–routine activities model in which online exposure, proximity to motivated offenders, target attractiveness, online deviance and the absence of capable guardianship predict cyberstalking victimisation; their study of 974 students supported each component. Leukfeldt and Yar (2016) found the theory's explanatory power varies by offence type, performing better for offences with a clear convergence of victim and offender. Choi (2008) and Bossler and Holt (2009) extended guardianship to technical controls, showing that software-based protection alone is a weak predictor relative to behavioural factors.

Self-control theory (Gottfredson & Hirschi, 1990) has been applied to both perpetration and victimisation, with Reyns et al. (2018) finding that opportunity and control balance outperformed low self-control in explaining cyberstalking victimisation among college women. Jaishankar's (2008) space transition theory, developed partly in an Indian context, argues that individuals behave differently in cyberspace because of anonymity, identity flexibility, and the dissociative effect of the absence of deterrence - a framework that fits the

Indian pattern of dispersed, low-cost, high-volume offending.

Feminist and socio-legal frameworks supply what opportunity theories omit. Citron (2009, 2014) argued that online harassment of women constitutes a civil-rights harm, not merely an individual grievance, because its cumulative effect is to drive women out of public digital space. Powell and Henry (2017) and Henry and Powell (2018) situate cyberstalking within technology-facilitated sexual violence, a continuum that includes image-based abuse, monitoring and doxing. In the Indian context, Halder and Jaishankar (2011, 2016) documented secondary victimisation - harm inflicted on the victim by the response of police, family and community - as a structuring feature of cyber gender harassment.

4. Current Status of Cybersecurity in India

4.1 The threat surface

Reported incident volumes provide the clearest longitudinal picture. The Indian Computer Emergency Response Team (CERT-In) recorded 1,158,208 incidents in 2020, 1,402,809 in 2021, 1,391,457 in 2022, 1,592,917 in 2023 and 2,041,360 in 2024 (Ministry of Electronics and Information Technology [MeitY], 2025). The government subsequently reported that CERT-In handled approximately 2.944 million incidents in 2025, alongside 1,530 alerts and 390 vulnerability notes (Press Information Bureau [PIB], 2026). Because reporting is partly voluntary and smaller organisations frequently do not disclose, these figures should be read as a floor rather than an estimate of true incidence.

Table 2 sets the incident series against the corresponding budget allocation for cyber security by the Ministry of Electronics and Information Technology, and Figure 2 places the series beside the separate count of cybercrime cases registered by police.

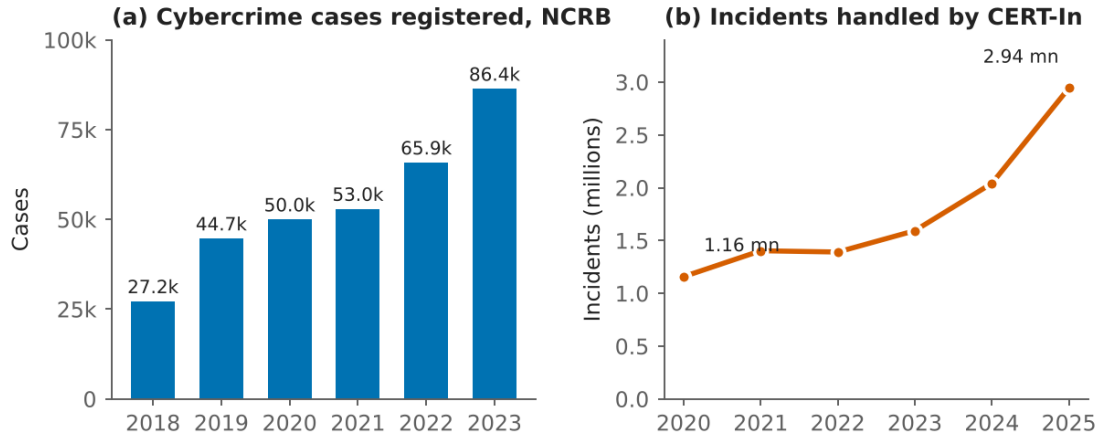
Table 2: *Cyber security incidents handled by CERT-In and MeitY cyber security budget, 2020–2025*

Year	Incidents handled	Change on previous year	MeitY cyber security budget (₹ crore)
2020	1,158,208	-	293 (FY 2020–21)
2021	1,402,809	+21.1%	411 (FY 2021–22)

2022	1,391,457	−0.8%	462 (FY 2022–23)
2023	1,592,917	+14.5%	580 (FY 2023–24)
2024	2,041,360	+28.1%	1,004 (FY 2024–25)
2025	≈2,944,000	+44.2%	Not reported

Note. Incident counts and budget figures for 2020–2024 from MeitY (2025a); the 2025 incident figure from PIB (2026). Percentage changes calculated by the author. Reporting is partly voluntary, so counts are a floor rather than an estimate of true incidence.

Figure 2: *Reported cybercrime cases and cyber security incidents handled, 2018–2025*



Note. Panel (a) from NCRB (2025); panel (b) from MeitY (2025a) and PIB (2026). The two panels count different things - police case registrations and technical incident reports - and are therefore plotted separately rather than on a shared axis.

Endpoint telemetry offers a complementary view. The Data Security Council of India [DSCI] and Seqrite (2024) reported 369.01 million malware detections across 8.44 million endpoints - an average of 702 detections per minute - with Trojans (43.25%) and infectors (34.10%) dominating, and banking and financial services, healthcare and hospitality among the most targeted sectors. This is a single vendor's installed base and cannot be generalised to the national device population, but the sectoral pattern is consistent with incidents reported elsewhere.

Critical information infrastructure has been directly targeted. The November 2022 ransomware attack on the All India Institute of Medical Sciences, New Delhi, disabled hospital systems for

an extended period and exposed sensitive records, and remains the most-cited domestic illustration of the operational consequences of an attack on a designated critical sector (Parliamentary Standing Committee on Home Affairs, 2025). Global benchmarking places breach costs for Indian organisations at record levels and identifies skills shortages and supply-chain exposure as the dominant aggravating factors (IBM Security, 2024; World Economic Forum, 2025). Attribution of intrusions in the power and government sectors to state-linked actors has been repeatedly asserted by commercial threat-intelligence firms and repeatedly complicated by the attribution problem itself.

4.2 Financial cybercrime

Financial fraud is now the dominant form. Complaints on the National Cybercrime Reporting Portal rose from 1,029,026 in 2022 to 1,596,493 in 2023 and 2,268,346 in 2024 (Ministry of Home Affairs [MHA], 2025). Reported losses to cyber fraud stood at ₹7,465.18 crore in 2023 and ₹22,845.73 crore in 2024, an increase of about 206 per cent, across 3,637,288 reported financial-fraud incidents in 2024 (MHA, 2025). Indian Cyber Crime Coordination Centre (I4C) data compiled through the portal placed 2025 losses at about ₹19,813 crore across roughly 2.18 million cheating-related complaints, with cumulative six-year losses of about ₹52,976 crore, and indicated that 45 per cent of complaints originated from Southeast Asian jurisdictions - principally Cambodia, Myanmar and Laos (Indo-Asian News Service, 2026).

The Parliamentary Standing Committee on Home Affairs (2025) recorded 5.393 million complaints on the portal between 2019 and November 2024, involving approximately ₹31,594 crore, with about 85 per cent classified as cyber-financial crime. Recovery remains the weak link: data reviewed in mid-2026 showed 1.271 million complaints and ₹10,178.97 crore in reported losses in the first half of that year, with only about ₹2,969 crore - under 30 per cent - placed under bank lien (Anantam, 2026). The gap between money lost and money preserved is the single most consequential operational failure in the current system.

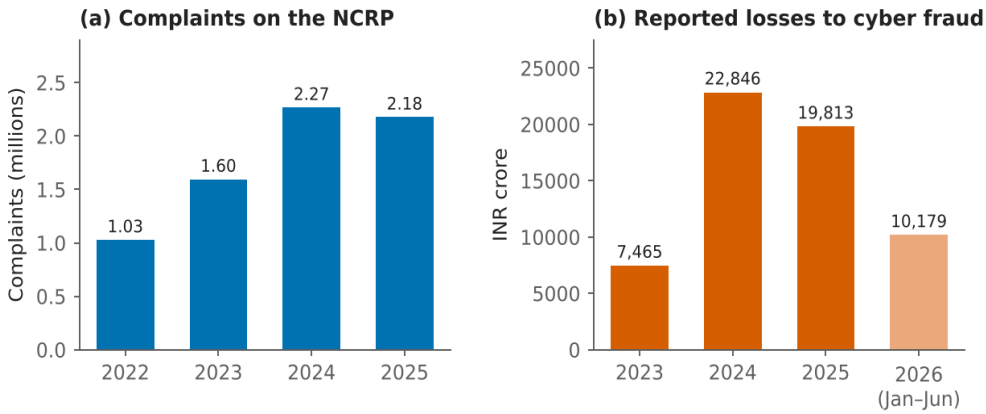
Table 3 assembles the complaint and loss series, and Figure 3 displays them.

Table 3: *Complaints and reported financial losses on the National Cybercrime Reporting Portal, 2022–2026*

Period	Complaints	Reported loss (₹ crore)	Observation
2022	1,029,026	Not separately reported	+127.4% on 2021
2023	1,596,493	7,465.18	+55.2% complaints on 2022
2024	2,268,346	22,845.73	Loss up ≈206% on 2023
2025	2,177,524 (cheating-related)	19,812.96	45% of complaints traced to South-East Asia
Jan–Jun 2026	1,271,000	10,178.97	₹2,968.85 crore (≈29%) placed under bank lien
2019 – Nov 2024 (cumulative)	5,393,000	≈31,594	≈85% classified as cyber-financial crime

Note. Rows for 2022–2024 from MHA (2025); 2025 from Indo-Asian News Service (2026); the 2026 half-year row from Anantam (2026); the cumulative row from the Parliamentary Standing Committee on Home Affairs (2025). The 2025 complaint figure counts cheating-related fraud complaints and is not strictly comparable with the all-category counts above it.

Figure 3: *Complaints and reported losses to cyber fraud*



4.3 Institutional architecture

India's cyber institutions are numerous and functionally distinct. CERT-In, established under Section 70B of the Information Technology Act, 2000, is the national incident-response agency

and issues directions including the six-hour incident-reporting requirement of April 2022 (CERT-In, 2022). The National Critical Information Infrastructure Protection Centre, constituted under Section 70A, protects designated critical sectors (NCIIPC, 2015). The National Cyber Coordination Centre performs situational awareness; the National Cyber Security Coordinator sits within the National Security Council Secretariat; and sectoral incident-response teams operate for finance and power (MeitY, 2025a).

On the crime side, I4C under the Ministry of Home Affairs coordinates the National Cybercrime Reporting Portal, the 1930 helpline and the Citizen Financial Cyber Fraud Reporting and Management System. In September 2024 four further instruments were launched: a Cyber Fraud Mitigation Centre co-locating banks, telecom operators, payment intermediaries and police; the Samanvay platform for cybercrime data sharing and analytics; a Cyber Commandos programme intended to train about 5,000 specialists over five years; and a national Suspect Registry (PIB, 2024).

Sectoral regulators add a further layer. The Reserve Bank of India's cyber security framework for banks (RBI, 2016) and its master direction on information technology governance (RBI, 2023) impose board-level accountability, while the Securities and Exchange Board of India's Cybersecurity and Cyber Resilience Framework (SEBI, 2024) extends comparable obligations across regulated market entities.

Table 4 maps the resulting architecture.

Table 4: *India's principal cybersecurity and cybercrime institutions*

Body	**Parent authority**	**Basis**	**Core function**
CERT-In	MeitY	s. 70B, IT Act, 2000	National incident response, alerts, advisories, audit empanelment
NCIIPC	National Technical Research Organisation	s. 70A, IT Act, 2000	Protection of designated critical information infrastructure
NCCC	MeitY, through CERT-In	Administrative	Situational awareness from cyberspace metadata
National Cyber Security Coordinator	National Security Council Secretariat	Administrative	Inter-agency coordination

I4C	Ministry of Home Affairs	Central sector scheme, 2018	Cybercrime coordination; NCRP and helpline 1930
Cyber Fraud Mitigation Centre	I4C	Launched 2024	Co-location of banks, telecom operators, intermediaries and police
Samanvay platform	I4C	Launched 2024	Cybercrime data repository, mapping and analytics
Suspect Registry	I4C	Launched 2024	National database of cybercrime suspects
Sectoral CSIRTs	CERT-In	Administrative	Sector response, including finance and power
RBI and SEBI frameworks	RBI; SEBI	Regulatory directions	Board-level cyber-resilience duties for regulated entities

Note. Compiled from MeitY (2025a), NCIIPC (2015), PIB (2024), RBI (2016, 2023) and SEBI (2024).

4.4 Legal and regulatory framework

The Information Technology Act, 2000, as amended in 2008, remains the principal statute, covering unauthorised access (s. 43, s. 66), identity theft (s. 66C), impersonation (s. 66D), violation of privacy through image capture or transmission (s. 66E), and obscene or sexually explicit electronic content (ss. 67, 67A, 67B). Section 79 provides conditional safe harbour for intermediaries, read down constitutionally in *Shreya Singhal v. Union of India* (2015), which struck down Section 66A and confined takedown obligations to court or authorised government orders.

The three new criminal statutes - the Bharatiya Nyaya Sanhita, 2023, the Bharatiya Nagarik Suraksha Sanhita, 2023, and the Bharatiya Sakshya Adhiniyam, 2023 - replaced the colonial-era codes with effect from July 2024. They carry forward stalking (BNS s. 78), sexual harassment (s. 75), voyeurism (s. 77), and organised crime provisions, and formalise electronic FIRs and audio-video recording of proceedings. Electronic evidence continues to be governed by the certification regime interpreted in *Anvar P.V. v. P.K. Basheer* (2014) and *Arjun Panditrao Khotkar v. Kailash Kushanrao Gorantyal* (2020), now restated in the Bharatiya Sakshya Adhiniyam.

Data protection arrived late. The Digital Personal Data Protection Act, 2023 gave statutory form to the privacy right recognised in *K. S. Puttaswamy v. Union of India* (2017), but remained inoperative until the Digital Personal Data Protection Rules, 2025 were notified on 13–14 November 2025 (MeitY, 2025b). The Rules adopt a three-phase schedule: provisions constituting the Data Protection Board took effect immediately, consent-manager registration applies after twelve months, and the substantive obligations - notice, security safeguards, breach notification, and significant data fiduciary duties - apply from May 2027.

Most recently, the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Amendment Rules, 2026, notified as G.S.R. 120(E) on 10 February 2026 and effective 20 February 2026, brought "synthetically generated information" within the due-diligence framework (MeitY, 2026). Platforms offering synthetic-content tools must label such content prominently and embed persistent provenance metadata; significant social media intermediaries must obtain and verify user declarations; the takedown window for court- or government-flagged unlawful content was compressed from thirty-six hours to three; and a two-hour window applies to complaints concerning non-consensual intimate imagery, including morphed and deepfake material.

Table 5 summarises the instruments and their bearing on cyberstalking specifically, and Figure 6 places them on a timeline.

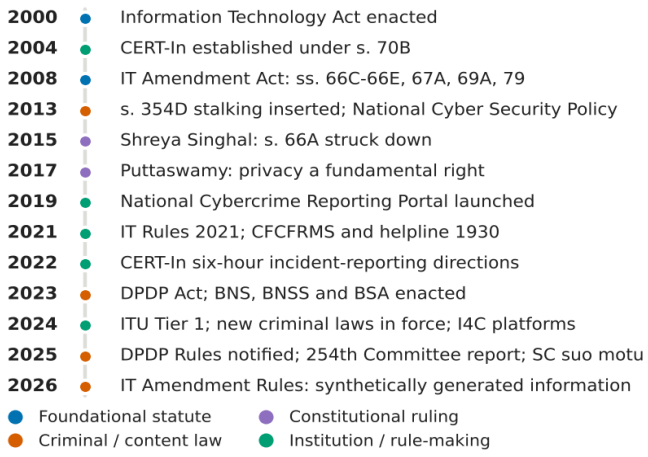
Table 5: *Legal instruments governing cybersecurity and cyberstalking in India*

Instrument	**Key provisions**	**Principal scope**	**Bearing on cyberstalking**
Information Technology Act, 2000 (am. 2008)	ss. 43, 66, 66C, 66D, 66E, 67, 67A, 69A, 79	Unauthorised access, identity misuse, privacy, content	ss. 66E, 67 and 67A carry image-based abuse
Bharatiya Nyaya Sanhita, 2023	ss. 75, 77, 78, 79	Sexual harassment, voyeurism, stalking, insult to modesty	s. 78 is the principal stalking offence
Bharatiya Nagarik Suraksha Sanhita, 2023	Electronic FIR; audio-video recording	Criminal procedure	Zero-FIR and electronic filing ease reporting

Bharatiya Sakshya Adhiniyam, 2023	Electronic records and certification	Evidence	Admissibility of device and platform records
POCSO Act, 2012	ss. 11–15	Offences against minors	Online sexual harassment of children
Indecent Representation of Women (Prevention) Act, 1986	ss. 3–4	Degrading depiction	Pre-digital drafting limits online use
DPDP Act, 2023 and Rules, 2025	Notice, consent, security safeguards, breach notification	Personal data	Curtails the leaked-data supply that enables pursuit
IT Rules, 2021, as amended 2026	r. 3(1)(d); SGI labelling and provenance	Intermediary due diligence	3-hour and 2-hour takedown; deepfake provenance
Telecommunications Act, 2023	Subscriber identity verification	Telecom	Addresses SIM-based anonymity

Note. Compiled by the author. Phased application of the DPDP Rules runs to May 2027; the 2026 amendment to the IT Rules took effect on 20 February 2026.

Figure 6: *Timeline of principal legal and institutional milestones, 2000–2026*



4.5 International standing and cooperation

India was placed in Tier 1 - "role-modelling" - of the International Telecommunication Union's Global Cybersecurity Index 2024, with a score of 98.49 out of 100 across the legal, technical,

organisational, capacity-development and cooperation pillars (ITU, 2024). The gap between this score, which measures institutional commitment, and the enforcement outcomes described below is itself an important finding.

India has not acceded to the Council of Europe's Convention on Cybercrime (2001), objecting historically to provisions on transborder access to stored data and to its exclusion from the drafting process. It participated actively in negotiating the United Nations Convention against Cybercrime, adopted by the General Assembly in December 2024 and opened for signature at Hanoi in October 2025, where 72 states signed; India did not sign at that ceremony, and the question of ratification was subsequently raised before the Supreme Court (UNODC, 2025).

5. Current Status of Cyberstalking in India

5.1 Official Data

The National Crime Records Bureau recorded 86,420 cybercrime cases in 2023, a 31.2 per cent increase over the 65,893 cases of 2022, with the rate per lakh population rising from 4.8 to 6.2 (NCRB, 2025). The series shows near-continuous growth: 27,248 (2018), 44,735 (2019), 50,035 (2020), 52,974 (2021), 65,893 (2022), 86,420 (2023). Of the 2023 total, 44,237 cases were registered under the Information Technology Act and 41,849 under the penal code. Fraud accounted for 68.9 per cent of cases (59,526), sexual exploitation for 4.9 per cent (4,199) and extortion for 3.8 per cent (3,326). Karnataka reported the highest volume (21,889), followed by Telangana (18,236) and Uttar Pradesh (10,794); Telangana recorded the highest rate at 47 per lakh.

Table 6: *Cybercrime cases registered in India, 2018–2023*

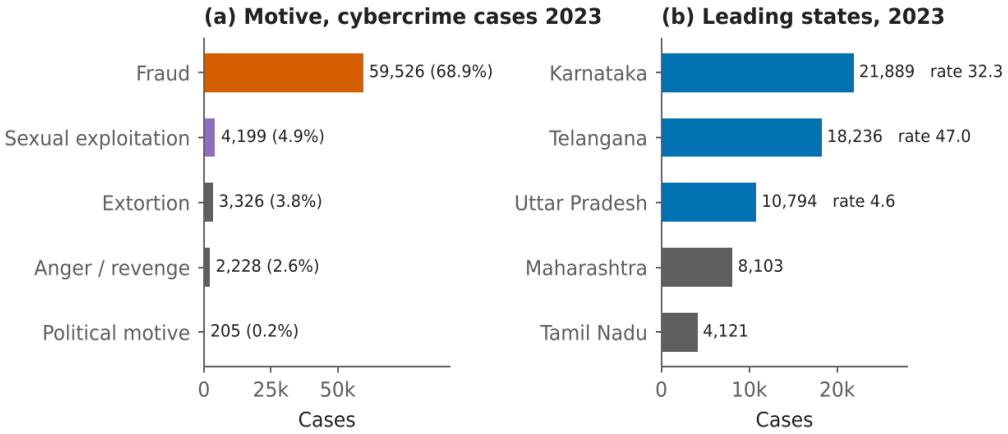
Year	Cases registered	Change on previous year	Rate per lakh population
2018	27,248	-	-
2019	44,735	+64.2%	-
2020	50,035	+11.8%	-
2021	52,974	+5.9%	-
2022	65,893	+24.4%	4.8
2023	86,420	+31.2%	6.2

Cyberstalking appears in this data only faintly. States and union territories reported 1,305 cases of cyberbullying and stalking of women and children in 2023, alongside 689 cases of cyber blackmailing or threatening, 2,168 cases of circulating sexually explicit material, and 1,472 cases where such material concerned children (NCRB, 2025). Against 86,420 total cases and a female population of roughly 690 million, 1,305 recorded cases of online stalking and bullying is not a plausible estimate of prevalence. It is a measure of reporting and classification, not of occurrence.

Table 7: *Cyberstalking-relevant offence heads, 2023*

Offence head	**Cases**	**Share of all cybercrime cases**
Cyberbullying and stalking of women and children	1,305	1.5%
Publication or transmission of sexually explicit material	2,168	2.5%
Sexually explicit material involving children	1,472	1.7%
Cyber blackmailing or threatening	689	0.8%
Fake news on social media	209	0.2%
All cybercrime cases	86,420	100%

Figure 4: *Motive behind cybercrime cases and leading states, 2023*



5.2 What independent evidence suggests

Independent sources point to a far larger problem. Sambasivan et al. (2019), in a qualitative study of 199 women and six NGO staff across India, Pakistan and Bangladesh, found that a

majority regularly contended with online abuse, with cyberstalking, impersonation and personal-content leakage as the three dominant forms; consequences included emotional harm, reputational damage, and physical and sexual violence. Critically, participants coped through informal channels - deleting accounts, withdrawing, involving family - rather than through platform tools or law enforcement. The same research group had earlier documented performative privacy practices among South Asian women, including device sharing and self-censorship, that both reflect and reproduce surveillance within households (Sambasivan et al., 2018).

Stalkerware - commercial monitoring software installed on a device, usually by someone with physical access - provides a partial quantitative proxy. Kaspersky (2024) reported 31,031 unique affected users globally in 2023, with India third after Russia and Brazil at 2,492 affected users; India has appeared in the top three every year since 2019. Because detection depends on the vendor's installed base, and because the most common installer is an intimate partner or family member, these figures materially understate prevalence (Chatterjee et al., 2018; Freed et al., 2018). Southworth et al. (2007) established early that intimate partner abusers adopt consumer monitoring technologies faster than advocacy and legal systems adapt to them, a pattern that has held for two decades.

For minors, McAfee (2022) reported that 85 per cent of surveyed Indian children aged 10–18 had experienced cyberbullying - the highest rate among the ten countries surveyed - with rates of racist cyberbullying (42%), sexual harassment (30%), threats of personal harm (28%) and doxing (23%) roughly double the global average, and 45 per cent of Indian children concealing these experiences from parents. Longitudinal Indian evidence from the UDAYA cohort in Uttar Pradesh and Bihar showed cyberbullying victimisation rising from 3.8 to 6.4 per cent among young women and 1.9 to 5.6 per cent among young men over three years, with victimisation significantly associated with subsequent depressive symptoms and suicidal ideation (Maurya et al., 2022); a follow-up analysis identified self-efficacy and parental communication as partial mediators (Maurya et al., 2023).

Table 8: *Selected empirical evidence on cyberstalking and cyber victimisation relevant to India*

Study	Design and sample	Principal finding
Sambasivan et al. (2019)	Qualitative; 199 women and 6 NGO staff; India, Pakistan, Bangladesh	Cyberstalking, impersonation and content leakage dominant; coping overwhelmingly informal
Maurya et al. (2022)	Longitudinal UDAYA cohort; 4,428 and 11,864; Uttar Pradesh and Bihar	Victimisation rose 3.8%→6.4% (female) and 1.9%→5.6% (male); linked to depression and suicidal ideation
Maurya et al. (2023)	Structural equation model; same cohort	Self-efficacy and parental communication partially mediate the effect on depression
McAfee (2022)	Survey; 11,687 parents and children; 10 countries	85% of Indian children cyberbullied - highest of the ten countries
Kaspersky (2024)	Vendor telemetry; 2023	India third globally, 2,492 affected users; top three every year since 2019
Stevens et al. (2021)	Systematic review; 43 studies	42 of 43 report adverse mental-health consequences
Kaur et al. (2021)	Systematic review; 49 studies	Definitional and measurement inconsistency is the field's central weakness
Halder and Jaishankar (2011)	Comparative socio-legal; US, UK, India	Secondary victimisation is structural in the Indian response
Reyns et al. (2011)	Survey; 974 students; United States	Exposure, proximity, guardianship and online deviance predict victimisation

Note. Compiled by the author. Designs and denominators differ, so findings are not pooled.

5.3 Consequences

The international literature is consistent on harm. Stevens et al. (2021), reviewing 43 studies, found that 42 reported adverse mental-health consequences for victims of cyberstalking or cyber harassment, including depression, anxiety, panic attacks and suicidal ideation, together with distrust of technology and dissatisfaction with criminal-justice responses. Dreßing et al. (2014) found clinically significant psychopathology among cyberstalking victims in a large social-network sample. Fissel and Reyns (2020) documented costs extending into work,

education and social functioning. Short et al. (2015) reported that harm intensity is driven less by the severity of any single act than by persistence over time - which is precisely the feature that episodic, complaint-driven policing is least equipped to detect.

In India these effects are compounded by secondary victimization. Halder and Jaishankar (2011) showed comparatively that Indian victims of cyber gender harassment face disproportionate institutional victimization, and Miftha et al. (2019, 2022) documented how reputational anxiety, family pressure and fear of social punishment deter reporting, producing what they term deindividuation of the victim. The result is a self-reinforcing cycle: low reporting produces low official counts, low counts justify low institutional priority, and low priority further suppresses reporting.

5.4 The legal treatment of cyberstalking

Section 78 of the Bharatiya Nyaya Sanhita, 2023 carries forward Section 354D of the Indian Penal Code, itself inserted by the Criminal Law (Amendment) Act, 2013 following the recommendations of the Justice Verma Committee (Verma et al., 2013). It provides that "any man" who follows a woman and repeatedly contacts or attempts to contact her despite a clear indication of disinterest, or who "monitors the use by a woman of the internet, e-mail or any other form of electronic communication," commits stalking. Punishment extends to three years on first conviction and five years on a second or subsequent conviction. Three statutory exceptions apply, covering crime prevention by persons, conduct under law, and conduct that is reasonable and justified in the circumstances. Four limitations follow directly from this drafting. First, the offence is gender-specific in both directions: only a man can commit it, and only a woman can be the victim, leaving male, transgender and non-binary victims, and female perpetrators, outside its scope - a design recognised as constitutionally arbitrary following the recognition of privacy as a fundamental right in *Puttaswamy* (2017). Second, the conduct element is confined to following and contacting, or monitoring internet use; courts have declined to extend it beyond this, as in a 2025 Himachal Pradesh High Court decision holding that merely photographing a person did not satisfy the definition. Third, the section does not squarely cover third-party proxy stalking, doxing, or the deployment of stalkerware by someone other than a man against a woman. Fourth, sentencing of up to three years places most first-offence stalking in a category where investigation is unlikely to be resourced against the volume of financial-fraud complaints competing for the same units. Adjacent provisions fill

gaps imperfectly. Section 66E of the Information Technology Act, 2000 addresses privacy violations through image capture and transmission; Sections 67 and 67A address obscene and sexually explicit publication; Section 79 of the Bharatiya Nyaya Sanhita addresses words or gestures intended to insult a woman's modesty; the Indecent Representation of Women (Prevention) Act, 1986 addresses degrading depiction, though its pre-digital drafting limits its utility online (Halder, 2013); and the Protection of Children from Sexual Offences Act, 2012 covers minors. The Amendment Rules of 2026 add a two-hour takedown obligation for non-consensual intimate imagery, which is the most practically significant recent development for victims of image-based abuse (MeitY, 2026). India's first recognised cyberstalking case, the Manish Kathuria matter of 2001 involving impersonation of Ritu Kohli, had to be prosecuted under general penal provisions because no specific offence then existed (Halder & Jaishankar, 2012) - a reminder of how recent the statutory framework is.

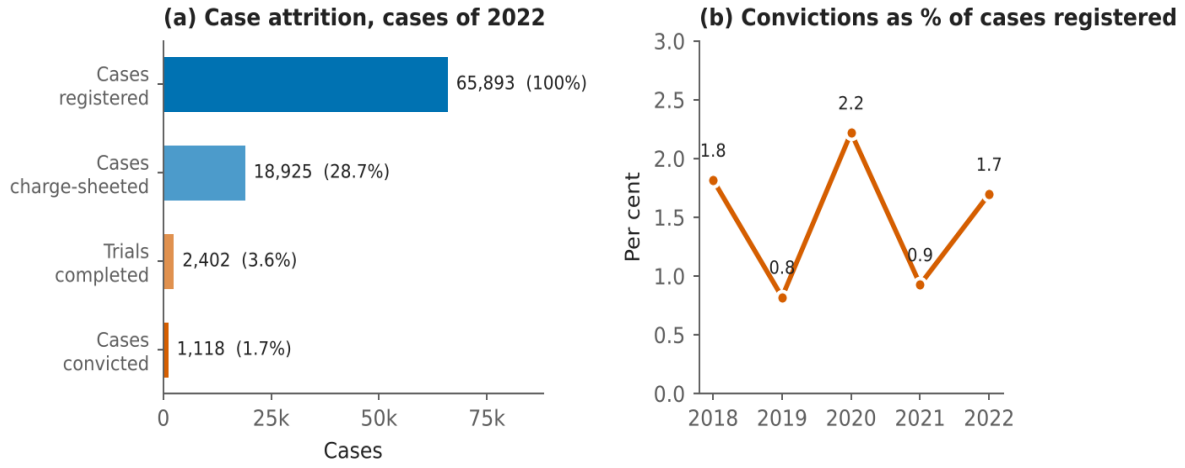
5.5 The enforcement gap

For cybercrime cases as a whole, 65,893 cases were registered in 2022, of which 18,925 were charge-sheeted, trials were completed in 2,402, and 1,118 resulted in conviction (MeitY, 2025a). The corresponding figures for earlier years show the same shape: 50,035 registered and 1,110 convicted in 2020; 52,974 registered and 491 convicted in 2021. Fewer than two per cent of registered cases reach conviction in the same period, and the number of completed trials is a small fraction of charge-sheeted cases, indicating that the binding constraint is judicial and forensic throughput rather than police registration alone. State-level reporting for Karnataka indicated 44 convictions against 60 acquittals in 2023, with conviction rates in Bengaluru below 0.3 per cent.

Table 9: *Disposal of cybercrime cases, 2018–2022*

Year	Cases registered	Charge-sheeted	Trials completed	Convicted	Convictions as % of cases registered
2018	27,248	7,234	1,044	495	1.8%
2019	44,735	9,187	1,051	367	0.8%
2020	50,035	14,176	1,626	1,110	2.2%
2021	52,974	18,744	1,155	491	0.9%
2022	65,893	18,925	2,402	1,118	1.7%

Figure 5: *Criminal justice attrition in cybercrime cases*



6. Future Prospects

6.1 Artificial intelligence on both sides of the line

Generative systems have lowered the cost of the two inputs that cyberstalking and fraud most require: plausible identity and plausible content. Voice cloning, face swapping and synthetic intimate imagery convert what was previously a technically demanding attack into a consumer activity. India's response - the 2026 Amendment Rules - is, in its labelling and provenance requirements, the first binding statutory scheme of its kind, and its practical effect over the next two years will be watched internationally (MeitY, 2026). The core question is enforceability: provenance metadata survives only where every tool in the pipeline preserves it, and open-weight models running locally are outside the reach of platform obligations.

The same technologies offer defensive leverage. Behaviour-based detection already accounts for a meaningful share of endpoint detections (DSCI & Seqrite, 2024), and machine-learning models applied to transaction graphs are the most plausible route to identifying mule-account networks at the speed at which funds move - a direction the Supreme Court has itself pressed upon the Reserve Bank (Supreme Court of India, 2025b).

6.2 Consolidating fragmented law

The Parliamentary Standing Committee on Home Affairs (2025) recommended a consolidated cybercrime statute defining offences coherently, an Integrated Cybercrime Task Force, State Cybercrime Coordination Centres in every state and union territory, expert verticals within the

telecom regulator, enforceable mechanisms for obtaining data held abroad, and a twenty-four-hour unit for coordination with foreign agencies. It also recommended reviewing intermediary safe harbour - a proposal that attracted dissenting notes from committee members warning of free-expression and federalism consequences (Parliamentary Standing Committee on Home Affairs, 2025). Whether consolidation occurs, and on what terms, is the most consequential open question in Indian cyber law.

6.3 Data protection as a security instrument

Full application of the Digital Personal Data Protection Rules, 2025 in May 2027 will, for the first time, impose enforceable breach-notification and security-safeguard obligations on data fiduciaries, with penalties reaching ₹250 crore for security failures under the parent Act. If the Data Protection Board operates independently and consent does not degenerate into a click-through ritual, the Rules could materially reduce the supply of leaked personal data on which both fraud and stalking depend (MeitY, 2025b).

6.4 International cooperation

Ratification of the United Nations Convention against Cybercrime would give India treaty-based mutual legal assistance and expedited preservation mechanisms with a broader set of states than existing bilateral arrangements (UNODC, 2025). Given that a substantial share of complaints now originates in Southeast Asian scam compounds, and that trafficked Indian nationals are among those coerced into operating them, cooperation instruments are no longer optional for effective investigation.

6.5 Capacity and the workforce

Estimates of India's cybersecurity workforce shortfall vary widely by methodology and should be treated with caution, but every available estimate is large, and the Data Security Council of India's skilling assessment identifies specialised roles - cloud-native security, operational technology, AI-assisted forensics - as the acute gaps rather than generalist roles (DSCI, 2026). The Cyber Commandos programme addresses police capacity specifically, but 5,000 specialists across a country policing several million annual complaints is an order of magnitude short of need.

6.6 Judicial momentum

The Supreme Court's suo motu proceedings on digital-arrest scams, initiated in October 2025 after an elderly couple in Ambala was defrauded of ₹1.05 crore using forged court orders, resulted in a December 2025 direction placing a nationwide investigation with the Central Bureau of Investigation, permitting recourse to Interpol, directing intermediaries to cooperate, requiring states to establish cybercrime centres expeditiously, and asking the Reserve Bank about machine-learning detection of mule accounts (Supreme Court of India, 2025a, 2025b). Judicial supervision of an investigative programme of this scale is unusual, and its results will indicate whether centralisation can overcome the coordination problems of state-level policing.

7. Limitations

7.1 Limitations of the evidence base

Under-reporting is systematic, not random. Sambasivan et al. (2019) and Miftha et al. (2022) both find that Indian women preferentially cope through informal channels; reporting is therefore selected on social position, family support and the severity of the precipitating incident, which means official data are biased in unknown directions rather than merely incomplete.

Registration data are not victimisation data. NCRB figures count FIRs, not victims or incidents, and the "principal offence" rule suppresses secondary offences in multi-offence cases. Rising counts confound genuine increases with improved reporting infrastructure - the National Cybercrime Reporting Portal itself generates registrations that would not previously have existed.

Definitional instability. Kaur et al. (2021) identify the absence of a common operational definition as the field's central weakness. Indian studies variously use cyberstalking, cyber harassment, cyberbullying and online abuse interchangeably, making cross-study comparison unreliable.

No national victimisation survey. India has no recurring, methodologically robust survey of cyber victimisation comparable to the Crime Survey for England and Wales. In its absence, prevalence estimates rest on convenience samples, commercial surveys with undisclosed sampling, or vendor telemetry.

Commercial telemetry has structural bias. Stalkerware and malware counts reflect a vendor's installed base and detection logic. Kaspersky (2024) and DSCI and Seqrite (2024) are informative about direction and composition, not about national prevalence.

Publication and language bias. Much Indian scholarship on cyberstalking appears in journals with limited indexing and inconsistent peer review, while Indian-language research is largely invisible in international databases.

7.2 Limitations of this review

This is a narrative rather than systematic review: no pre-registered protocol, no formal quality appraisal, and no quantitative synthesis. Source selection favoured recent official documents and highly cited scholarship, which may under-represent smaller empirical studies. The legal analysis reflects the position as of the most recent notifications and judgments consulted and will require updating as the Digital Personal Data Protection Rules enter their later phases and as the Supreme Court's supervision of the digital-arrest investigation proceeds. Finally, figures drawn from different administrative systems - NCRB registrations, CERT-In incidents, portal complaints - are not commensurable and are reported separately for that reason.

8. Challenges

Definitional and statutory. Section 78's gender specificity and narrow conduct element leave whole categories of victims and behaviours outside the stalking offence. Doxing, proxy stalking, persistent surveillance through shared accounts, and stalkerware deployment are addressed only obliquely, if at all.

The enforcement and adjudication gap. With fewer than two per cent of registered cybercrime cases ending in conviction, deterrence is negligible. Forensic laboratories face backlogs; evidence certification requirements are demanding; and specialised prosecutorial capacity is thin.

Federalism. Police and public order are state subjects. Central agencies coordinate but do not command, which is why the Standing Committee and the Supreme Court have both pressed for State Cybercrime Coordination Centres and why offences spanning several states default to jurisdictional disputes.

Cross-border attribution and recovery. With a large share of fraud originating from organised compounds abroad, investigation depends on cooperation instruments India has not yet fully joined, and recovery depends on freezing funds within minutes of transfer - a window current banking processes rarely meet.

Financial-system exploitation. Mule accounts, SIM-card misuse and cryptocurrency laundering form the operational backbone of the fraud economy. Each is a know-your-customer failure at scale rather than a cyber-technical failure.

Platform accountability versus expression. Compressing takedown windows to three hours, and to two hours for intimate imagery, protects victims where speed is everything, but creates strong incentives for over-removal. Reconciling this with *Shreya Singhal* (2015) is unresolved.

Privacy, surveillance and trust. Expanded state monitoring capacity, traceability requirements and suspect registries sit uneasily with *Puttaswamy* (2017). Victims of stalking need effective investigation; the same tools, unchecked, enable the surveillance that stalking consists of.

The literacy divide. Most new users are rural, frequently on shared devices, often in households where device access is itself mediated by others (IAMAI & Kantar, 2025; Sambasivan et al., 2018). Safety guidance premised on individual device ownership does not transfer to this setting.

Victim support. There is no systematic provision of psychological support, legal aid or protective orders for cyberstalking victims, despite consistent evidence of severe mental-health consequences (Stevens et al., 2021).

The gap between commitment and capability. A Tier 1 Global Cybersecurity Index score alongside a sub-two-per-cent conviction rate captures the central paradox: India has built institutions and passed statutes faster than it has built the enforcement capacity to operate them.

9. Recommendations

1. **Redraft the stalking offence** in gender-neutral terms, extend the conduct element to cover doxing, proxy pursuit and unauthorised device monitoring, and graduate penalties by persistence and demonstrated fear rather than by count of convictions.

2. **Regulate stalkerware explicitly**, criminalising the sale, distribution and non-consensual installation of covert monitoring applications, and require app stores to detect and delist them.

3. **Institute a national cyber-victimisation survey** on a recurring basis, disaggregated by gender, age, region and device-access pattern, to replace registration counts as the basis for policy design.

4. **Resource adjudication, not only investigation** - expand forensic laboratory capacity, designate cybercrime courts, and train prosecutors, since completed trials are currently the binding constraint.

5. **Mandate a short, hard deadline for fund freezing** in reported financial fraud, with supervisory penalties for banks and payment intermediaries that miss it, and publish lien and recovery rates by institution.

6. **Establish victim-support infrastructure**, integrating psychological support, legal aid and expedited content removal through a single point of contact rather than requiring victims to approach police, platforms and courts separately.

7. **Build safety education for shared-device and low-literacy contexts**, delivered in Indic languages and designed around household realities rather than individual ownership.

8. **Resolve the international cooperation question** on data access and mutual legal assistance, whether through accession to the United Nations Convention or through equivalent bilateral instruments.

9. **Fund independent evaluation** of the 2026 synthetic-media rules, the Digital Personal Data Protection Rules and the Cyber Commandos programme, so that the next decade's policy rests on measured outcomes rather than announced intentions.

Table 10 maps each challenge identified in Section 8 to the corresponding recommendation, the actor best placed to act, and a realistic horizon.

Table 10: *Challenges, recommended responses, responsible actors and horizon*

Challenge (Section 8)	Recommended response	Primary actor	Horizon
Gender-specific, conduct-limited stalking offence	Redraft s. 78 in gender-neutral terms; extend to doxing, proxy pursuit and device monitoring	Parliament; Ministry of Home Affairs	Medium
Stalkerware outside regulatory reach	Criminalise sale and non-consensual installation; require app-store delisting	Parliament; MeitY	Medium
No measure of actual prevalence	Institute a recurring national cyber-victimisation survey	NCRB; Ministry of Statistics	Medium
Enforcement and adjudication gap	Expand forensic capacity; designate cybercrime courts; train prosecutors	States; High Courts; MHA	Long
Slow recovery of defrauded funds	Hard deadline for fund freezing; publish lien and recovery rates by institution	RBI; banks; I4C	Short
Absence of victim support	Single point of contact combining psychological, legal and takedown assistance	States; I4C; MWCD	Short
Digital-literacy divide	Safety education designed for shared-device, low-literacy contexts	MeitY; states; civil society	Medium
Cross-border attribution and evidence	Resolve accession to the UN Convention or equivalent bilateral instruments	Ministry of External Affairs; MHA	Medium
Policy adopted without evaluation	Fund independent evaluation of the 2026 Rules, DPDP Rules and Cyber Commandos	MeitY; MHA; research councils	Short

10. Conclusion

India has constructed, in roughly a decade, a cyber governance architecture that compares favourably with most jurisdictions on paper: a national incident-response agency with statutory directions, a critical-infrastructure protection centre, a coordinating body for cybercrime with a citizen-facing portal and helpline, a data protection statute now operational through subordinate rules, a recodified criminal law, and the world's first binding provenance mandate

for synthetic media. The Tier 1 placement in the Global Cybersecurity Index 2024 reflects this institutional achievement accurately.

What it does not reflect is outcome. Reported cases have tripled in five years; reported financial losses tripled in a single year; and fewer than two in a hundred registered cases end in conviction. Cyberstalking occupies the least favourable position within this picture. It is defined narrowly and asymmetrically by gender, recorded in the low thousands against independent evidence suggesting a problem orders of magnitude larger, competes for investigative attention against high-value financial fraud, and is measured by no instrument capable of establishing its actual prevalence.

The binding constraints are therefore not primarily legislative. They are enforcement throughput, forensic and judicial capacity, the federal division of policing, the speed of financial recovery, the absence of victim-support infrastructure, and an evidence base too thin to support precise intervention. Closing the distance between India's declared commitment and its demonstrated capability - and generating the victimisation data that would allow anyone to measure that distance accurately - is the work of the next decade.

REFERENCES:

Alexy, E. M., Burgess, A. W., Baker, T., & Smoyak, S. A. (2005). Perceptions of cyberstalking among college students. *Brief Treatment and Crisis Intervention, 5*(3), 279–289. https://doi.org/10.1093/brief-treatment/mhi020

Anantam. (2026, July). *Cyber fraud complaints cross 12.7 lakh in six months, with over Rs 10,000 crore lost*. https://anantamias.com/current-affairs/cyber-fraud-complaints-12-7-lakh-six-months/

Anvar P.V. v. P.K. Basheer, (2014) 10 SCC 473 (India).

Arjun Panditrao Khotkar v. Kailash Kushanrao Gorantyal, (2020) 7 SCC 1 (India).

Bharatiya Nagarik Suraksha Sanhita, No. 46 of 2023, India Code (2023).

Bharatiya Nyaya Sanhita, No. 45 of 2023, India Code (2023).

Bharatiya Sakshya Adhiniyam, No. 47 of 2023, India Code (2023).

Bocij, P. (2004). *Cyberstalking: Harassment in the internet age and how to protect your family*. Praeger.

Bocij, P., & McFarlane, L. (2003). Cyberstalking: The technology of hate. *The Police Journal, 76*(3), 204–221. https://doi.org/10.1350/pojo.76.3.204.19442

Bossler, A. M., & Holt, T. J. (2009). On-line activities, guardianship, and malware infection: An examination of routine activities theory. *International Journal of Cyber Criminology, 3*(1), 400–420.

Basu, S., & Jones, R. (2007). Regulating cyberstalking. *Journal of Information, Law and Technology, 2007*(2), 1–30.

Chatterjee, R., Doerfler, P., Orgad, H., Havron, S., Palmer, J., Freed, D., Levy, K., Dell, N., McCoy, D., & Ristenpart, T. (2018). The spyware used in intimate partner violence. In *Proceedings of the 2018 IEEE Symposium on Security and Privacy* (pp. 441–458). IEEE. https://doi.org/10.1109/SP.2018.00061

Choi, K.-S. (2008). Computer crime victimization and integrated theory: An empirical assessment. *International Journal of Cyber Criminology, 2*(1), 308–333.

Citron, D. K. (2009). Cyber civil rights. *Boston University Law Review, 89*, 61–125.

Citron, D. K. (2014). *Hate crimes in cyberspace*. Harvard University Press.

Citron, D. K., & Franks, M. A. (2014). Criminalizing revenge porn. *Wake Forest Law Review, 49*, 345–391.

Cohen, L. E., & Felson, M. (1979). Social change and crime rate trends: A routine activity approach. *American Sociological Review, 44*(4), 588–608. https://doi.org/10.2307/2094589

Council of Europe. (2001). *Convention on Cybercrime* (European Treaty Series No. 185). https://www.coe.int/en/web/conventions/full-list?module=treaty-detail&treatynum=185

Criminal Law (Amendment) Act, No. 13 of 2013, India Code (2013).

Data Security Council of India. (2026). *Indian cyber security skilling landscape 2025–2026*. https://www.dsci.in/resource/content/indian-cyber-security-skilling-landscape-2025-2026

Data Security Council of India & Seqrite. (2024). *India cyber threat report 2025*. https://www.dsci.in/resource/content/india-cyber-threat-report-2025

Digital Personal Data Protection Act, No. 22 of 2023, India Code (2023).

Dreßing, H., Bailer, J., Anders, A., Wagner, H., & Gallas, C. (2014). Cyberstalking in a large sample of social network users: Prevalence, characteristics, and impact upon victims. *Cyberpsychology, Behavior, and Social Networking, 17*(2), 61–67. https://doi.org/10.1089/cyber.2012.0231

Finn, J. (2004). A survey of online harassment at a university campus. *Journal of Interpersonal Violence, 19*(4), 468–483. https://doi.org/10.1177/0886260503262083

Fissel, E. R., & Reyns, B. W. (2020). The aftermath of cyberstalking: School, work, social, and health costs of victimization. *American Journal of Criminal Justice, 45*(1), 70–87. https://doi.org/10.1007/s12103-019-09489-1

Freed, D., Palmer, J., Minchala, D., Levy, K., Ristenpart, T., & Dell, N. (2018). "A stalker's paradise": How intimate partner abusers exploit technology. In *Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems* (pp. 1–13). ACM. https://doi.org/10.1145/3173574.3174241

Gottfredson, M. R., & Hirschi, T. (1990). *A general theory of crime*. Stanford University Press.

Halder, D. (2013). Examining the scope of the Indecent Representation of Women (Prevention) Act, 1986, in the light of cyber victimisation of women in India. *National Law School Journal, 11*, 188–218.

Halder, D., & Jaishankar, K. (2009). Cyber socialising and victimisation of women. *Temida, 12*(3), 5–26. https://doi.org/10.2298/TEM0903005H

Halder, D., & Jaishankar, K. (2011). Cyber gender harassment and secondary victimization: A comparative analysis of the United States, the UK, and India. *Victims & Offenders, 6*(4), 386–398. https://doi.org/10.1080/15564886.2011.607402

Halder, D., & Jaishankar, K. (2012). *Cyber crime and the victimization of women: Laws, rights and regulations*. IGI Global.

Halder, D., & Jaishankar, K. (2013). Revenge porn by teens in the United States and India: A socio-legal analysis. *International Annals of Criminology, 51*(1–2), 85–111.

Halder, D., & Jaishankar, K. (2014). Online victimization of Andaman Jarawa tribal women: An analysis of the "human safari" YouTube videos (2012) and its effects. *British Journal of Criminology, 54*(4), 673–688. https://doi.org/10.1093/bjc/azu026

Halder, D., & Jaishankar, K. (2016). *Cyber crimes against women in India*. SAGE.

Henry, N., & Powell, A. (2018). Technology-facilitated sexual violence: A literature review of empirical research. *Trauma, Violence, & Abuse, 19*(2), 195–208. https://doi.org/10.1177/1524838016650189

Henson, B., Reyns, B. W., & Fisher, B. S. (2013). Fear of crime online? Examining the effect of risk, previous victimization, and exposure on fear of online interpersonal victimization.

Journal of Contemporary Criminal Justice, 29(4), 475–497. https://doi.org/10.1177/1043986213507403

Hinduja, S., & Patchin, J. W. (2015). *Bullying beyond the schoolyard: Preventing and responding to cyberbullying* (2nd ed.). Corwin.

IBM Security. (2024). *Cost of a data breach report 2024*. IBM Corporation.

Holt, T. J., & Bossler, A. M. (2014). An assessment of the current state of cybercrime scholarship. *Deviant Behavior, 35*(1), 20–40. https://doi.org/10.1080/01639625.2013.822209

Indian Computer Emergency Response Team. (2022). *Directions under sub-section (6) of section 70B of the Information Technology Act, 2000 relating to information security practices, procedure, prevention, response and reporting of cyber incidents*. Ministry of Electronics and Information Technology.

Indo-Asian News Service. (2026, January 3). *Indians lose over Rs 52,976 crore to cyber frauds over six years: Report*. https://ianslive.in/

Information Technology Act, No. 21 of 2000, India Code (2000).

Information Technology (Amendment) Act, No. 10 of 2009, India Code (2009).

Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021, G.S.R. 139(E) (India).

Indecent Representation of Women (Prevention) Act, No. 60 of 1986, India Code (1986).

Internet and Mobile Association of India & Kantar. (2025). *Internet in India report 2024*. IAMAI.

International Telecommunication Union. (2024). *Global Cybersecurity Index 2024*. ITU. https://www.itu.int/epublications/publication/global-cybersecurity-index-2024

Jaishankar, K. (2008). Space transition theory of cyber crimes. In F. Schmalleger & M. Pittaro (Eds.), *Crimes of the Internet* (pp. 283–301). Prentice Hall.

Jaishankar, K. (Ed.). (2011). *Cyber criminology: Exploring internet crimes and criminal behavior*. CRC Press.

K. S. Puttaswamy v. Union of India, (2017) 10 SCC 1 (India).

Kaspersky. (2024). *The state of stalkerware 2023*. Kaspersky. https://www.kaspersky.com/about/press-releases/2024_global-kaspersky-report-reveals-digital-violence-has-increased

Kaur, P., Dhir, A., Tandon, A., Alzeiby, E. A., & Abohassan, A. A. (2021). A systematic literature review on cyberstalking: An analysis of past achievements and future promises. *Technological Forecasting and Social Change, 163*, 120426. https://doi.org/10.1016/j.techfore.2020.120426

Kirwan, G., & Power, A. (2013). *Cybercrime: The psychology of online offenders*. Cambridge University Press.

Kowalski, R. M., Giumetti, G. W., Schroeder, A. N., & Lattanner, M. R. (2014). Bullying in the digital age: A critical review and meta-analysis of cyberbullying research among youth. *Psychological Bulletin, 140*(4), 1073–1137. https://doi.org/10.1037/a0035618

Kshetri, N. (2016). Cybercrime and cybersecurity in India: Causes, consequences and implications for the future. *Crime, Law and Social Change, 66*(3), 313–338. https://doi.org/10.1007/s10611-016-9629-3

Leukfeldt, E. R., & Yar, M. (2016). Applying routine activity theory to cybercrime: A theoretical and empirical analysis. *Deviant Behavior, 37*(3), 263–280. https://doi.org/10.1080/01639625.2015.1012409

Maple, C., Short, E., & Brown, A. (2011). *Cyberstalking in the United Kingdom: An analysis of the ECHO pilot survey*. University of Bedfordshire, National Centre for Cyberstalking Research.

Marcum, C. D., Higgins, G. E., & Ricketts, M. L. (2014). Juveniles and cyber stalking in the United States: An analysis of theoretical predictors of patterns of online perpetration. *International Journal of Cyber Criminology, 8*(1), 47–56.

Maurya, C., Muhammad, T., Das, A., Fathah, A., & Dhillon, P. (2023). The role of self-efficacy and parental communication in the association between cyber victimization and depression among adolescents and young adults: A structural equation model. *BMC Psychiatry, 23*, 337. https://doi.org/10.1186/s12888-023-04841-6

Maurya, C., Muhammad, T., Dhillon, P., & Maurya, P. (2022). The effects of cyberbullying victimization on depression and suicidal ideation among adolescents and young adults: A three year cohort study from India. *BMC Psychiatry, 22*, 599. https://doi.org/10.1186/s12888-022-04238-x

McAfee. (2022). *Cyberbullying in plain sight: A McAfee connected family report*. McAfee Corp.

Miftha, A., Conrad, M., & Gibson, M. (2019). Cyber stalking is a social evil: From the Indian women's perspective. In *Proceedings of the 17th International Conference e-Society 2019* (pp. 293–296). IADIS Press.

Miftha, A., Conrad, M., & Gibson, M. (2022). Cyberstalking in India: Challenges on the social side and the underlying contradictions. In *Proceedings of the International Conference e-Society 2022* (pp. 297–300). IADIS Press.

Ministry of Electronics and Information Technology. (2013). *National Cyber Security Policy 2013*. Government of India.

Ministry of Electronics and Information Technology. (2025a). *Lok Sabha unstarred question no. 4482: Cybersecurity incidents* (answered 20 August 2025). Government of India. https://eparlib.sansad.in/

Ministry of Electronics and Information Technology. (2025b). *Digital Personal Data Protection Rules, 2025*, G.S.R. 846(E), notified 13 November 2025. Government of India.

Ministry of Electronics and Information Technology. (2026). *Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Amendment Rules, 2026*, G.S.R. 120(E), notified 10 February 2026. Government of India.

Ministry of Home Affairs. (2025, July 22). *Reply to Lok Sabha question on losses due to cyber frauds*. Government of India.

National Critical Information Infrastructure Protection Centre. (2015). *Guidelines for the protection of national critical information infrastructure*. Government of India.

National Crime Records Bureau. (2025). *Crime in India 2023*. Ministry of Home Affairs, Government of India.

Ngo, F. T., & Paternoster, R. (2011). Cybercrime victimization: An examination of individual and situational level factors. *International Journal of Cyber Criminology, 5*(1), 773–793.

Nobles, M. R., Reyns, B. W., Fox, K. A., & Fisher, B. S. (2014). Protection against pursuit: A conceptual and empirical comparison of cyberstalking and stalking victimization among a national sample. *Justice Quarterly, 31*(6), 986–1014. https://doi.org/10.1080/07418825.2012.723030

Parliamentary Standing Committee on Home Affairs. (2025). *Two hundred fifty-fourth report: Cyber crime - Ramifications, protection and prevention*. Rajya Sabha Secretariat, Parliament of India.

Powell, A., & Henry, N. (2017). *Sexual violence in a digital age*. Palgrave Macmillan. https://doi.org/10.1057/978-1-137-58047-4

Pittaro, M. L. (2007). Cyber stalking: An analysis of online harassment and intimidation. *International Journal of Cyber Criminology, 1*(2), 180–197.

Press Information Bureau. (2024, September 10). *Union Home Minister launches Cyber Fraud Mitigation Centre, Samanvay platform, Cyber Commandos programme and Suspect Registry at the first foundation day of I4C* [Press release]. Ministry of Home Affairs, Government of India.

Press Information Bureau. (2026, January 23). *CERT-In handled over 29.44 lakh cyber incidents in 2025* [Press release]. Ministry of Electronics and Information Technology, Government of India.

PRS Legislative Research. (2025). *Standing committee report summary: Cyber crime - Ramifications, protection and prevention*. https://prsindia.org/policy/report-summaries/cyber-crime-ramifications-protection-and-prevention

Protection of Children from Sexual Offences Act, No. 32 of 2012, India Code (2012).

Reserve Bank of India. (2016). *Cyber security framework in banks* (DBS.CO/CSITE/BC.11/33.01.001/2015-16). RBI.

Reserve Bank of India. (2023). *Master direction on information technology governance, risk, controls and assurance practices*. RBI.

Reyns, B. W., Fisher, B. S., & Randa, R. (2018). Explaining cyberstalking victimization against college women using a multitheoretical approach: Self-control, opportunity, and control balance. *Crime & Delinquency, 64*(13), 1742–1764. https://doi.org/10.1177/0011128717753116

Reyns, B. W., Henson, B., & Fisher, B. S. (2011). Being pursued online: Applying cyberlifestyle–routine activities theory to cyberstalking victimization. *Criminal Justice and Behavior, 38*(11), 1149–1169. https://doi.org/10.1177/0093854811421448

Reyns, B. W., Henson, B., & Fisher, B. S. (2012). Stalking in the twilight zone: Extent of cyberstalking victimization and offending among college students. *Deviant Behavior, 33*(1), 1–25. https://doi.org/10.1080/01639625.2010.538364

Sambasivan, N., Batool, A., Ahmed, N., Matthews, T., Thomas, K., Gaytán-Lugo, L. S., Nemer, D., Bursztein, E., Churchill, E., & Consolvo, S. (2019). "They don't leave us alone anywhere we go": Gender and digital abuse in South Asia. In *Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems* (pp. 1–14). ACM. https://doi.org/10.1145/3290605.3300232

Sambasivan, N., Checkley, G., Batool, A., Ahmed, N., Nemer, D., Gaytán-Lugo, L. S., Matthews, T., Consolvo, S., & Churchill, E. (2018). "Privacy is not for me, it's for those rich women": Performative privacy practices on mobile phones by women in South Asia. In *Proceedings of the Fourteenth USENIX Conference on Usable Privacy and Security* (pp. 127–142). USENIX Association.

Securities and Exchange Board of India. (2024). *Cybersecurity and cyber resilience framework (CSCRF) for SEBI regulated entities*. SEBI.

Sheridan, L. P., & Grant, T. (2007). Is cyberstalking different? *Psychology, Crime & Law, 13*(6), 627–640. https://doi.org/10.1080/10683160701340528

Southworth, C., Finn, J., Dawson, S., Fraser, C., & Tucker, S. (2007). Intimate partner violence, technology, and stalking. *Violence Against Women, 13*(8), 842–856. https://doi.org/10.1177/1077801207302045

Short, E., Guppy, A., Hart, J. A., & Barnes, J. (2015). The impact of cyberstalking. *Studies in Media and Communication, 3*(2), 23–37. https://doi.org/10.11114/smc.v3i2.970

Shreya Singhal v. Union of India, (2015) 5 SCC 1 (India).

Smith, P. K., Mahdavi, J., Carvalho, M., Fisher, S., Russell, S., & Tippett, N. (2008). Cyberbullying: Its nature and impact in secondary school pupils. *Journal of Child Psychology and Psychiatry, 49*(4), 376–385. https://doi.org/10.1111/j.1469-7610.2007.01846.x

Spitzberg, B. H., & Hoobler, G. (2002). Cyberstalking and the technologies of interpersonal terrorism. *New Media & Society, 4*(1), 71–92. https://doi.org/10.1177/14614440222226271

Stevens, F., Nurse, J. R. C., & Arief, B. (2021). Cyber stalking, cyber harassment, and adult mental health: A systematic review. *Cyberpsychology, Behavior, and Social Networking, 24*(6), 367–376. https://doi.org/10.1089/cyber.2020.0253

Supreme Court of India. (2025a). *In Re: Victims of digital arrest related to forged documents* (Suo Motu Writ Petition, order dated 17 October 2025).

Supreme Court of India. (2025b). *In Re: Victims of digital arrest related to forged documents* (Suo Motu Writ Petition, order dated 1 December 2025).

Telecommunications Act, No. 44 of 2023, India Code (2023).

Tokunaga, R. S. (2010). Following you home from school: A critical review and synthesis of research on cyberbullying victimization. *Computers in Human Behavior, 26*(3), 277–287. https://doi.org/10.1016/j.chb.2009.11.014

United Nations Office on Drugs and Crime. (2025). *United Nations Convention against Cybercrime*. UNODC. https://www.unodc.org/unodc/en/cybercrime/convention/home.html

Verma, J. S., Seth, L., & Subramanium, G. (2013). *Report of the Committee on Amendments to Criminal Law*. Government of India.

Wall, D. S. (2007). *Cybercrime: The transformation of crime in the information age*. Polity Press.

Woodlock, D. (2017). The abuse of technology in domestic violence and stalking. *Violence Against Women, 23*(5), 584–602. https://doi.org/10.1177/1077801216646277

World Economic Forum. (2025). *Global cybersecurity outlook 2025*. World Economic Forum.

Yar, M. (2005). The novelty of "cybercrime": An assessment in light of routine activity theory. *European Journal of Criminology, 2*(4), 407–427. https://doi.org/10.1177/147737080556056