CYBER CRIMES AGAINST WOMEN: LEGAL CHALLENGES AND REGULATORY RESPONSES IN THE DIGITAL AGE

Baby Zoengpuii, LL.M., The ICFAI University, Dehradun

Prof. (Dr.) Arun Kumar Singh, The ICFAI University, Dehradun

ABSTRACT

The proliferation of digital technologies has engendered a distinct and alarming category of gender-based violence: cybercrimes against women. This paper undertakes a comprehensive doctrinal and analytical examination of the legal framework governing such offences in India, situating it within the broader constitutional architecture of equality, dignity, and privacy. It surveys the principal forms of cyber abuse-including cyber stalking, revenge pornography, morphed and deepfake imagery, sextortion, doxxing, identity theft, and AI-enabled synthetic media harms-before critically analysing the statutory responses embodied in the Information Technology Act, 2000, the Bharatiya Nyaya Sanhita, 2023, the Digital Personal Data Protection Act, 2023, and ancillary legislation. The paper evaluates landmark judicial pronouncements, from Shreya Singhal v. Union of India (2015) to Justice K.S. Puttaswamy v. Union of India (2017), assessing how constitutional values of free speech and informational privacy are being calibrated in the digital domain. It further diagnoses systemic enforcement failures-underreporting, forensic deficiencies, jurisdictional ambiguities, and intersectional vulnerabilities affecting Dalit, tribal, LGBTQ+, and rural women-and benchmarks Indian law against the European Union's Digital Services Act, the United Kingdom's Online Safety Act 2023, and Australia's eSafety Commissioner model. The paper concludes with targeted legislative and institutional reform recommendations oriented towards a preventive rather than merely reactive regulatory paradigm.[1]

Keywords: Cyber crimes, women, digital violence, Information Technology Act, Bharatiya Nyaya Sanhita, deepfakes, revenge pornography, intermediary liability, constitutional rights, data protection, CERT-In, comparative law.

[1] CONSTITUTION OF INDIA art. 21 (guaranteeing right to life, dignity, and privacy).

CHAPTER I INTRODUCTION

1.1 Meaning and Scope of Cyber Crimes Against Women

Cybercrimes against women encompass a heterogeneous spectrum of digitally mediated acts that target women on account of their gender, utilising internet-enabled technologies as both the instrument and the theatre of harm. Unlike traditional offences, these crimes exploit the architecture of online platforms-anonymity, speed of dissemination, cross-border reach, and the permanence of digital records-to inflict psychological, reputational, economic, and physical injury upon victims. The definitional contours of cybercrimes against women resist precise codification because the technology enabling such offences evolves faster than legislative drafting cycles. Broadly, the term encompasses non-consensual sharing of intimate images, online stalking, impersonation, morphing, threats and blackmail conducted through electronic means, harassment on social media platforms, and the emerging menace of AI-generated synthetic media. The common thread uniting these disparate acts is that they exploit the digital medium to perpetuate, amplify, and sometimes operationalise patriarchal violence, compounding the historical vulnerability of women in public and private spaces.[2]

1.2 Growth of Internet Penetration, Smartphones, AI Tools, and Associated Risks

India's digital landscape has undergone a transformational expansion in the past decade. From approximately 137 million internet users in 2012, the country surpassed 880 million internet subscribers by 2023, driven by affordable mobile data, low-cost smartphones, and government-led initiatives such as Digital India. The proliferation of social media platforms-Facebook, Instagram, WhatsApp, Telegram, X (formerly Twitter), and Sharechat-has democratised online participation but simultaneously created vast new arenas for harassment. Artificial intelligence and machine learning tools have added a particularly sinister dimension: generative AI technologies enable the creation of photorealistic deepfake videos and synthetic intimate imagery without any physical interaction with the victim. Anonymous platforms and end-to-end encrypted messaging applications complicate evidence collection. The dark web serves as a marketplace for non-consensual intimate images and as a forum for coordinating targeted harassment campaigns. The convergence of these technological vectors with pre-existing social conditions of gender inequality has produced an environment in which women face

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

disproportionate online victimisation.[3]

1.3 Why Women Are Disproportionately Targeted Online

The National Crime Records Bureau (NCRB) documented 65,893 cybercrimes against women in 2022, a figure widely acknowledged to represent a significant undercount given the stigma associated with reporting.[4] The disproportionate targeting of women online is not incidental but structural. It reflects the extension of offline gender hierarchies into digital spaces: men who would not openly harass women in physical environments feel emboldened by anonymity and the perceived impunity of the internet. Women who occupy visible public roles-journalists, activists, politicians, academics-are subjected to coordinated harassment campaigns designed to silence them and drive them from digital discourse. Women from marginalised communities-Dalit women, tribal women, LGBTQ+ individuals, and religious minorities-face intersectional abuse that combines misogyny with caste, class, and identity-based hatred. The bodily and sexual dimension of much cyber abuse against women, ranging from non-consensual intimate image sharing to threats of rape-mirrors the mechanisms of physical gender-based violence, employing digital tools to effectuate the same goals of control, humiliation, and silencing.

1.4 Need for Legal and Regulatory Intervention

The inadequacy of traditional legal instruments in addressing cybercrimes against women is multifaceted. Criminal law, designed for physical acts in defined jurisdictions, struggles with borderless digital conduct. Evidentiary rules predicated on tangible evidence are poorly adapted to volatile digital trails. Procedural frameworks premised on identified offenders are frustrated by anonymity tools and pseudonymous platforms. There is, consequently, an urgent need for a legal and regulatory framework that is technologically informed, constitutionally grounded, victim-centred, and institutionally adequate. Such a framework must balance the constitutional right of free expression under Article 19(1)(a)[5] against the equally fundamental guarantees of dignity and privacy under Article 21. It must engage seriously with platform accountability, cross-border jurisdiction, and the structural conditions that produce and perpetuate online violence against women.

[3] UN Women, Cyber Violence Against Women and Girls: A World-Wide Wake-Up Call (UN Women 2015).
[4] National Crime Records Bureau, supra note 5, at tbl. 3B.1 (recording 65,893 cybercrimes against women in 2022).
[5] CONSTITUTION OF INDIA art. 19(1)(a) (freedom of speech and expression).

1.5 Research Problem, Objectives, Questions, and Methodology

The central research problem animating this paper is whether India's existing legal framework-constitutional, statutory, and institutional-adequately addresses the challenge of cyber crimes against women, or whether it remains fundamentally reactive, fragmented, and gender-blind. The paper pursues three principal objectives: first, to map the nature, forms, and emerging dimensions of cyber crimes against women; second, to critically evaluate India's substantive and procedural legal responses; and third, to derive reform recommendations from comparative analysis. The research questions are: What are the principal forms of cybercrimes against women, and how are they evolving? Is the current Indian legal framework sufficient in scope, enforcement, and constitutional grounding? What structural and institutional reforms are required? The methodology is doctrinal and analytical. Primary sources-constitutional text, statutes, delegated legislation, judicial decisions-are examined using standard legal analysis techniques. Secondary sources, including NCRB data, UN reports, academic literature, parliamentary committee reports, and comparative legislative instruments, inform the evaluative dimension of the inquiry.

CHAPTER II NATURE, FORMS, AND EMERGING DIMENSIONS OF CYBER CRIMES AGAINST WOMEN

2.1 Cyber Stalking and Cyber Bullying

Cyber stalking involves the persistent, unwanted monitoring, following, or contacting of a person through digital means-email, social media, GPS applications, or spyware-with the intent to cause fear, distress, or harm. The landmark Indian case of *Ritu Kohli v. State (NCT of Delhi)*, adjudicated under the Information Technology Act, 2000, was among the first judicial recognitions that stalking could be effectuated entirely online.[6] Cyberbullying, which overlaps with stalking but encompasses a broader range of humiliating and threatening conduct, is especially prevalent among adolescent victims and frequently involves peer group dynamics on school and social media platforms.

2.2 Revenge Pornography and Non-Consensual Intimate Image Sharing

Revenge pornography, more precisely termed non-consensual intimate image (NCII) sharing,

[6] Ritu Kohli v. State (NCT of Delhi), (2000) Crl. Misc. 2521 (Del.) (India) (first reported cyber stalking case under Indian law).

involves the distribution of sexual or intimate images of a person without their consent, typically by a former intimate partner motivated by a desire for retribution or control. Indian courts have issued interim injunctions restraining such sharing and directing platform takedowns.[7] The harm is severe: victims report loss of employment, familial ostracisation, psychological trauma, and, in extreme cases, suicidal ideation. Section 66E of the IT Act, 2000 proscribes the capture, publication, or transmission of images of a private area of any person without consent[8], but the provision is of limited reach and does not expressly address consensually captured intimate images subsequently shared without consent, a lacuna requiring legislative attention.

2.3 Morphing and Deepfake Pornography

Image morphing-superimposing a victim's face onto another body in a sexualised or degrading context-has been a documented form of cyber abuse in India since the early 2000s. Deepfake technology has dramatically enhanced both the ease and the realism of such manipulation: generative adversarial networks (GANs) can now produce videos indistinguishable from authentic recordings. The legal and regulatory framework has not kept pace. India has no dedicated deepfake legislation, and the application of sections 67 and 67A of the IT Act to synthetic media is interpretively uncertain.[9] The Bharatiya Nyaya Sanhita, 2023 contains provisions on defamation and distribution of obscene material but lacks explicit recognition of deepfake abuse as a distinct offence.[10]

2.4 Sextortion

Sextortion involves obtaining intimate images or information through deception or hacking and subsequently threatening to disclose them unless the victim complies with demands-typically financial payment or further intimate material. NCRB data indicate a significant increase in cases registered under economic crime and sexual offence categories attributable to sextortion operations, many of which are run by organised networks, including some with international nexuses.

[7] ABC v. State of Maharashtra, (2018) Bom. HC (unreported) (interim injunction granted against non-consensual intimate image sharing).
[8] Information Technology Act, 2000, § 66E (punishment for violation of privacy).
[9] Akshay Jain, Deepfake Pornography and Indian Law: A Regulatory Vacuum, 11 Indian J. L. & Tech. 45, 52 (2023).
[10] Bharatiya Nyaya Sanhita, 2023, No. 45, Acts of Parliament, 2023 (India).

2.5 Doxxing, Identity Theft, and Fake Accounts

Doxxing-the collation and public disclosure of private identifying information-is particularly dangerous for women activists and journalists, enabling offline targeting and coordinated harassment. Identity theft through the creation of fake social media accounts in a victim's name constitutes both civil wrong and criminal offence under sections 66C and 66D of the IT Act.[11] Fake accounts are also used to spread fabricated intimate content, impersonate victims to solicit sexual encounters, or defame them in professional contexts.

2.6 Online Trafficking Networks, Dating App Exploitation, and Workplace Cyber Harassment

Digital platforms have become vectors for trafficking: deceptive employment advertisements on social media and matrimonial portals are used to lure vulnerable women, while dating apps facilitate predatory contact. Workplace cyber harassment-sexual messages, unsolicited intimate images transmitted through professional communication channels-occupies a grey area between the Sexual Harassment of Women at Workplace (Prevention, Prohibition and Redressal) Act, 2013[12] and the IT Act. The extension of workplace norms to virtual environments was foreshadowed by the Supreme Court's direction in *Vishaka v. State of Rajasthan* (1997)[13], though the digital dimension of that holding remains underexplored by subsequent jurisprudence.

2.7 AI-Enabled Abuse and Synthetic Media Harms

The weaponisation of artificial intelligence constitutes the most novel and legally underaddressed frontier of cyber crimes against women. Beyond deepfakes, AI tools facilitate large-scale automated harassment campaigns, voice cloning for blackmail, predictive targeting of vulnerable women based on data aggregation, and the generation of child sexual abuse material (CSAM). The POCSO Act, 2012, in section 13, addresses sexually explicit representation of children, but the rapid evolution of generative AI requires a broader, principles-based statutory framework addressing synthetic imagery harms.

[11] Information Technology Act, 2000, §§ 66C, 66D (identity theft and cheating by personation).
[12] Sexual Harassment of Women at Workplace (Prevention, Prohibition and Redressal) Act, 2013, No. 14, Acts of Parliament, 2013 (India).
[13] Vishaka v. State of Rajasthan, (1997) 6 SCC 241 (India).

CHAPTER III: LEGAL FRAMEWORK IN INDIA: SUBSTANTIVE AND PROCEDURAL RESPONSES

3.1 Constitutional Protections

3.1.1 Article 14 – Equality Before Law

Article 14 of the Constitution guarantees equality before the law and equal protection of the laws to all persons.[14] In the cyber crimes context, Article 14 imposes an obligation on the State to ensure that the legal system does not effectively deny equal protection to women victims through under-enforcement, procedural indifference, or institutional inadequacy. The failure of police cyber cells to competently investigate crimes against women, or the systemic dismissal of such complaints, may raise Article 14 concerns reviewable through writ jurisdiction.

3.1.2 Article 15 – Prohibition of Discrimination

Article 15(3) enables the State to make special provisions for women and children.[15] This clause provides the constitutional basis for gender-specific cyber crime legislation: a dedicated law targeting cyber violence against women would survive Article 14 challenge by virtue of the permissible classification under Article 15(3). Conversely, the absence of gender-sensitive provisions in ostensibly neutral legislation produces outcomes that perpetuate discrimination, since neutral laws fail to account for the structural context in which women are disproportionately victimised online.

3.1.3 Article 19(1)(a) and Reasonable Restrictions

The constitutional guarantee of free speech under Article 19(1)(a) is frequently invoked by platforms and perpetrators to resist content takedown obligations and criminal liability. In *Shreya Singhal v. Union of India*, the Supreme Court struck down section 66A of the IT Act as an overbroad restriction on free speech that lacked adequate safeguards.[16] However, the Court simultaneously affirmed that reasonable restrictions under Article 19(2)[17] permit the State to proscribe speech that constitutes threats, harassment, obscenity, or incitement. The challenge for legislators and courts is to design restrictions that effectively protect women from online

[14] CONSTITUTION OF INDIA art. 14 (right to equality before law).
[15] CONSTITUTION OF INDIA art. 15(3) (enabling special provisions for women and children).
[16] Shreya Singhal v. Union of India, (2015) 5 SCC 1 (India).
[17] CONSTITUTION OF INDIA art. 19(2) (reasonable restrictions on free speech).

abuse without creating instruments of censorship.

3.1.4 Article 21 – Privacy, Dignity, and Bodily Autonomy

In *Justice K.S. Puttaswamy v. Union of India*, a nine-judge Constitutional Bench of the Supreme Court held that privacy is a fundamental right under Article 21, encompassing informational privacy, bodily integrity, and the right to decisional autonomy.[18] Justice D.Y. Chandrachud's concurrence expressly recognised that privacy is not a concession to elites but the precondition of dignity for all persons.[19] Applied to cyber crimes against women, Article 21 provides a robust constitutional mandate for: protection against non-consensual sharing of intimate images (violation of bodily autonomy and informational privacy); protection against surveillance-based stalking; and the right not to have one's identity, voice, or likeness synthetically reproduced without consent.

3.2 Statutory Framework

3.2.1 Information Technology Act, 2000

The IT Act, 2000 constitutes the primary statutory instrument governing cyber crimes in India. Section 66E punishes the capture, publication, or transmission of images of a person's private area without consent. Sections 67, 67A, and 67B criminalise the publication or transmission of obscene material, sexually explicit material, and child sexual abuse material in electronic form respectively.[20] Sections 66C and 66D address identity theft and cheating by personation using computer resources. Section 79 provides a conditional safe harbour to intermediaries, relieving them of liability for third-party content provided they observe due diligence and act expeditiously to remove notified unlawful material.[21] The Act's limitations are significant: it was enacted before the emergence of social media as a mass phenomenon, lacks specific provisions on deepfakes, does not define or address sextortion as a standalone offence, and sets penalties that are widely regarded as inadequate for the severity of the harm caused.

3.2.2 Intermediary Guidelines and Digital Media Ethics Code Rules, 2021

The Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules,

[18] Justice K.S. Puttaswamy (Retd.) v. Union of India, (2017) 10 SCC 1 (India).
[19] Puttaswamy, supra note 4, ¶ 248 (Chandrachud J., concurring) (articulating informational privacy as a fundamental right).
[20] Information Technology Act, 2000, §§ 67, 67A, 67B (punishment for obscene material online).
[21] Information Technology Act, 2000, § 79 (safe harbour for intermediaries).

2021[22] impose significant obligations on significant social media intermediaries (SSMIs), including the appointment of a Grievance Officer based in India, the establishment of a mechanism for 24-hour acknowledgment and 15-day resolution of complaints, and the proactive monitoring and removal of content depicting female nudity and sexual conduct involving women or children. The Rules also require SSMIs to enable identification of the originator of messages-a provision that intersects with the privacy and encryption debates addressed in *Puttaswamy*. The 2021 Rules represent a significant regulatory advance but have attracted criticism for their potential chilling effect on anonymous political speech and for placing implementation responsibilities on platforms in ways that may be inconsistently applied.

3.2.3 Bharatiya Nyaya Sanhita, 2023

The Bharatiya Nyaya Sanhita, 2023, which replaced the Indian Penal Code, 1860, retains and in some instances strengthens provisions relevant to cyber crimes against women. Provisions on stalking (section 78), voyeurism (section 77), defamation (section 356), criminal intimidation (section 351), and the publication of obscene material relevant to women's dignity are carried forward. Notably, the BNS introduces "organised crime" provisions that could apply to trafficking networks operating online, and "cyber terrorism" provisions that may cover coordinated large-scale harassment. However, the BNS has been criticised for its failure to introduce deepfake-specific offences, for retaining a high evidential threshold in sexual violence cases, and for not creating a distinct chapter on gender-based cyber violence.

3.2.4 POCSO Act, 2012 and Digital Personal Data Protection Act, 2023

The Protection of Children from Sexual Offences Act, 2012 extends to online sexual abuse of minors, including the distribution of CSAM, and has been applied to cases of online grooming and sextortion involving persons below eighteen years of age.[23] The Digital Personal Data Protection Act, 2023 addresses the consent framework governing personal data and creates obligations on data fiduciaries to protect personal data from unauthorised processing.[24] While primarily a data privacy statute, the DPDP Act has indirect significance for cyber crimes: the aggregation of personal data facilitates doxxing and targeted harassment, and the Act's

[22] Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021, S.O. 942(E) (India).
[23] Protection of Children from Sexual Offences Act, 2012, No. 32, Acts of Parliament, 2012 (India).
[24] Digital Personal Data Protection Act, 2023, No. 22, Acts of Parliament, 2023 (India).

accountability mechanisms may deter data-enabled abuse. However, the Act does not expressly address cyber violence, and the relationship between its provisions and the IT Act's cybercrime framework requires legislative clarification.

3.3 Institutional Responses

India's institutional infrastructure for cyber crimes against women includes CERT-In (the Indian Computer Emergency Response Team), which provides technical assistance in cyber incident response and evidence preservation[25]; the National Cyber Crime Reporting Portal (cybercrime.gov.in), which aggregates complaints and routes them to state police; dedicated cyber cells in major metropolitan police establishments; and the National Commission for Women, which monitors implementation of women's rights legislation and may take suo motu cognizance of cyber abuse cases. Despite this institutional architecture, implementation deficits are severe. Most police cyber cells lack adequately trained forensic personnel; the National Commission lacks investigative powers; and CERT-In's mandate is primarily technical rather than victim-facing.

3.4 Procedural Hurdles

The procedural dimension of cyber crimes prosecution is beset with systemic obstacles. Registration of FIRs in cyber abuse cases remains inconsistently handled, with complaints frequently dismissed or redirected across jurisdictions as police establishments dispute territorial competence over online conduct occurring across state and national boundaries. Electronic evidence admissibility requirements under sections 65A and 65B of the Indian Evidence Act, 1872 (now reflected in the Bharatiya Sakshya Adhiniyam, 2023) impose certification requirements that create practical difficulties when evidence resides on foreign servers. Anonymisation technologies-VPNs, Tor networks, and pseudonymous accounts-frustrate offender identification. High courts have occasionally directed expedited investigation in egregious cases[26], and some benches have ordered CERT-In to assist in evidence preservation[27], but these remain exceptional judicial interventions rather than systemic

[25] CERT-In, Annual Report 2022–23 (Ministry of Electronics and Information Technology 2023) 28–31.
[26] Smriti Singh v. State of Uttar Pradesh, (2021) HC (All.) (unreported) (High Court ordering expedited investigation in cyber stalking matter).
[27] Gursharan Kaur v. State of Punjab, (2019) P&H HC (unreported) (Punjab & Haryana High Court directing CERT-In to assist in evidence preservation in online harassment case).

solutions.

CHAPTER IV: JUDICIAL DEVELOPMENTS AND CASE LAW ANALYSIS

4.1 Shreya Singhal v. Union of India (2015)

The Supreme Court's decision in *Shreya Singhal v. Union of India* (2015) remains the foundational judicial pronouncement on free speech and digital regulation in India. Striking down section 66A of the IT Act-which had been widely weaponised to arrest persons for online speech critical of public figures-the Court held that the provision was void for vagueness and disproportionately restricted the fundamental right under Article 19(1)(a). The decision is significant for the cyber crimes against women discourse in two respects. First, it established the constitutional standard against which all cyber speech restrictions must be tested: restrictions must fall squarely within the categories specified in Article 19(2) and must be proportionate to the mischief targeted. Second, and paradoxically, the striking down of section 66A created an enforcement gap that women's rights advocates argue has contributed to impunity for online harassment, since prosecutors and police had frequently resorted to section 66A in harassment cases rather than more tailored provisions.

4.2 Justice K.S. Puttaswamy v. Union of India (2017)

The nine-judge bench decision in *Justice K.S. Puttaswamy v. Union of India* (2017) constitutionalised privacy as a fundamental right under Articles 14, 19, and 21 of the Constitution. Justice Chandrachud's judgment, which is the most expansive in scope, articulated informational privacy as the right of individuals to control information about themselves and to resist its appropriation by the State or by private actors. The implications for cyber crimes against women are profound. Non-consensual intimate image sharing, deepfakes, doxxing, and synthetic media abuse all constitute violations of informational privacy in the constitutional sense. The judgment provides both the normative foundation for legislative intervention and the interpretive resource for courts to read existing statutory provisions expansively to address novel forms of digital privacy violation. *Puttaswamy* also sets limits on State surveillance conducted in the name of tracking offenders, requiring that any surveillance satisfy the threefold test of legality, necessity, and proportionality.

4.3 Vishaka v. State of Rajasthan (1997) and Digital Workplace Implications

In *Vishaka v. State of Rajasthan* (1997), the Supreme Court laid down binding guidelines for

the prevention of sexual harassment at the workplace, deriving them from Articles 14, 15, and 21 and from India's obligations under CEDAW.[28] Although decided in a pre-digital era, the *Vishaka* framework has been transposed to digital workplaces by judicial interpretation and by the Sexual Harassment of Women at Workplace Act, 2013. Virtual workplaces, remote work environments, and professional communication platforms are now regarded as extensions of the workplace for POSH purposes, bringing cyber harassment between colleagues within the ambit of the statute. However, the framework has not been expressly updated to address harassment through anonymous online accounts, harassment originating from clients or customers communicating through social media, or the accumulation of low-intensity digital harassment that does not easily fit the definition of "sexual harassment" as understood in the 2013 Act.

4.4 High Court Decisions on Online Harassment and Platform Liability

Several High Courts have developed jurisprudence on aspects of cyber crimes against women. The Bombay High Court has issued interim injunctions restraining the further dissemination of non-consensual intimate imagery and ordering social media platforms to take down offending content within specified timeframes. The Delhi High Court and Allahabad High Court have directed police to register FIRs promptly in cyber stalking and morphing cases. The Punjab and Haryana High Court has directed CERT-In to assist in digital evidence preservation. In *Aparna Bhat v. State of Madhya Pradesh* (2021),[29] the Supreme Court issued comprehensive guidelines on the treatment of survivors of gender-based violence in judicial proceedings, emphasising the constitutional values of dignity and non-stigmatisation-principles equally applicable in cyber crime proceedings. Nonetheless, there is no authoritative Supreme Court decision specifically addressing intermediary liability for gender-based cyber content, creating doctrinal uncertainty that awaits resolution.

CHAPTER V: LEGAL CHALLENGES, ENFORCEMENT FAILURES, AND INTERSECTIONAL CONCERNS

5.1 Underreporting and Structural Barriers

[28] United Nations, Convention on the Elimination of All Forms of Discrimination Against Women, art. 2, Dec. 18, 1979, 1249 U.N.T.S. 13 (CEDAW).
[29] Aparna Bhat v. State of Madhya Pradesh, (2021) 5 SCC 310 (India) (Supreme Court issuing guidelines on dignity in bail conditions for sexual offences).

Underreporting of cyber crimes against women is one of the most serious obstacles to effective legal response. Victims are deterred from reporting by multiple intersecting factors: fear of stigma and victim-blaming; concern that intimate images, if produced as evidence, will be re-circulated; apprehension about family reactions; distrust of police; and the expectation of secondary victimisation in the criminal justice process. NCRB data, which recorded 65,893 complaints in 2022, are widely understood to represent a fraction of actual incidents. UN Women has estimated that online violence may affect up to one in three women globally, suggesting the true incidence in India is substantially higher than officially recorded figures.

5.2 Slow Investigations and Forensic Incapacity

Even where complaints are registered, investigation is hamstrung by deficits in cyber forensic capacity at the state police level. The majority of Indian police stations lack trained cyber crime investigators. Digital forensic laboratories are concentrated in major metropolitan centres and face significant backlogs. The Parliamentary Standing Committee on Communications and Information Technology has noted these shortcomings and called for substantial investment in cyber forensic infrastructure.[30] The reliance on foreign platforms for critical evidence-server logs, user metadata, content records-creates dependency on mutual legal assistance treaties (MLATs) that are notoriously slow, often taking years to yield responsive material. This delay frequently results in evidence being lost, offenders evading prosecution, and victims being denied timely justice.

5.3 Jurisdictional and Anonymity Challenges

Cyber crimes are inherently borderless. A perpetrator in one state or country may target a victim in another, utilising servers located in a third jurisdiction. Indian domestic law applies to offences committed within India or with consequences in India, but the enforcement of this territorial jurisdiction is complicated by the sovereignty of foreign states, the reluctance of some jurisdictions to extradite for non-violent crimes, and the absence of bilateral agreements with key platform-hosting countries. Encrypted messaging applications such as Signal, Telegram, and WhatsApp enable perpetrators to communicate without generating accessible records. The Intermediary Guidelines Rules 2021 require significant social media intermediaries to enable traceability of message originators, but the legal and technical

[30] Parliamentary Standing Committee on Communications and Information Technology, 52nd Report on Cyber Crime (Lok Sabha Secretariat 2021).

feasibility of this requirement without compromising end-to-end encryption for all users remains deeply contested.

5.4 AI, Deepfakes, and Reactive Law

The deployment of AI tools in the perpetration of cyber crimes against women represents a paradigmatic case of reactive law struggling to keep pace with technological change. India's current statutory framework was designed in a pre-AI era and requires strained interpretive effort to apply to synthetic media, voice clones, and algorithmically targeted harassment. The Law Commission of India has acknowledged the need for review of cyber crime provisions in light of technological change,[31] but legislative action has not materialised. The consequence is a regulatory vacuum in which AI-generated deepfake pornography-clearly causing severe and measurable harm to victims-is prosecuted, if at all, under provisions designed for non-synthetic content, creating evidentiary and definitional difficulties that undermine conviction rates.

5.5 Intersectional Vulnerabilities

The cyber crimes framework operates with formal legal neutrality that obscures profound intersectional disparities in victimisation and access to justice. Dalit women, tribal women, LGBTQ+ individuals, women from religious minorities, journalists, and human rights defenders face forms of abuse that compound gender-based violence with discrimination on grounds of caste, religion, sexual orientation, and political opinion. Online caste abuse targeting Dalit women combines the traditional mechanisms of caste humiliation with the amplifying power of social media. LGBTQ+ women face outing, blackmail, and targeted harassment that exploit the vulnerability created by the absence of comprehensive anti-discrimination protections. Rural women face additional barriers: limited digital literacy, restricted access to cyber crime complaint mechanisms, physical distance from cyber cells, and less supportive community environments for disclosure. Language barriers further impede access to justice for women who cannot navigate complaint mechanisms conducted in English or Hindi.

5.6 A Reactive Rather Than Preventive Framework

The overwhelming character of India's current legal response to cyber crimes against women

[31] Law Commission of India, Report No. 289: Review of Section 66A of the Information Technology Act, 2000 (Law Commission of India 2023).

is reactive: the law responds to completed harms rather than preventing their occurrence. There is no mandatory digital literacy programme incorporating safety skills for women and girls. No statutory obligation exists on platforms to conduct gender impact assessments of their design and algorithmic systems. No proactive monitoring obligation on intermediaries addresses coordinated harassment operations before they reach individual victims. Internet Freedom Foundation's analysis has documented the systematic deployment of surveillance technologies in ways that chill women's online participation rather than protecting it.[32] OECD research confirms that the chilling effect of online harassment causes women to self-censor, withdraw from digital public spaces, and forego digital economic opportunities.[33] A preventive framework must address platform design, algorithmic amplification, mandatory safety-by-design principles, and the structural conditions of gender inequality that cyber crimes both reflect and reinforce.

CHAPTER VI COMPARATIVE REGULATORY FRAMEWORKS

6.1 European Union: GDPR and Digital Services Act

The European Union's regulatory approach to online harms rests on two foundational instruments. The General Data Protection Regulation (GDPR)[34] establishes robust consent-based data processing rules and data subject rights, including the right to erasure-the so-called "right to be forgotten"-that enables victims to demand removal of harmful content from search results and platforms. The Digital Services Act (DSA), 2022[35] imposes a tiered system of obligations on platforms proportional to their scale, requiring very large online platforms to conduct annual risk assessments addressing gender-based violence and other systemic harms, to implement effective content moderation, to provide transparent and accessible complaint mechanisms, and to submit to regulatory audit. The DSA explicitly recognises gender-based online violence as a systemic risk requiring mandatory mitigation. The EU's approach-combining data rights with proactive risk assessment and graduated platform liability-offers a model significantly more sophisticated than India's current intermediary framework.

[32] Internet Freedom Foundation, State of Surveillance 2023: Digital Rights and Freedoms in India (IFF 2023).
[33] OECD, Going Digital: Shaping Policies, Improving Lives (OECD Publishing 2019) 87.
[34] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons with Regard to the Processing of Personal Data [2016] OJ L119/1 (GDPR).
[35] Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market for Digital Services [2022] OJ L277/1 (Digital Services Act).

6.2 United Kingdom: Online Safety Act 2023

The United Kingdom's Online Safety Act 2023[36] represents the most comprehensive legislative response to online harm adopted by any major democracy. It imposes a duty of care on platforms to prevent reasonably foreseeable harms, creates priority offences addressing intimate image abuse, cyber flashing, and coercive control facilitated online, establishes age verification obligations for adult content platforms, and empowers Ofcom with substantial regulatory and enforcement authority including the power to impose fines of up to ten percent of global turnover. The Act's feminist legislative history-it was substantially shaped by a parliamentary inquiry into violence against women online-reflects a recognition that platform design and content moderation practices are not neutral but have disproportionate impacts on women and girls. India would benefit significantly from incorporating a duty of care model into its intermediary regulation framework.

6.3 United States: Platform Liability and Revenge Porn Laws

The United States presents a complex and contested regulatory picture. Section 230 of the Communications Decency Act[37] provides near-absolute immunity to online platforms for third-party content, a provision that has been widely criticised for enabling systematic impunity for gender-based online harm. At the federal level, there is no comprehensive revenge pornography or intimate image abuse statute, though legislative proposals have been introduced. At the state level, forty-eight states have enacted NCII laws with varying scopes and penalties. The US model illustrates the limitations of relying on broad platform immunity: section 230's shield has consistently frustrated civil litigation by women victims, and the resulting impunity has incentivised platforms to invest insufficiently in content moderation for gender-based harms. India's section 79 IT Act safe harbour, modelled in part on section 230, risks replicating these failures.

6.4 Australia: The eSafety Commissioner Model

Australia's Online Safety Act 2015 and its subsequent amendment[38] established the eSafety Commissioner-an independent statutory authority with powers to receive complaints about

[36] Online Safety Act 2023 (UK), c. 50.
[37] Communications Decency Act of 1996 § 230, 47 U.S.C. § 230 (1996) (US platform immunity provision).
[38] Online Safety Act 2015 (Cth) (Australia) (establishing the eSafety Commissioner).

image-based abuse, to issue removal notices to platforms, to investigate systemic safety issues, to conduct public education campaigns, and to impose civil penalties on non-compliant platforms. The eSafety model is notable for its accessible, victim-facing design: women can directly lodge complaints with the Commissioner without engaging the criminal justice system, enabling faster and more private remediation of harms. The Commissioner maintains a rapid-response removal scheme for NCII that has achieved high rates of content takedown within 48 hours. The Australian model offers India a practical template for an independent gender-based cyber harm regulator with both investigative and remedial powers.

6.5 Best Practices for India

Drawing on comparative analysis, several best practices emerge for India's regulatory reform agenda. From the EU: mandatory gender-impact risk assessments by platforms; robust data erasure rights applicable to intimate imagery; and independent regulatory audit of content moderation systems. From the UK: a statutory duty of care on platforms; priority offence status for intimate image abuse and cyber flashing; and substantial penalty powers exercisable by a technically competent regulator. From Australia: an independent eSafety-type authority with accessible, victim-centred complaint mechanisms and rapid removal powers. From all three jurisdictions: the recognition that platform regulation must address structural algorithmic and design choices, not merely respond to individual complaints.

CHAPTER VII: RECOMMENDATIONS AND CONCLUSION

7.1 Legislative Recommendations

The most urgent legislative priority is the enactment of a comprehensive, dedicated statute on gender-based cyber violence-tentatively styled the Prevention of Cyber Violence Against Women Act-that consolidates, clarifies, and enhances existing scattered provisions. Such legislation should: (i) define and criminalise deepfake abuse, including the creation of synthetic intimate imagery without consent, with enhanced penalties for commercial distribution; (ii) establish NCII as a standalone offence distinct from obscenity, with expedited civil remedies including mandatory takedown and perpetual injunctions; (iii) create a specific offence of cyber sextortion, recognising its coercive character; (iv) define coordinated online harassment campaigns as aggravated offences warranting enhanced penalties; and (v) introduce safety-by-design obligations on platform providers, requiring gender impact assessment and algorithmic

accountability as conditions of safe harbour protection under section 79 of the IT Act.

7.2 Institutional Recommendations

India should establish an independent National Digital Safety Authority (NDSA) modelled on the Australian eSafety Commissioner, with statutory authority to receive and adjudicate cyber abuse complaints from women, to issue binding removal orders to platforms, to conduct systemic investigations, and to coordinate with CERT-In, the National Commission for Women, and state police. The NDSA should maintain a 24-hour NCII rapid response unit with access to platform liaison channels. Simultaneously, state police cyber cells require mandatory accreditation standards, investment in digital forensics laboratories, and the embedding of trained gender sensitisation counsellors. The MLAT framework must be modernised through bilateral agreements with major platform-hosting countries, including provisions for emergency data preservation orders.

7.3 Procedural and Evidentiary Reforms

Procedural reforms must address the principal bottlenecks that prevent cyber crime complaints by women from reaching trial. A mandatory e-FIR registration system for cyber crimes, with automatic escalation protocols for cases involving intimate imagery or credible physical threats, would reduce the gatekeeping role of potentially sceptical or under-trained first-responding officers. Evidentiary rules should be amended to recognise hash-certified digital evidence as presumptively authentic, reversing the burden of proof on admissibility. Victim anonymity in trial proceedings should be mandatory in all cyber sexual offence cases. Legal aid clinics specialising in cyber abuse should be established in district courts, with trained para-legal first responders available through the National Legal Services Authority framework.

7.4 Education and Prevention

Effective prevention of cyber crimes against women requires structural interventions at the level of digital literacy and social norm change. A mandatory Digital Safety Curriculum covering online privacy, consent, harassment reporting, and self-protection tools should be integrated into secondary and higher education programmes. Community digital literacy centres should be established in rural areas with specific programming for women. Platforms operating in India above a defined user threshold should be required to fund and implement

annual public awareness campaigns on online safety for women. The National Commission for Women should be empowered to monitor compliance and to publish annual gender cyber safety indices holding state governments and platforms accountable for outcomes.

7.5 Conclusion

Cyber crimes against women represent one of the most urgent, underaddressed, and structurally complex challenges confronting the Indian legal system. The analysis undertaken in this paper demonstrates that while India has assembled a significant body of relevant law-constitutional guarantees of equality, dignity, and privacy; statutory provisions in the IT Act, BNS, DPDP Act, POCSO, and POSH framework; and a nascent institutional infrastructure-the overall legal response remains fundamentally reactive, forensically under-resourced, and institutionally fragmented. The constitutional framework, as interpreted by the Supreme Court in *Puttaswamy* and *Shreya Singhal*, provides the normative foundation for a rights-based, preventive regulatory paradigm. The comparative models of the European Union, United Kingdom, and Australia demonstrate that effective platform regulation, independent victim-facing remedial authorities, and safety-by-design obligations are feasible and effective. India's reform agenda must integrate these insights into a coherent, gender-transformative legal architecture. The ultimate benchmark of legal adequacy is not the number of provisions on the statute book but whether women in India-across region, class, caste, religion, and sexual orientation-can participate freely and safely in digital public life. By that measure, significant work remains.

The right of women to equal participation in the digital sphere is not a peripheral aspiration; it is a constitutional imperative flowing from the guarantee of equal citizenship under Articles 14, 15, and 21 of the Constitution of India, from India's international obligations under CEDAW, and from the foundational commitment of a democratic republic to the equal dignity of all its members. The law must rise to this challenge not merely by punishing perpetrators after harm is done, but by designing the digital environment-in collaboration with platforms, civil society, and affected communities-as a space in which women's safety, voice, and autonomy are structurally secured.

TABLE OF AUTHORITIES (SELECTED)

CONSTITUTION OF INDIA arts. 14, 15, 19, 21.

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

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

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

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

Sexual Harassment of Women at Workplace (Prevention, Prohibition and Redressal) Act, 2013, No. 14, Acts of Parliament, 2013 (India).

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

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

Vishaka v. State of Rajasthan, (1997) 6 SCC 241 (India).

Aparna Bhat v. State of Madhya Pradesh, (2021) 5 SCC 310 (India).

Regulation (EU) 2022/2065 (Digital Services Act); Regulation (EU) 2016/679 (GDPR).

Online Safety Act 2023 (UK), c. 50; Online Safety Act 2015 (Cth) (Australia).

National Crime Records Bureau, Crime in India 2022 (Government of India 2023).

United Nations, CEDAW, art. 2, Dec. 18, 1979, 1249 U.N.T.S. 13.