

**INTERNATIONAL JOURNAL OF LAW
MANAGEMENT & HUMANITIES**
[ISSN 2581-5369]

Volume 9 | Issue 5

2026

© 2026 International Journal of Law Management & Humanities

Follow this and additional works at: <https://www.ijlmh.com/>

Under the aegis of VidhiAagaz – Inking Your Brain (<https://www.vidhiaagaz.com/>)

This article is brought to you for free and open access by the International Journal of Law Management & Humanities at VidhiAagaz. It has been accepted for inclusion in the International Journal of Law Management & Humanities after due review.

In case of **any suggestions or complaints**, kindly contact support@vidhiaagaz.com.

To submit your Manuscript for Publication in the **International Journal of Law Management & Humanities**, kindly email your Manuscript to submission@ijlmh.com.

Cybercrime Against Women in India: Closing the Consent, Evidence and Enforcement Gaps

CH. RAJENDER REDDY*  AND SRINIVAS M** 

ABSTRACT

Digital communication has widened women's access to education, work, commerce and public debate, but it has also enabled persistent and scalable forms of gender-based abuse. This article examines whether Indian law provides a coherent response to cyberstalking, impersonation, doxxing, sextortion, voyeurism, non-consensual dissemination of intimate images and sexually explicit deepfakes. It uses a doctrinal and analytical method, drawing on constitutional provisions, the Information Technology Act, 2000, the Bharatiya Nyaya Sanhita, 2023, procedural and evidentiary legislation, intermediary rules and leading judicial decisions. The analysis finds that India has numerous applicable provisions, but they are distributed across statutes framed around different legal interests such as privacy, obscenity, stalking, intimidation, cheating and data protection. This fragmentation produces uncertainty in offence selection, reporting, evidence preservation and content removal. The central deficiency is the absence of a comprehensive, consent-centred offence covering the creation, threatened distribution and distribution of authentic, altered or wholly artificial intimate material. The article further finds that legal protection is weakened by underreporting, jurisdictional delay, uneven forensic capacity, dependence on platform-held information and recurrent re-uploading of harmful content. It concludes that effective reform must combine precise substantive law with immediate evidence-preservation protocols, specialised investigative and prosecutorial support, coordinated intermediary action and survivor-centred safeguards. Such an approach would protect privacy and dignity without reviving vague restrictions on lawful online expression.

Keywords: Cybercrime Against Women, Image-Based Sexual Abuse, Cyberstalking, Deepfakes, Electronic Evidence

I. INTRODUCTION

Digital space is now an ordinary site of citizenship. Education, employment, banking, political participation and personal relationships are increasingly mediated through connected devices

* Author is a Student at Aurora Deemed to be University, Bhongir, Telangana, India. ORCID: <https://orcid.org/0009-0000-4036-3998>

** Author is a Student at Aurora Deemed to be University, Bhongir, Telangana, India. ORCID: <https://orcid.org/0009-0000-7836-454X>

and online platforms. For women, this expansion creates opportunity and exposure at the same time. The very features that make digital communication useful, namely speed, reach, replicability, searchability and remote access, also allow an offender to monitor a victim continuously, conceal identity, mobilise an audience or reproduce intimate material at negligible cost. Cybercrime against women is therefore not simply an old offence committed through a computer. Technology changes the scale, duration and social meaning of victimisation.

Online and offline abuse frequently form one course of conduct. A former partner may use private information obtained during a relationship to monitor, threaten or humiliate a woman. A stranger may move from anonymous messages to doxxing and physical intimidation. A fabricated profile may be used simultaneously for personation, sexualised defamation and fraud. The legal response must consequently recognise patterns rather than isolate each message, account or upload.

The constitutional stakes are also broader than personal safety. Articles 14 and 15 require equal protection and permit special measures for women, while Articles 19 and 21 protect expression, dignity, privacy and personal autonomy.¹ When targeted sexual threats or mass harassment force women to withdraw from public platforms, the injury affects both privacy and equal participation. Yet the State cannot pursue safety through vague prohibitions on merely offensive speech. The invalidation of section 66A of the Information Technology Act, 2000 (IT Act) confirms that restrictions on online expression must remain precise and constitutionally justified.²

A. Research problem, method and argument

India does not have a single enactment dealing comprehensively with technology-facilitated gender-based violence. The applicable rules are dispersed across the IT Act, the Bharatiya Nyaya Sanhita, 2023 (BNS), the Bharatiya Nagarik Suraksha Sanhita, 2023 (BNSS), the Bharatiya Sakshya Adhiniyam, 2023 (BSA), special legislation and delegated rules governing intermediaries. A single episode may engage provisions on identity theft, privacy, stalking, voyeurism, intimidation, extortion and sexually explicit electronic material. The availability of several offences does not itself produce coherence. It can instead generate uncertain classification, incomplete investigation and inconsistent relief.

This article adopts a qualitative doctrinal method. It analyses legislation, delegated rules and leading decisions concerning privacy, expression, electronic evidence and intermediary

¹ INDIA CONST. arts. 14, 15, 19 & 21.

² *Shreya Singhal v. Union of India*, (2015) 5 SCC 1, 152–65 (India).

responsibility. Institutional materials are used only to explain the reporting and forensic structure; no claim is made that registered cases represent the prevalence of victimisation. The article advances three connected arguments. First, the distinctive wrong in image-based abuse is the intentional defeat of sexual and representational consent, not merely obscenity. Secondly, procedural speed and the preservation of reliable electronic evidence are as important as the definition of offences. Thirdly, content removal and criminal attribution must operate together: deletion without preservation may weaken prosecution, while preservation without rapid restriction allows the injury to continue.

II. THE NATURE AND PATTERNS OF GENDERED CYBERCRIME

“Cybercrime against women” describes unlawful conduct in which digital technology is the instrument, environment or target of an offence and the victim is selected, controlled or harmed in a gendered manner. It includes conduct directed exclusively at women as well as general cyber offences deployed through sexualised threats, reputational pressure or intimate knowledge. The category should not imply that all women encounter identical risks. Age, caste, disability, occupation, economic position, digital literacy and public visibility shape both exposure and access to remedies.

A. Principal forms of abuse

Cyberstalking includes repeated unwanted contact and the monitoring of a woman’s use of electronic communications. It may involve persistent messages, location tracking, surveillance through linked accounts, spyware, the repeated creation of new profiles after blocking, or threats based on observed activity. Online harassment ranges from sexual remarks and rape threats to coordinated attacks intended to overwhelm or silence a victim. Cyberbullying commonly describes repeated humiliation or exclusion, particularly among younger users, although legally relevant conduct must still be matched to the elements of a statutory offence.

Image-based sexual abuse is a more accurate expression than “revenge pornography.” The latter wrongly assumes that the perpetrator acts only after a failed relationship and can shift attention towards the victim’s prior conduct. Image-based abuse includes the non-consensual capture, threatened disclosure, distribution or manipulation of nude or sexual material. Consent to create or privately share an image is not consent to forward it. The violation lies in taking control over a person’s intimate representation and converting it into a means of punishment, profit or coercion.³

³ Clare McGlynn, Erika Rackley & Ruth Houghton, *Beyond “Revenge Porn”: The Continuum of Image-Based Sexual Abuse*, 25 FEMINIST LEGAL STUD. 25, 29–34 (2017), <https://doi.org/10.1007/s10691-017-9343-2>.

Artificial intelligence has widened this category. Face-swapping, generative systems and “nudification” tools can produce realistic sexualised material without an authentic intimate image. The harm does not depend on whether the depicted event occurred. Viewers may believe the material, employers or family members may encounter it, and the victim must repeatedly disprove a manufactured representation. The availability of low-cost tools also allows production at a scale that conventional forgery provisions were not designed to address.

Sextortion combines sexual privacy with coercion. An offender threatens to publish actual or fabricated intimate content unless the victim supplies money, more images, sexual access or another benefit. Impersonation and fake profiles may be used to solicit information, damage reputation or facilitate romance and employment fraud. Doxxing discloses identifying or location information in order to expose a woman to further harassment. Cyber voyeurism and unauthorised recording often begin in a physical space but acquire their most serious consequences through digital transmission. These categories overlap: a fake profile can distribute a deepfake, identify the victim, invite mass abuse and support an extortion demand in a single operation.

B. Digital characteristics, causes and consequences

Anonymity lowers the perceived risk of detection, although it is rarely absolute. Offenders may use false accounts, virtual numbers, compromised devices, encrypted services or virtual private networks. Digital evidence is also fragile. Accounts can disappear, messages may be set to vanish, and providers retain different categories of information for different periods. The victim sees the visible post; attribution may require subscriber information, device artefacts, login records, IP data and a lawful chain connecting the accused to the account.

Replication creates a second difficulty. Once content is copied, removing the originating post does not restore control. Identical files may remain on private devices, migrate to messaging groups or reappear through new URLs. Searchability and persistent storage mean that the injury can recur after months or years. Online access also removes the protective value of physical distance: an abusive former partner can remain continuously present through notifications, surveillance and threats.

Technology enables rather than wholly explains the offending. Misogyny, sexual entitlement, intimate-partner retaliation, financial motivation and hostility towards women in public life remain important drivers. The coercive force of sextortion often depends upon anticipated victim-blaming and the social association of a woman’s sexuality with family reputation. An offender may expect silence because disclosure could produce restrictions at home, damage

employment or intensify unwanted attention. Advice about passwords and privacy settings is useful but cannot substitute for confronting these social conditions.

The consequences are psychological, social, physical and economic. Victims may experience anxiety, insomnia, fear of physical attack, loss of work or education, and withdrawal from digital participation. Women in journalism, politics, academia, law and activism can be targeted through sexualised attacks calculated to deter public speech. International research on women journalists documents the chilling effect of such violence.⁴ The harm therefore extends beyond individual distress: it excludes voices from the digital public sphere.

III. CONSTITUTIONAL FOUNDATIONS

Privacy, equality and expression supply the normative framework within which cybercrime laws should operate. In *Justice K.S. Puttaswamy (Retd.) v. Union of India*, a nine-judge Bench recognised privacy as a fundamental right connected with dignity, bodily integrity, choice and informational control.⁵ This understanding applies directly to unauthorised surveillance, disclosure of personal data and loss of control over intimate representations. A woman does not abandon privacy merely because an image was voluntarily created or shared with a trusted recipient.

Equality matters because technology-facilitated abuse is often designed to reproduce gendered control. The formal availability of a complaint mechanism is insufficient if stigma, inaccessible procedures or insensitive evidence handling make the remedy practically unusable. Article 15(3) supports victim-sensitive procedures, including the recording of specified complaints by women officers and special protection for children. Equal citizenship also requires a digital environment in which women need not trade public participation for personal safety.

Freedom of expression has two roles. It protects women who speak online, and it restrains the State from using cyber-safety concerns as a pretext for broad censorship. In *Shreya Singhal v. Union of India*, the Supreme Court struck down section 66A because expressions such as “grossly offensive” and “annoyance” created an overbroad and chilling restriction.⁶ The lesson is not that online abuse is beyond regulation. It is that prosecution should rely upon offences with ascertainable elements, such as stalking, intimidation, privacy invasion, extortion or unlawful sexual publication, and should distinguish targeted harm from disagreement, satire or unpopular speech.

⁴ Julie Posetti et al., *The Chilling: Global Trends in Online Violence Against Women Journalists* 14–29 (UNESCO 2021), https://www.icfj.org/sites/default/files/2021-04/The%20Chilling_POSETTI%20ET%20AL_FINAL.pdf.

⁵ *Justice K.S. Puttaswamy (Retd.) v. Union of India*, (2017) 10 SCC 1, 297–302 (India).

⁶ *Shreya Singhal*, *supra* note 2, at 152–65.

IV. INDIA'S FRAGMENTED STATUTORY FRAMEWORK

A. The Information Technology Act, 2000

The IT Act remains the principal specialised cyber statute. Sections 43 and 66 address unauthorised access, copying and dishonest or fraudulent interference with computer resources. Section 66C criminalises the dishonest or fraudulent use of another person's electronic signature, password or unique identification feature, while section 66D covers cheating by personation through a communication device or computer resource.⁷ These provisions can apply to account takeovers, fraudulent profiles and gender-linked scams, provided their specific mental and factual elements are proved.

Section 66E punishes the intentional or knowing capture, publication or transmission of an image of a person's private area without consent, in circumstances violating privacy. Sections 67 and 67A address the publication or transmission of obscene and sexually explicit electronic material respectively; section 67B supplies additional protection where children are depicted.⁸ These provisions overlap but protect different interests. Section 66E is limited by its definition of "private area," while sections 67 and 67A concentrate on the character of the published material. Neither supplies a complete consent-based rule for every authentic, altered or wholly artificial intimate image.

That distinction is critical. Obscenity asks whether material meets a content standard; image-based abuse asks whether a person authorised its creation or dissemination. In *Aveek Sarkar v. State of West Bengal*, the Supreme Court adopted a contemporary community-standards approach and required allegedly obscene material to be considered as a whole and in context.⁹ An image may consequently fall outside an obscenity prohibition and still constitute a grave invasion of sexual privacy. Using obscenity as the primary doctrinal vehicle can also obscure the victim's autonomy and invite irrelevant moral inquiry.

Sections 72 and 72A deal with specified breaches of confidentiality and disclosure of personal information. Section 75 gives the IT Act extraterritorial operation where conduct outside India involves a computer, computer system or network located in India.¹⁰ Formal extraterritoriality is valuable, but practical enforcement still depends on identifying the offender and obtaining information or evidence from a foreign service provider.

⁷ Information Technology Act, No. 21 of 2000, INDIA CODE (2000), §§ 43, 66, 66C–66D.

⁸ *Id.* §§ 66E, 67–67B.

⁹ *Aveek Sarkar v. State of West Bengal*, (2014) 4 SCC 257, 268–71 (India).

¹⁰ Information Technology Act, No. 21 of 2000, INDIA CODE (2000), §§ 72, 72A & 75.

B. The Bharatiya Nyaya Sanhita and special legislation

The BNS supplements the IT Act. Section 75 treats showing pornography against a woman's will and making sexually coloured remarks as forms of sexual harassment. Section 77 criminalises voyeurism and expressly distinguishes consent to capture from consent to dissemination. Section 78 covers repeated contact despite a clear indication of disinterest and the monitoring of a woman's use of the internet, email or any other form of electronic communication. Section 79 addresses words, gestures or acts intended to insult a woman's modesty and includes intrusion upon her privacy.¹¹

Sextortion may engage section 308 where fear of injury is used dishonestly to induce the delivery of property or valuable security, and section 351 where threats to person, reputation or property cause alarm or compel conduct. Romance or employment fraud may attract sections 318 and 319 on cheating and cheating by personation. A fabricated electronic record may engage section 336, and a defamatory publication may fall within section 356.¹² These provisions should not be added mechanically. Each charge requires proof of its own ingredients, and indiscriminate overcharging can conceal the prosecution's central theory.

When the victim is under eighteen, the Protection of Children from Sexual Offences Act, 2012 (POCSO Act) adds important safeguards. Section 11 includes repeated electronic contact and threats involving real or fabricated sexual depictions of a child. Sections 13 to 15 address the use of children for pornographic purposes and specified possession or storage, while section 19 creates a reporting duty.¹³ These provisions operate alongside section 67B of the IT Act and require child-friendly handling of statements and evidence.

Technology-facilitated abuse by an intimate partner may amount to sexual, verbal, emotional or economic abuse under the Protection of Women from Domestic Violence Act, 2005 and justify protection or compensation orders.¹⁴ Cyber harassment connected with employment can also fall within the Sexual Harassment of Women at Workplace (Prevention, Prohibition and Redressal) Act, 2013.¹⁵ Internal redress does not displace criminal proceedings where the conduct independently constitutes an offence.

The Digital Personal Data Protection Act, 2023 may assist where an organisation unlawfully processes or fails to safeguard personal data, but it is not a substitute for offences addressing

¹¹ Bharatiya Nyaya Sanhita, No. 45 of 2023, INDIA CODE (2023), §§ 75, 77–79.

¹² *Id.* §§ 308, 318–19, 336, 351 & 356.

¹³ Protection of Children from Sexual Offences Act, No. 32 of 2012, INDIA CODE (2012), §§ 11, 13–15 & 19.

¹⁴ Protection of Women from Domestic Violence Act, No. 43 of 2005, INDIA CODE (2005), §§ 3, 18 & 22.

¹⁵ Sexual Harassment of Women at Workplace (Prevention, Prohibition and Redressal) Act, No. 14 of 2013, INDIA CODE (2013), §§ 2(n), 4 & 9.

stalking, coercion or intimate-image distribution.¹⁶ The Digital Personal Data Protection Rules, 2025 use phased commencement: rules 1, 2 and 17 to 21 came into force on publication, rule 4 commences after twelve months, and the remaining operational provisions commence after eighteen months.¹⁷ Any reliance on this regime must therefore identify which provisions are actually in force at the relevant time.

V. REPORTING, INVESTIGATION AND ELECTRONIC EVIDENCE

Section 173 of the BNSS permits information about a cognizable offence to be given orally or through electronic communication irrespective of the area where the offence was committed. It supports recording before transfer to the police station with territorial jurisdiction, and it requires specified information concerning offences against women to be recorded by a woman police officer or a woman officer.¹⁸ In cyber cases this early stage is decisive. A jurisdictional debate must not precede basic preservation when an account, message or live stream may disappear.

The complaint should describe the entire course of conduct. Repeated messages may establish stalking; a threat to release an image may show intimidation or extortion; the account history may reveal personation or unlawful access. Treating the visible post as the whole offence can lead investigators to preserve content but not attribution evidence. Victims should be asked necessary questions respectfully and should not have to transmit intimate material repeatedly to multiple officials.

Screenshots are useful for reporting, but they do not invariably prove authorship, completeness or authenticity. Sections 61 to 63 of the BSA govern electronic and digital records and retain a certificate-based method for qualifying computer output.¹⁹ The principles articulated under section 65B of the former Evidence Act in *Arjun Panditrao Khotkar v. Kailash Kushanrao Gorantyal* remain instructive because section 63 of the BSA continues a certification framework.²⁰ A sustainable case may require the original device, forensic extraction, metadata, platform records, subscriber information, hashes and documentation of custody. Deepfake cases may also require expert examination of generation artefacts and provenance.

Preservation must begin before takedown where possible. A platform or investigator should retain the relevant content, account identifiers, timestamps and access records securely while

¹⁶ Digital Personal Data Protection Act, No. 22 of 2023, INDIA CODE (2023), §§ 4–8 & 11–13.

¹⁷ Digital Personal Data Protection Rules, 2025, r. 1(2), G.S.R. 846(E), GAZETTE OF INDIA, Extraordinary, pt. II, sec. 3(i) (Nov. 13, 2025).

¹⁸ Bharatiya Nagarik Suraksha Sanhita, No. 46 of 2023, INDIA CODE (2023), § 173.

¹⁹ Bharatiya Sakshya Adhiniyam, No. 47 of 2023, INDIA CODE (2023), §§ 61–63 & sched..

²⁰ *Arjun Panditrao Khotkar v. Kailash Kushanrao Gorantyal*, (2020) 7 SCC 1, 45–61 (India).

disabling public access. Evidence handling must minimise further exposure: intimate files should not circulate through ordinary messaging services, access should be limited, and every transfer should be documented. These safeguards protect both the victim's dignity and evidentiary reliability.

The National Cyber Crime Reporting Portal provides a route for online complaints, with handling assigned to the relevant State or Union Territory agency.²¹ The Indian Cybercrime Coordination Centre (I4C) also supports coordination, forensic capacity, training and multi-jurisdictional action.²² These mechanisms do not remove the need for a competent local response. A victim at an ordinary police station should receive prompt registration, risk assessment and evidence preservation even if advanced attribution is later transferred to a specialised unit.

VI. INTERMEDIARY RESPONSIBILITY AND CONTENT REMOVAL

Intermediaries occupy a dual position. They host or transmit third-party content, but they also possess account data and technical capacity unavailable to victims. Section 79 of the IT Act grants conditional safe-harbour protection where the intermediary's role and due diligence satisfy the statute. In *Shreya Singhal*, the Supreme Court confined "actual knowledge" for the general takedown rule to a valid court order or governmental notification, preventing platforms from having to adjudicate every private allegation of illegality.²³

Image-based abuse receives a more immediate grievance mechanism. Rule 3(2)(b) of the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021 requires an intermediary, upon receiving an individual's complaint, to take reasonable and practicable measures within two hours (reduced from twenty-four hours by the 2026 amendment) concerning material that exposes a private area, depicts nudity or a sexual act, or involves impersonation, including artificially morphed images.²⁴ Speed is justified because every additional hour can multiply copies and viewers.

²¹ MINISTRY OF HOME AFFAIRS, *National Cyber Crime Reporting Portal: Frequently Asked Questions*, <https://cybercrime.gov.in/Webform/FAQ.aspx> (last visited Sept. 6, 2026).

²² MINISTRY OF HOME AFFAIRS, *Details About Indian Cybercrime Coordination Centre (I4C) Scheme*, https://www.mha.gov.in/en/division_of_mha/cyber-and-information-security-cis-division/Details-about-Indian-Cybercrime-Coordination-Centre-I4C-Scheme (last visited Sept. 6, 2026).

²³ *Shreya Singhal*, *supra* note 2, at 194–97.

²⁴ Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021, r. 3(2)(b), G.S.R. 139(E), GAZETTE OF INDIA, Extraordinary, pt. II, sec. 3(i) (Feb. 25, 2021), as amended by Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Amendment Rules, 2026, G.S.R. 120(E), GAZETTE OF INDIA, Extraordinary, pt. II, sec. 3(i) (Feb. 10, 2026) (substituting "two hours" for "twenty-four hours" with effect from Feb. 20, 2026).

Link-by-link removal nevertheless has structural limits. Identical material can appear through mirror sites, fresh accounts and private groups. In *X v. Union of India*, the Delhi High Court confronted the recurrent circulation of intimate images and recognised the inadequacy of relief limited to individual URLs.²⁵ A more effective model would allow privacy-preserving matching of adjudged unlawful files and coordinated de-indexing, subject to auditable procedures, human review and remedies against erroneous blocking. The objective is not general automated censorship but the prevention of the same established violation from being endlessly re-created. Removal and preservation must be coordinated. Immediate deletion without retaining evidentiary data may frustrate identification of the offender. Conversely, retaining content in public view while awaiting a criminal process perpetuates harm. Platforms should disable access promptly, preserve necessary records confidentially for lawful investigation and communicate clearly with the complainant. Standard request formats and designated law-enforcement channels would reduce delay without weakening due process.

VII. JUDICIAL RESPONSE AND THE ENFORCEMENT GAP

Indian courts have developed essential principles, although no single decision resolves the full field. *Puttaswamy* supplies the constitutional basis for informational and intimate privacy. *Shreya Singhal* requires precision in speech regulation and clarifies intermediary knowledge. *Aveek Sarkar* separates contextual obscenity analysis from the automatic condemnation of nudity. *Arjun Panditrao* emphasises the statutory method for electronic proof.

Other cases demonstrate the institutional dimension. In *Sabu Mathew George v. Union of India*, the Supreme Court required search intermediaries to adopt measures against specifically prohibited advertisements, illustrating that platforms may be directed to deploy technological controls for defined unlawful categories.²⁶ *Google India Private Limited v. Visaka Industries* confirms that intermediary immunity is conditional and depends on the applicable law, the intermediary's role and its due diligence.²⁷ The proceedings in *In re Prajwala Letter Dated 18.2.2015* produced a series of orders directing coordination among the government, law-enforcement bodies and platforms concerning videos of sexual violence.²⁸

The principal weakness remains the conversion of legal protection into a provable and timely case. Victims may delay reporting because they anticipate stigma, family consequences or

²⁵ *X v. Union of India*, W.P. (CrI.) 1082/2020, 2021 SCC OnLine Del 1788, ¶¶ 75–91 (India), <https://indiankanoon.org/doc/190535334/>.

²⁶ *Sabu Mathew George v. Union of India*, (2018) 3 SCC 229, 236–41 (India).

²⁷ *Google India Pvt. Ltd. v. Visaka Industries*, (2020) 4 SCC 162, 190–208 (India).

²⁸ *In re Prajwala Letter Dated 18.2.2015 Videos of Sexual Violence and Recommendations*, Suo Motu Writ Petition (CrI.) No. 3 of 2015, order dated Dec. 11, 2018 (India), <https://indiankanoon.org/doc/80437106/>.

repeated exposure of the material. Police may misclassify a complaint, debate jurisdiction or lack technical capacity. Providers may retain data abroad, respond slowly or be unable to produce information once retention periods expire. Forensic backlogs can make device examination untimely. Trials may then fail not because the harm was unreal but because the evidence does not establish that the accused controlled the account, or because statutory formalities were overlooked.

Secondary victimisation compounds these problems. Questions about why an image was created or shared can displace scrutiny from the unauthorised act. Consent given to one person, for one purpose or in one context cannot be expanded into universal consent. Courts and investigating agencies should protect identity, avoid reproducing intimate details or active links unnecessarily, and give victims intelligible updates about reporting, removal and protective options.

VIII. A CONSENT-CENTRED REFORM MODEL

The first reform should be a specific offence addressing intimate representations. It should cover the intentional creation, threatened distribution and distribution of authentic, altered or wholly artificial nude or sexual material where the depicted person did not consent to the relevant act. Liability should require knowledge or recklessness regarding the absence of consent and should include carefully drawn exceptions for legitimate law-enforcement, medical, evidentiary or public-interest activity. Aggravating factors may include extortion, profit, repeated dissemination, the targeting of a child or breach of an intimate relationship. The offence should focus on autonomy and foreseeable harm rather than a general obscenity standard.

Secondly, every receiving police unit should follow a minimum preservation protocol. It should record account handles, URLs, timestamps and transaction details; preserve original files where safely available; issue prompt provider requests; document hashes and custody; and refer technically complex work to a specialised unit. A victim should receive a simple preservation checklist, but failure to collect technical material personally must not become a reason to reject the complaint.

Thirdly, specialised support should connect investigation, forensics and prosecution. Prosecutorial advice at an early stage can ensure that the collected records correspond with the offence elements and BSA requirements. Training should address platform records, cloud data, artificial intelligence, cross-border requests and trauma-informed interviewing. Capacity should be distributed through regional support so that rural and small-town complainants are not placed at a permanent disadvantage.

Fourthly, intermediary coordination needs enforceable service standards. The two-hour restriction pathway for intimate and morphed content should be paired with secure evidence preservation, an accessible escalation route and status information. Once content has been judicially or lawfully determined to be non-consensual, proportionate tools should prevent identical re-uploads. Transparency reporting should distinguish complaints received, action taken, time to restriction, preservation requests and restoration after appeal.

Fifthly, victim assistance must extend beyond prosecution. Depending on the circumstances, a woman may need emergency safety planning, protection from a former partner, counselling, workplace support, compensation information or help in restoring compromised accounts. Children require POCSO-compliant procedures. Confidentiality rules should limit access to intimate files and sanction unnecessary reproduction or disclosure by officials.

Finally, official measurement should follow cases through the justice process. Complaint totals alone cannot show effectiveness. Data should distinguish complaints, first information reports, preservation requests, identified suspects, charge-sheets, trials, outcomes and the time taken for content restriction. Separate categories for cyberstalking, sextortion, image-based abuse, deepfakes, doxxing and impersonation would reveal where law or institutional practice is failing.

IX. CONCLUSION

Cybercrime against women exposes a mismatch between distributed digital harm and a fragmented legal response. Indian law already provides significant protection through constitutional rights, the IT Act, the BNS, procedural and evidentiary statutes, special enactments and intermediary obligations. These rules can address many incidents, but their overlap does not eliminate important gaps. Image-based abuse is still forced into categories built around obscenity, privacy, voyeurism, forgery, intimidation or extortion, even though its central wrong is often the deliberate destruction of control over an intimate representation.

The research problem is therefore not answered by adding harsher punishment alone. Effective protection requires four functions to work together: accurate classification, immediate preservation, rapid restriction of continuing exposure and admissible proof connecting the accused to the conduct. Failure at any one stage can defeat the others. A removed post without preserved records can weaken prosecution; a preserved file left online prolongs injury; a broad speech offence threatens constitutional expression; and a precise offence is ineffective when local police cannot secure transient evidence.

India should adopt a consent-centred offence covering authentic and synthetic intimate material, supported by standard evidence protocols, specialised technical and prosecutorial assistance, coordinated intermediary action and strict confidentiality. These measures would preserve the constitutional lesson of *Shreya Singhal* by targeting defined injury rather than subjective offensiveness, while giving practical effect to the privacy, dignity and autonomy recognised in *Puttaswamy*. Digital safety should not be framed as a demand that women withdraw, remain anonymous or accept surveillance as the price of participation. The proper objective is a system in which technological development enlarges women's freedom without enlarging the impunity of those who seek to intimidate, exploit or silence them.
