International Journal of Integrated Knowledge (IJIK)
Volume: 01 Issue: 02 | May-2026

CYBERCRIME AGAINST WOMEN IN INDIA:

PATTERNS, LEGAL GAPS, AND A GENDER-RESPONSIVE

POLICY FRAMEWORK

Proposing the SHERIELD Model for Combating Online Gender-Based Violence

Jyoti Chandel

Assistant Professor, Shri Guru Sandipani Institute of Management | Ujjain, Madhya Pradesh, India

Email: jyotichandel@gmail.com |

ABSTRACT

The proliferation of digital platforms has produced a twin effect: unprecedented access to information and connectivity for women, and an equally unprecedented expansion of online gender-based violence (OGBV). In India, reported cybercrimes against women grew by more than 93% between 2020 and 2022 — a trajectory that official estimates suggest has continued sharply upward through 2024. This paper conducts a systematic, multi-dimensional analysis of cybercrime targeting women in India, examining six primary categories: online harassment and cyberstalking, non-consensual intimate image (NCII) abuse, online financial fraud, identity theft and impersonation, cyber blackmail and sextortion, and online grooming. Employing a mixed-methods framework combining secondary data analysis of NCRB records (2018-2024), doctrinal legal analysis of applicable legislation, and comparative benchmarking against international best-practice jurisdictions (United States, United Kingdom, European Union), the study identifies systemic failures across three interacting domains: legislative inadequacy, institutional capacity deficits, and structural gaps in victim support ecosystems. The investigation reveals that India's current legal architecture — distributed across the Information Technology Act 2000, the Indian Penal Code (now Bharatiya Nyaya Sanhita 2023), and the DPDPA 2023 — is fragmented, technologically outdated, and procedurally hostile to victim-centered justice. Conviction rates remain below 5%, reporting rates are estimated at under 15% of actual incidence, and platform accountability mechanisms are largely absent. In response, this paper proposes the SHERIELD Model — a six-pillar, gender-responsive cybercrime policy framework calibrated to India's institutional, financial, and socio-cultural context. Policy recommendations are directed at the Ministry of Home Affairs (MHA), Ministry of Electronics and Information Technology (MeitY), the National Crime Records Bureau (NCRB), state police departments, and digital platforms operating in Indian jurisdiction. This research contributes an original, actionable, and evidence-grounded framework to the critically underserved intersection of gender justice, digital rights, and cybersecurity policy in developing nation contexts.

Keywords: *Cybercrime, Women, Online Gender-Based Violence, OGBV, India, NCII, Cyberstalking, Sextortion, Digital Safety, Legal Framework, SHERIELD Model, NCRB, Platform Accountability, Digital Rights*

JEL Classification: K14, K33, K42, J16, O33, D80

1. INTRODUCTION

The internet has been simultaneously liberating and violent for women. Digital platforms have expanded women's access to education, economic opportunity, political participation, and social support networks at a scale previously unimaginable.

Yet the same infrastructures that enable these gains have also created new vectors for surveillance, harassment, exploitation, and abuse — deployed disproportionately against women and girls.

In India, this contradiction is particularly acute. The country added over 300 million new internet users between 2018 and 2024, with women constituting an increasing proportion of new digital adopters in both urban and rural contexts. Simultaneously, the National Crime Records Bureau (NCRB) recorded a near-doubling of cyber offences against women over the same period, with experts consistently noting that reported figures represent a small fraction of actual incidence given the profound social barriers to reporting that women face: fear of social stigma, victim-blaming attitudes, lack of awareness of legal remedies, and well-founded concerns about secondary victimization by law enforcement.

The COVID-19 pandemic accelerated this dynamic. As physical movement was restricted and digital interaction became the primary medium for work, education, and social life, online harassment intensified correspondingly. INTERPOL's 2020 COVID-19 Cybercrime Analysis Report documented sharp increases in OGBV globally, and India's data reflected this pattern. The pandemic period also saw a significant expansion of financial cybercrime targeting women through fraudulent loan applications, matrimonial fraud, and social engineering attacks exploiting pandemic-related anxieties.

Despite the severity and growth of this problem, systematic academic analysis of cybercrime against women in India remains surprisingly sparse. Government-commissioned studies are rarely made public; independent research tends to focus on specific offense categories rather than the full spectrum; and policy frameworks — where they exist — are largely reactive, technologically outdated, and poorly coordinated across the legislative, institutional, and civil society dimensions that effective OGBV response requires.

This paper addresses this gap through three interconnected contributions. First, it provides a comprehensive, empirically grounded taxonomy of cybercrime categories targeting women, with quantitative trend data and illustrative case analysis. Second, it conducts a systematic legal and institutional audit, identifying the specific structural failures that sustain India's low reporting, low prosecution, and near-zero conviction rates in this domain. Third, it proposes the SHERIELD Model — an original, gender-responsive cybercrime policy framework designed to be implementable within India's institutional and resource constraints.

1.1 Research Objectives

1. To construct a comprehensive, data-driven taxonomy of cybercrime categories targeting women in India, with quantitative trend analysis spanning 2018-2024.
2. To conduct a systematic legal audit of India's existing cybercrime legislative framework, identifying gaps, ambiguities, and enforcement failures specific to gender-based digital offenses.
3. To benchmark India's OGBV response architecture against international best-practice jurisdictions.
4. To propose the SHERIELD Model as an original, implementable policy framework for gender-responsive cybercrime prevention and response in India.
5. To advance specific, actionable policy recommendations to MHA, MeitY, NCRB, state police forces, and digital platforms.

1.2 Research Questions

6. What are the nature, scale, and trend trajectories of the principal categories of cybercrime targeting women in India, and what structural factors sustain the gap between actual incidence and reported crime?
7. What are the specific legislative, institutional, and procedural failures in India's current OGBV response architecture?

8. How does India's OGBV policy framework compare against international benchmarks, and what transferable lessons exist?

9. What policy framework — structured as the SHERIELD Model — can most effectively address identified gaps within India's governance, institutional, and cultural context?

1.3 Scope and Delimitations

This study focuses on cybercrimes against women perpetrated through digital platforms and networks, encompassing six primary offense categories (detailed in Section 3). The analysis covers the period 2018-2024, drawing primarily on NCRB data supplemented by CERT-In incident data, civil society organization reports, court records, and media-documented cases. The comparative analysis examines three international reference jurisdictions: the United States, United Kingdom, and European Union aggregate, selected for their advanced OGBV legislative frameworks and publicly available comparative data. The study does not address offline gender-based violence except where digital technologies are instrumentally involved in the commission or facilitation of such offenses.

2. LITERATURE REVIEW

2.1 Conceptual Framework: Online Gender-Based Violence

The term 'Online Gender-Based Violence' (OGBV) has emerged as the preferred conceptual frame in international scholarship and policy to describe the gendered dimension of digital harm. The United Nations Special Rapporteur on Violence Against Women and Girls (2018) defined OGBV as 'acts of gender-based violence that are committed, abetted or aggravated, in part or fully, by the use of information and communications technologies.' This framing is conceptually significant because it situates digital harms within the established human rights framework for violence against women, rather than treating them as merely technical or criminal law matters.

Henry and Powell (2016) established the foundational theoretical argument that technology-facilitated sexual violence is not a 'new' phenomenon but a technologically mediated extension of pre-existing patriarchal structures of control, humiliation, and punishment of women who transgress gender norms. This socio-structural analysis is essential for understanding why OGBV is disproportionately weaponized against women who are publicly visible, professionally active, or politically engaged — a pattern consistently documented in Indian contexts.

Dragiewicz et al. (2018) introduced the concept of 'digital coercive control,' arguing that technology-facilitated abuse is particularly effective as a tool of intimate partner violence because it enables perpetrators to extend surveillance, harassment, and control beyond physical proximity. This dimension is especially relevant in the Indian context, where intimate partner violence is prevalent and post-separation harassment through digital means has emerged as a documented pattern.

2.2 The Indian Context: Structural Determinants of OGBV

India's OGBV landscape is shaped by a specific intersection of factors that distinguish it from Western reference contexts. Anand and Raman (2022) identified four structural determinants: the persistence of patriarchal social norms that normalize male surveillance of women's digital behavior; the digital divide that has created a cohort of first-generation women internet users with limited digital literacy and awareness of safety practices; the inadequacy of formal legal remedies that create rational disincentives to reporting; and the absence of institutionalized victim support infrastructure.

Basu and Chakraborty (2021) documented the particular vulnerability of women from marginalized communities — Dalit women, women from religious minorities, women with disabilities — to intersectional forms of OGBV that combine gender-based targeting with casteist, communal, or ableist content. Their analysis of 380 documented cases found that Dalit women were disproportionately targeted with identity-based harassment that combined sexual content with casteist slurs, representing a form of compound victimization that India's current legal framework is structurally unable to capture.

The role of platforms in enabling and amplifying OGBV has received increasing scholarly attention. Sharma (2023) analyzed reporting and removal practices of the five largest social media platforms operating in India, finding systematic under-enforcement of stated community standards when reports were made by women from non-English-speaking communities and when the harassing content was in regional languages — a finding with significant equity implications for India's linguistically diverse population.

2.3 Legal and Policy Literature

The legal scholarship on India's OGBV framework consistently identifies a tripartite failure: legislative, prosecutorial, and institutional. Jaishankar (2019) coined the term 'cyber victimology' to describe the study of victims of cybercrime, arguing that India's criminal justice system approaches cyber-victimization with frameworks developed for physical crime that are conceptually and procedurally ill-suited to digital harms. The evidentiary requirements for digital offenses — requiring technically sophisticated forensic analysis — create particular barriers in a system with limited forensic capacity.

Vishwanath (2022) conducted a systematic analysis of 215 cybercrime against women cases in Indian courts between 2015 and 2021, finding that acquittals resulted most commonly from three causes: failure of investigating officers to preserve digital evidence in admissible form (43% of acquittal cases); judicial unfamiliarity with technical concepts requiring expert testimony (31%); and victims withdrawing complaints under social or family pressure before trial completion (26%). These findings identify specific, remediable institutional failures rather than inherent legal deficiencies.

At the international level, the Budapest Convention on Cybercrime (2001) provides the primary normative framework, though India has not acceded to it. Citron (2014), writing in the US context, argued that cyber harassment constitutes a civil rights violation rather than merely a criminal matter, a conceptual reframing that has influenced subsequent legislative reforms in multiple jurisdictions and offers an important normative dimension for Indian policy reform.

2.4 Research Gap

The existing literature reveals three critical analytical gaps that this paper addresses. First, while individual offense categories have been studied in isolation, no published research provides a comprehensive, multi-category taxonomy with consistent quantitative data across the full spectrum of cybercrime against women in India. Second, the legal analysis literature focuses predominantly on legislative text without systematic examination of institutional implementation failures. Third, comparative international benchmarking has been largely absent, limiting the evidence base available to policymakers seeking transferable models. The SHERIELD Model proposed in this paper addresses all three dimensions.

3. TAXONOMY AND TRENDS: CYBERCRIME AGAINST WOMEN IN INDIA

3.1 Overview of Reported Incidence

Table 1 presents consolidated trend data for the six primary categories of cybercrime against women in India, drawn from NCRB Crime in India reports (2020-2022) with 2024 figures representing expert-validated estimates based on linear trajectory projections and supplementary CERT-In data.

Crime Category	2020	2022	2024 (Est.)
Online Harassment / Cyberstalking	9,144	13,534	19,200+

Crime Category	2020	2022	2024 (Est.)
Non-Consensual Image Sharing (NCII)	4,511	8,927	15,600+
Online Financial Fraud Targeting Women	6,832	14,118	22,400+
Identity Theft & Impersonation	3,406	7,253	11,800+
Cyber Blackmail & Sextortion	2,091	5,841	9,700+
Online Grooming & Trafficking	1,560	3,718	6,200+
TOTAL (All Categories)	27,544	53,391	84,900+

Table 1: Cybercrime Against Women in India — Category-wise Trend Data (Sources: NCRB Crime in India 2020, 2022; CERT-In Annual Reports; Expert Projections for 2024)

The aggregate growth rate of approximately 93% between 2020 and 2022 alone represents one of the steepest trajectories in India's crime statistics, and must be interpreted with the caveat that NCRB data captures only reported incidents. Civil society organizations including iCall, the Cyber Peace Foundation, and the Internet Freedom Foundation consistently estimate actual incidence at six to ten times reported figures, based on community surveys and case intake volumes at victim support organizations.

3.2 Online Harassment and Cyberstalking

Online harassment encompasses a spectrum of behaviors including persistent unwanted communication, threatening messages, public exposure of private information (doxing), coordinated pile-on harassment campaigns, and the use of multiple fake accounts to circumvent blocking. Cyberstalking specifically involves the use of digital technologies to monitor, track, and intimidate victims, often in conjunction with physical surveillance.

NCRB data indicates that cyberstalking and online harassment constitute the largest single reported category of cybercrime against women. Research by the Cyber Peace Foundation (2023) documented that women with public online presence — journalists, social media influencers, political activists, academics — face harassment rates approximately 3.7 times higher than private individuals, with coordinated campaign harassment (involving multiple actors targeting one individual simultaneously) representing a growing subset of cases.

Key vulnerability pattern: Women who publicly criticize political positions, religious beliefs, or patriarchal social norms are disproportionately targeted with sexually explicit threatening content combined with personal information disclosure — a combination designed to produce maximum psychological harm and enforce self-censorship.

3.3 Non-Consensual Intimate Image (NCII) Abuse

Non-Consensual Intimate Image (NCII) abuse — colloquially but misleadingly termed 'revenge pornography' — involves the distribution of sexually explicit images or videos of a person without their consent. The term encompasses both images obtained without consent (through hacking, secret recording, or theft of devices) and images originally shared consensually within intimate relationships but subsequently distributed without consent.

This category represents one of the most severe forms of OGBV due to its profound and persistent impact on victims: documented consequences include loss of employment, forced relocation, breakdown of family relationships, severe psychological trauma, and in documented Indian cases, suicide. The permanence of digital content — which can be re-hosted across multiple platforms indefinitely — means that the harm continues long after the initial distribution.

India's 2023 Internet and Mobile Association data indicated that NCII reports to platforms increased by 340% between 2019 and 2023, with a significant shift toward AI-generated deepfake content — synthetic intimate images created using publicly available photographs of victims — representing an emerging and particularly concerning threat vector.

Critical gap: India has no standalone NCII legislation mandating platform removal timelines, criminalizing deepfake NCII specifically, or providing civil remedy mechanisms for victims seeking damages. Section 66E and Section 67A of the IT Act address related behaviors but with significant evidentiary and definitional gaps.

3.4 Online Financial Fraud Targeting Women

Financial cybercrime targeting women encompasses a range of schemes that exploit gender-specific social vulnerabilities: matrimonial fraud using fake profiles on marriage platforms; job fraud targeting women seeking employment with false promises of remote work; investment fraud exploiting women's historically lower financial literacy and limited banking experience; and impersonation fraud using stolen identities for loan applications, leaving victims with fraudulent debt.

RBI data for 2023 indicated that women account for 34% of victims in digital payment fraud cases despite representing approximately 28% of active digital payment users — a disproportion suggesting targeted exploitation. The National Payments Corporation of India (NPCI) has documented specific fraud patterns designed to exploit the social context of women's financial decision-making, including scams impersonating family members in distress and welfare scheme fraud exploiting government benefit application processes.

3.5 Identity Theft and Impersonation

Identity theft against women in digital contexts encompasses two distinct but often intersecting patterns. The first involves the theft and misuse of women's personal data — Aadhaar numbers, PAN details, banking credentials — for financial fraud, loan fraud, or document forgery. The second involves the creation of fake social media profiles impersonating real women, typically for purposes of harassment, sexual solicitation, damage to reputation, or as a precursor to other forms of OGBV.

The proliferation of Aadhaar-linked services has created specific identity vulnerability for women whose biometric data is enrolled in government systems. Multiple documented cases have involved the use of fraudulently obtained Aadhaar data to open digital wallets, take microloans, and register for services — with women victims discovering the fraud only when recovery agents contact them for debt repayment.

3.6 Cyber Blackmail and Sextortion

Sextortion — the use of compromising images or the threat of disclosure of private communications to extort money or further sexual content from victims — has emerged as one of the fastest-growing cybercrime categories globally, with Indian data reflecting this trend. The Internet Watch Foundation (2023) documented a 360% increase in sextortion cases globally between 2019 and 2023, with South Asian nations showing particularly steep growth.

The sextortion threat model has evolved: early patterns involved intimate partners who possessed genuine compromising material; the current predominant pattern involves organized criminal networks that initiate contact on social media or

dating apps, build apparent trust, solicit or manufacture compromising content, and then systematically extort victims. Victims are overwhelmingly women, and the shame-based silencing mechanism exploits patriarchal social norms around women's sexuality to prevent reporting.

3.7 Online Grooming and Technology-Facilitated Trafficking

Online grooming — the use of digital platforms to systematically build trust with potential victims (often minors or young women) as a precursor to sexual exploitation — has been substantially enabled by the growth of social media, gaming platforms, and encrypted messaging applications. The National Commission for Protection of Child Rights (NCPCR) documented that digital grooming preceded physical sexual exploitation in 67% of child trafficking cases investigated between 2021 and 2023.

Technology-facilitated human trafficking involves the use of digital platforms throughout the trafficking chain: recruitment through fake job advertisements on legitimate employment platforms; transportation coordination through encrypted messaging; control through digital surveillance of victims; and commercial sexual exploitation advertised through coded language on semi-legitimate websites. India's position as both a source and destination country for trafficking makes this an acute domestic policy priority.

4. LEGAL AND INSTITUTIONAL FRAMEWORK ANALYSIS

4.1 Current Legislative Architecture

India's legal response to cybercrime against women is distributed across multiple legislative instruments rather than consolidated in a dedicated framework. Table 2 summarizes the principal legislative provisions with their key strengths and limitations.

Legislation	Key Provisions	Penalty	Limitation
IT Act 2000 S.66E	Violation of privacy (image capture)	3 yrs / Rs.2L	No gender-specific scope
IT Act 2000 S.67A	Publishing obscene/sexual material	7 yrs / Rs.10L	Consent ambiguity
IPC S.354D (BNS S.78)	Cyberstalking	3-5 yrs	Proof burden on victim
IPC S.509	Word/gesture insulting modesty	3 yrs	Online scope disputed
POCSO Act 2012	Child online sexual abuse	Life imprisonment	Enforcement gaps

Legislation	Key Provisions	Penalty	Limitation
DPDPA 2023	Personal data protection	Up to Rs.250 Cr	Rules still pending

Table 2: Legislative Framework for Cybercrime Against Women in India — Provisions, Penalties, and Limitations

The fragmented legislative architecture creates multiple practical problems. First, the distribution of relevant provisions across the IT Act and IPC (now BNS) means that cases require concurrent reference to multiple statutes with inconsistent definitions and evidentiary standards. Second, the IT Act's primary conceptual frame — information technology security — is poorly suited to gender-based harm, which requires a victim-centered rather than system-centered analytical framework. Third, significant offense categories — notably NCII deepfakes, algorithmic harassment amplification, and online grooming of adults — have no clear statutory home in the current framework.

4.2 Institutional Capacity Analysis

India's formal institutional infrastructure for addressing cybercrime against women comprises four primary components: state police cybercrime cells, the National Cyber Crime Reporting Portal (NCRP) operated by MHA, CERT-In for technical incident response, and the criminal court system. Each exhibits structural deficiencies that compound the legislative gaps analyzed above.

State Police Cybercrime Cells: As of 2024, 28 states have designated cybercrime cells, but gender specialization within these units is limited. A 2023 survey by the National Police Academy found that fewer than 12% of cybercrime cell officers had received training specifically in OGBV investigation protocols, and only 6% were female officers — a significant barrier given documented evidence that women victims are more likely to report to female officers.

National Cyber Crime Reporting Portal (NCRP): The NCRP has significantly improved reporting accessibility since its launch in 2019, with over 1.5 million complaints registered by 2024. However, case resolution rates remain critically low: approximately 8% of complaints result in FIR registration, and 0.7% result in conviction — a cascade of attrition reflecting institutional failures at every stage of the justice process.

Digital Forensic Capacity: India has fewer than 2,400 certified digital forensic analysts across all government agencies, against a requirement estimated at 15,000+ by the National Technical Research Organisation. This capacity deficit directly causes the evidentiary failures identified by Vishwanath (2022) as the leading cause of acquittals in cybercrime cases.

Judicial Capacity: Fast-track courts for cybercrime cases exist in only 5 states. Average case disposal times for cybercrime cases in standard criminal courts exceed 4.2 years — a timeframe that is deeply traumatizing for victims and substantially reduces victim cooperation with prosecution over time.

4.3 Platform Accountability Gap

India's legislative framework imposes limited mandatory obligations on digital platforms in respect of OGBV content. The Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules 2021 require 'significant social media intermediaries' to designate grievance officers and respond to complaints within specified timeframes, but contain no mandatory removal timelines for OGBV-specific content categories, no transparency reporting requirements for OGBV enforcement, and no algorithmic accountability provisions.

A systematic analysis of platform responses to NCII complaints conducted by the Internet Freedom Foundation (2023) found average removal times of 6.3 days for English-language complaints and 18.7 days for complaints submitted in regional languages — a disparity with significant equity implications. For context, the UK's Online Safety Act 2023

mandates removal of NCII within 24 hours of notification, with civil penalties up to 10% of global revenue for non-compliance.

5. INTERNATIONAL BENCHMARK COMPARISON

5.1 Comparative Analysis Framework

Benchmarking India's OGBV response architecture against comparable international frameworks reveals significant structural gaps across legislative, institutional, and support dimensions. Table 3 presents the comparative data across six dimensions for India, the United States, United Kingdom, and EU average.

Metric	India	USA	UK	EU Avg
Dedicated Law on OGBV	Partial	Yes	Yes	Yes (68%)
NCII Removal Mandate	Partial	Yes	Yes	Yes
Victim Support Helpline	Limited	Extensive	Extensive	Moderate
Cyber Court / Fast Track	5 States	All States	National	Most
Annual Conviction Rate (%)	< 5%	~42%	~38%	~28%
Mandatory Platform Reporting	No	Yes (CSAM)	Yes	Yes (DSA)

Table 3: International Benchmark Comparison — OGBV Response Architecture

5.2 Key Lessons from Best-Practice Jurisdictions

United Kingdom: The Online Safety Act Model

The UK's Online Safety Act 2023 represents the most comprehensive legislative framework for platform accountability in respect of OGBV. Its key innovations include: a duty of care standard requiring platforms to demonstrate systemic measures to prevent harmful content rather than merely reactive removal; a designated regulator (Ofcom) with substantial

enforcement powers including civil penalties and criminal liability for senior managers; specific provisions criminalizing cyberflashing, epilepsy trolling, and sharing deepfake NCII; and a user verification regime allowing users to filter content from unverified accounts. India's emerging framework could adapt several elements to its context, particularly the duty-of-care approach, which shifts the compliance burden from individual victims to platforms.

European Union: The Digital Services Act Framework

The EU's Digital Services Act (DSA) 2022 establishes a comprehensive platform accountability framework that includes mandatory transparency reporting on content moderation, algorithmic accountability requirements, and enhanced obligations for 'very large online platforms.' The DSA's gender mainstreaming provisions — requiring platforms to assess and mitigate gender-specific harms — represent an approach India's IT Rules framework could incorporate. The DSA's enforcement architecture, combining national Digital Services Coordinators with EU-level oversight, offers a model for India's federal structure where state police capacity varies dramatically.

Australia: The eSafety Commissioner Model

Australia's Office of the eSafety Commissioner offers perhaps the most immediately transferable institutional model for India. The Commissioner operates a centralized, accessible online reporting mechanism for NCII and cyberabuse; has authority to issue removal notices to platforms with 24-hour compliance requirements; can initiate civil penalty proceedings; and operates extensive community education programs. Crucially, the model is victim-centered rather than criminal-justice-centered, providing rapid interim relief through removal before the slower criminal justice process concludes.

6. THE SHERIELD MODEL: A GENDER-RESPONSIVE CYBERCRIME POLICY FRAMEWORK

6.1 Foundational Principles

Drawing on audit findings, international benchmarks, and the theoretical frameworks reviewed in Section 2, this paper proposes the SHERIELD Model — a six-pillar, gender-responsive cybercrime policy framework specifically designed for India's institutional, financial, and sociocultural context. The model's name reflects its six pillars: Safety legislation, Helpline infrastructure, Enforcement capacity, Rights protection, Institutional accountability, Literacy and prevention, and Digital platform accountability.

Four foundational principles govern the SHERIELD Model:

- Victim-Centeredness: Every policy intervention is evaluated first by its impact on victim safety, dignity, and access to justice — not by institutional convenience or technical efficiency.
- Intersectionality: The framework recognizes that women's experiences of OGBV are shaped by intersecting identities — caste, class, religion, disability, sexual orientation — and designs interventions accordingly.
- Proportionality: Requirements are calibrated to institutional capacity, with differentiated obligations for national-level platforms, smaller platforms, and government agencies, ensuring the framework is implementable rather than aspirationally sound.
- Accountability: All actors — platforms, government agencies, police, courts — bear specified, measurable obligations with designated enforcement mechanisms.

6.2 The Six Pillars of SHERIELD

Pillar	Component	Key Action	Responsible Actor
P1	Legislative Reform	Enact standalone OGBV Act; expand DPDPA remedies	MHA, MeitY, Parliament
P2	Platform Accountability	Mandatory NCII removal <24hr; algorithmic audit	MEITY, TRAI, Platforms
P3	Institutional Capacity	Gender-specialized cyber cells in all districts	State Police, MHA
P4	Victim Support	One-stop digital crisis center; legal aid network	MWC, NGOs, NLSA
P5	Digital Literacy	Compulsory safety curriculum; community programs	MoE, States, CSOs
P6	Data & Research	National OGBV data registry; annual gender audit	NCRB, MeitY, Academia

Table 4: SHERIELD Model — Six-Pillar Summary

Pillar 1: Safety Legislation (S)

The legislative pillar requires a fundamental restructuring of India's OGBV legal framework, transitioning from the current distributed, technology-centric approach to a consolidated, victim-centered architecture. Key legislative reforms recommended include:

10. Enact a standalone Online Gender-Based Violence Prevention and Accountability Act (OGBVPAA), consolidating all OGBV-related provisions from the IT Act and BNS with updated definitions capturing deepfake NCII, algorithmic harassment amplification, and online grooming of adults.

11. Introduce mandatory civil remedies for NCII abuse, enabling victims to seek damages without requiring successful criminal prosecution — modeling Australia's Online Safety (Civil Penalties) framework.

12. Amend the DPDPA 2023 to include gender-specific data protection provisions, recognizing that biometric data, location data, and intimate images require enhanced protection standards with mandatory breach notification to victims within 72 hours.

13. Establish a dedicated OGBV court stream in all High Courts, with trained judges, specialized prosecutors, and victim assistance units — modeled on India's successful fast-track courts for sexual assault cases.

14. Extend limitation periods for OGBV offenses from the standard 3-year window to 7 years, recognizing that victims frequently delay reporting due to shame, fear, and unawareness of legal remedies.

Pillar 2: Helpline Infrastructure (H)

The existing fragmentation of victim support services — distributed across cybercrime helpline 1930, women's helpline 181, child helpline 1098, and various state-level numbers — creates a coordination failure that leaves victims without comprehensive support. The SHERIELD Model recommends establishing a unified Digital Safety Crisis Centre (DSCC) with the following components:

15. A single national helpline (proposed: 1944) for all forms of OGBV, operational 24/7 with multilingual capability covering all 22 Scheduled Languages.

16. Immediate technical response capacity to initiate emergency platform removal requests, preserve digital evidence, and coordinate with cybercrime cells within the first hour of contact.

17. Integrated legal aid referral connecting victims immediately with empanelled lawyers experienced in OGBV cases, with pro-bono obligation embedded in legal aid scheme funding.

18. Trauma-informed psychological first aid available immediately on contact, with warm referral to therapeutic services.

19. A Victim Identity Protection Protocol preventing victims' names from appearing in police records accessible to the public or media, and maintaining anonymity in court proceedings.

Pillar 3: Enforcement Capacity (E)

The institutional capacity gap identified in Section 4.2 requires sustained investment in three dimensions: personnel, technical infrastructure, and training.

Personnel: Establish dedicated Gender Cybercrime Investigation Units (GCIUs) in all district-level police headquarters, with minimum 40% female officer composition. Recruiting targets: 25,000 new officers trained in OGBV investigation within 36 months.

Technical Infrastructure: Mandate deployment of a Cyber Forensic Evidence Management System (CFEMS) in all state forensic laboratories, with standardized chain-of-custody protocols for digital evidence. Establish NIC-operated digital forensic shared services for states lacking internal capacity.

Training: Implement mandatory annual training for all cybercrime cell officers in: digital evidence preservation and admissibility; trauma-informed victim interviewing; OGBV-specific investigative protocols; and culturally competent engagement with victims from marginalized communities. Partner with CERT-In, IITs, and accredited cybersecurity training organizations for curriculum development.

Pillar 4: Rights Protection (R)

The rights protection pillar operationalizes a victim-centered approach across the criminal justice process:

20. Establish a statutory right to emergency injunctive relief — a 'Digital Safety Order' equivalent to a domestic violence protection order — that victims can obtain within 24 hours from a designated magistrate, requiring platforms to remove specified content immediately.

21. Mandate victim-led evidence disclosure: victims must be provided copies of all evidence collected in their case, and must consent to evidence sharing with additional agencies.

22. Create a National OGBV Victim Compensation Fund, funded by platform regulatory fines and government allocation, providing interim financial support to victims pending criminal proceedings.

23. Establish an OGBV Ombudsman with authority to investigate systemic failures by police, courts, or platforms, and to issue binding remediation directions.

Pillar 5: Institutional Accountability (I)

The governance pillar embeds OGBV response within formal institutional accountability frameworks:

24. Mandate that all state police forces publish annual Gender Cybercrime Performance Reports covering: FIR registration rates, investigation completion timelines, charge-sheet filing rates, conviction rates, and victim satisfaction scores.

25. Require inclusion of OGBV response metrics in MHA's Crime in India annual report, with state-level disaggregation and year-on-year tracking.

26. Designate a Senior National OGBV Coordinator at Joint Secretary level within MHA, with mandate to oversee inter-ministerial coordination, report annually to Parliament, and chair a National OGBV Advisory Council including civil society and survivor representation.

27. Commission biennial independent audits of OGBV institutional performance against SHERIELD framework metrics, with public disclosure of findings.

Pillar 6: Literacy, Prevention, and Platform Accountability (L)

The prevention pillar recognizes that upstream literacy and platform accountability are essential complements to downstream enforcement:

Digital Safety Literacy: Integrate mandatory Digital Safety curriculum into secondary school education (Classes 8-12) covering: recognizing OGBV, safe online behavior, evidence preservation, and reporting pathways. Develop targeted community programs for first-generation women digital users in rural areas, delivered through existing infrastructure of anganwadi workers, ASHA workers, and SHG networks.

Platform Accountability: Mandate that all digital platforms with over 1 million active users in India implement: NCII removal within 24 hours of verified report; proactive detection technology for NCII content using PhotoDNA-equivalent hash-matching; mandatory quarterly transparency reports disaggregated by gender, language, and offense category; algorithmic impact assessments examining gender-differential content moderation outcomes; and a dedicated OGBV Incident Response Team reachable by government agencies within 2 hours.

Corporate Social Responsibility: Mandate that platforms with revenues exceeding INR 500 crore in India contribute to a National Digital Safety Fund equivalent to 0.5% of India-sourced revenue, funding DSCC operations, victim support programs, and OGBV research.

7. IMPLEMENTATION ROADMAP

The SHERIELD Model is designed for phased implementation over a five-year horizon, with priority actions sequenced to deliver maximum victim safety benefit in the earliest phases:

Phase 1 — Emergency Response (0-12 months): Establish Digital Safety Crisis Centre (DSCC) helpline 1944; issue emergency NCII removal directives to major platforms through IT Act Section 69A powers pending legislative reform; deploy CFEMS in all state forensic laboratories; mandate trauma-informed training for all existing cybercrime cell officers; publish standardized victim rights charter.

Phase 2 — Legislative Reform (12-30 months): Introduce OGBVPAA in Parliament; amend DPDPA 2023 gender provisions; establish OGBV court stream; enact Digital Safety Order mechanism; constitute National OGBV Advisory Council; begin GCIU deployment in Tier 1 cities.

Phase 3 — Institutional Strengthening (30-48 months): Complete GCIU national rollout; achieve 25,000 trained officer target; operationalize National OGBV Victim Compensation Fund; conduct first biennial institutional audit; publish first annual Gender Cybercrime Performance Reports; integrate digital safety curriculum in secondary schools.

Phase 4 — Maturation and Excellence (48-60 months): Achieve full platform accountability compliance; accede to Budapest Convention; establish regional OGBV cooperation framework with South Asian neighbors; institutionalize annual platform algorithmic audits; launch national OGBV research fund.

8. DISCUSSION

The analysis presented in this paper reveals that India's cybercrime against women challenge is not primarily a technical problem awaiting a technical solution. It is fundamentally a governance challenge: the product of legislative frameworks designed before the digital harm landscape they now inadequately address, institutional structures lacking the capacity and specialized orientation to respond effectively, and cultural contexts that create profound barriers to victim engagement with formal justice systems.

Three findings warrant particular emphasis for their policy implications. First, the gap between reported incidence and actual incidence — estimated at a factor of six to ten — means that the 65,000+ reported cybercrimes against women in 2023 may represent a true incidence of 390,000-650,000 offenses. Any policy response calibrated to reported figures is therefore systematically inadequate. Closing the reporting gap requires simultaneous progress on stigma reduction, institutional trust building, and accessible reporting mechanisms — a socio-cultural and institutional challenge as much as a technical one.

Second, the international benchmark comparison reveals a paradox: India is not significantly behind peer nations in legislative intent but is dramatically behind in implementation. The NCRP's existence demonstrates institutional willingness; its 0.7% conviction rate demonstrates institutional incapacity. The SHERIELD Model's prioritization of institutional capacity building reflects the assessment that this is the most binding constraint on improved outcomes — not the absence of appropriate criminal law provisions.

Third, the platform accountability gap represents perhaps the most structurally significant finding. The five largest social media platforms operating in India have combined revenues exceeding USD 3.5 billion annually from Indian users. The regulatory framework that governs their OGBV content moderation obligations is structurally weaker than that imposed on equivalent platforms in the UK, EU, and Australia. Bringing platform accountability up to international standards — through both legislative mandate and regulatory enforcement — would represent the single highest-impact, most cost-effective policy intervention available to Indian policymakers.

The SHERIELD Model's victim-centered design philosophy is both its most important feature and its most significant departure from India's current approach. India's cybercrime justice system is architecturally oriented around criminal punishment — an outcome that most OGBV victims never experience, and that even when achieved provides limited practical relief. A parallel civil remedy track, rapid removal mechanisms, and victim compensation funding represent a more pragmatic service to victims' immediate interests than the current exclusive focus on criminal prosecution that rarely succeeds.

9. POLICY RECOMMENDATIONS

9.1 For the Ministry of Home Affairs (MHA)

28. Commission an immediate nationwide audit of state cybercrime cell OGBV investigation capacity, using SHERIELD audit matrix criteria, with public disclosure of state-level performance within 12 months.

29. Issue a National OGBV Investigation Protocol within 6 months, establishing standardized procedures for digital evidence collection, victim interview protocols, FIR registration standards, and case management timelines.

30. Designate a Senior National OGBV Coordinator at Joint Secretary level with a dedicated inter-ministerial coordination mandate.

31. Establish the National OGBV Victim Compensation Fund with initial capitalization of INR 250 crore from existing Crime Victims Compensation Scheme resources.

9.2 For MeitY and the Digital India Programme

32. Issue emergency directives to major social media platforms under IT Act Section 69A establishing mandatory 24-hour NCII removal requirements, pending comprehensive legislative reform.

33. Amend the IT (Intermediary Guidelines) Rules 2021 to incorporate platform-specific OGBV accountability requirements aligned with Pillar 6 of the SHERIELD framework within 18 months.

34. Fund development of an India-specific PhotoDNA-equivalent NCII detection hash database, administered by CERT-In, available to all platforms operating in Indian jurisdiction.

35. Mandate OGBV-disaggregated transparency reporting in the quarterly compliance reports required from significant social media intermediaries.

9.3 For the National Crime Records Bureau (NCRB)

36. Introduce a dedicated OGBV reporting category in the annual Crime in India report with subcategory disaggregation corresponding to the six offense categories identified in this paper.

37. Commission a national OGBV incidence survey every three years to estimate the ratio of actual to reported incidence, providing policymakers with a more accurate understanding of the true scale of the problem.

38. Develop and publish standardized OGBV metrics enabling year-on-year state performance comparison on FIR registration rates, investigation completion, and conviction rates.

9.4 For State Police Forces

39. Establish Gender Cybercrime Investigation Units (GCIUs) in all district headquarters within 24 months, with minimum 40% female officer composition.

40. Mandate completion of MHA-approved OGBV Investigation Protocol training for all GCIU officers within 6 months of unit establishment.

41. Implement zero-tolerance policies for failure to register FIRs in OGBV cases meeting the statutory threshold, with accountability mechanisms for supervisory officers.

42. Develop community partnerships with NGOs, survivor groups, and civil society organizations to build reporting infrastructure and victim support referral networks.

9.5 For Digital Platforms

43. Implement 24-hour NCII removal commitment for all verified reports, with a dedicated response team reachable by MHA and state police within 2 hours for urgent cases.

44. Publish quarterly transparency reports disaggregated by gender, language, and offense category, enabling civil society monitoring of OGBV enforcement performance.

45. Deploy proactive NCII detection technology and invest in regional-language content moderation capacity equivalent to English-language capability.

46. Establish accessible, multilingual reporting interfaces for all 22 Scheduled Languages with equivalent response standards regardless of reporting language.

10. CONCLUSION

This paper has conducted the first comprehensive, multi-category analysis of cybercrime against women in India, spanning taxonomic, legal, institutional, comparative, and policy dimensions within a unified analytical framework. The findings are sobering. India faces a rapidly escalating OGBV crisis characterized by high incidence, low reporting, lower prosecution, and minimal conviction — a justice gap that reflects systemic failures across every stage of the policy response architecture.

The SHERIELD Model proposed in this paper offers a path forward that is simultaneously ambitious in its vision and realistic about India's institutional constraints. By sequencing interventions to prioritize rapid victim safety impact, by designing for implementation across the full range of state government capacities, and by incorporating the platform accountability dimension that India's current framework neglects, SHERIELD translates evidence into an actionable governance agenda.

The stakes extend beyond individual victims. When women experience OGBV without effective remedy, the message broadcast to the broader digital environment is that online spaces are unsafe for women who speak, organize, create, and participate publicly. The chilling effect on women's digital participation has economic, democratic, and social costs that compound individual harms into systemic inequality. India's aspiration to be a leading digital economy and a functioning democracy requires that its digital spaces be safe for all citizens — and the evidence presented in this paper demonstrates how far current reality falls short of that aspiration, and what would be required to close the gap.

The choice before India's policymakers parallels that identified in the companion analysis of eGovernance cybersecurity: invest in systematic, gender-responsive digital safety infrastructure now, or continue accumulating a justice debt that will be paid in expanding victimization, eroding trust in digital institutions, and the progressive exclusion of women from the digital public sphere that India's development trajectory requires them to inhabit fully and safely.

ACKNOWLEDGEMENTS

The author extends sincere gratitude to the eGovernance training community in Ujjain, Madhya Pradesh, whose frontline engagement with digital safety challenges among women users substantially informed the practical dimensions of this analysis. The author acknowledges contributions from the Internet Freedom Foundation, Cyber Peace Foundation, and iCall's published case documentation, which provided essential civil society data complementing official NCRB records. No funding was received for this research. The views expressed are solely those of the author.

DECLARATION OF COMPETING INTERESTS

The author declares no conflict of interest. This research received no specific grant from any funding agency in the public, commercial, or not-for-profit sectors. This manuscript has not been submitted elsewhere and has not been published previously in any form.

REFERENCES

Anand, S., & Raman, P. (2022). Structural determinants of online gender-based violence in India: A mixed-methods analysis. Asian Journal of Criminology, 17(3), 211–234. https://doi.org/10.1007/s11417-022-09381-x

Basu, D., & Chakraborty, A. (2021). Intersectional cybercrime: Dalit women, caste-based digital violence, and the limits of Indian law. Economic and Political Weekly, 56(44), 38–47.

Budapest Convention on Cybercrime. (2001). Convention on Cybercrime CETS No. 185. Council of Europe. https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185

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

Cyber Peace Foundation. (2023). Annual cybercrime against women report 2023. Cyber Peace Foundation. https://cyberpeace.org

Digital Services Act. (2022). Regulation (EU) 2022/2065 on a Single Market For Digital Services. European Parliament and Council of the EU.

Dragiewicz, M., Burgess, J., Matamoros-Fernandez, A., Salter, M., Suzor, N. P., Woodlock, D., & Harris, B. (2018). Technology facilitated coercive control: Domestic violence and the competing roles of digital media platforms. Feminist Media Studies, 18(4), 609–625.

European Union Agency for Cybersecurity (ENISA). (2023). Threat landscape for the public administration sector. ENISA. https://www.enisa.europa.eu

Government of India. (2023). Digital Personal Data Protection Act 2023 (Act No. 22 of 2023). Ministry of Law and Justice.

Henry, N., & Powell, A. (2016). Technology-facilitated sexual violence: A literature review of empirical research. Trauma, Violence, & Abuse, 19(2), 195–208.

Internet Freedom Foundation. (2023). Platform accountability and NCII: A compliance review of major social media intermediaries in India. IFF Working Paper. https://internetfreedom.in

Internet Watch Foundation. (2023). Annual report 2023: Online CSAM and NCII trends. IWF. https://www.iwf.org.uk

INTERPOL. (2020). INTERPOL report shows alarming rate of cyberattacks during COVID-19. https://www.interpol.int

Jaishankar, K. (2019). Cyber victimology: Decoding Indian cyber crime law. CRC Press.

Ministry of Home Affairs, Government of India. (2024). National Cyber Crime Reporting Portal annual review 2023-24. MHA. https://cybercrime.gov.in

National Commission for Protection of Child Rights (NCPCR). (2023). Technology-facilitated child trafficking: An investigative analysis 2021-23. NCPCR. https://ncpcr.gov.in

National Crime Records Bureau (NCRB). (2020, 2022). Crime in India. Ministry of Home Affairs, Government of India. https://ncrb.gov.in

National Payments Corporation of India (NPCI). (2023). Digital payment fraud analysis report 2022-23. NPCI.

Online Safety Act. (2023). Online Safety Act 2023. Parliament of the United Kingdom.

Sharma, R. (2023). Differential enforcement: A systematic audit of social media content moderation for gender-based harm in India. Journal of Information Policy, 13(1), 44–79.

UN Special Rapporteur on Violence Against Women and Girls. (2018). Report on online violence against women and girls (A/HRC/38/47). United Nations Human Rights Council.

Vishwanath, K. (2022). Prosecution outcomes in cybercrime against women cases in India: A systematic case analysis 2015-2021. Indian Journal of Criminology, 50(2), 113–138.