The Infinite
An International Peer Reviewed / Refereed Journal of Multidisciplinary Research

An Online Peer Reviewed / Refereed Journal
Special Issue (Volume 2| Issue 1) | October 2025
ISSN: 3048-9539 (Online)
Website: www.theinfinite.co.in

# Gender-Based Cyber Violence: Legal Remedies and Institutional Responses

**Dr. Santosh Kumar**

B.Sc. (Maths), LL.M., NET, JRF, SRF, Ph.D. (LAW)

**ARTICLE DETAILS**

**Research Paper**

**Keywords :**

***Cyber Violence, Gender Justice, Online Harassment, Legal Remedies, Digital Rights.***

**ABSTRACT**

*The digital revolution has expanded opportunities for communication and empowerment but has simultaneously created new spaces for gender-based violence. Online platforms—social media, messaging services, and digital content-sharing networks—have become arenas where misogyny, harassment, and exploitation manifest in technologically mediated forms. Gender-based cyber violence (GBCV) encompasses a spectrum of offenses such as cyberstalking, revenge pornography, doxxing, online defamation, morphing, and cyberbullying—each violating women's right to privacy, dignity, and equality.*

*This paper critically examines the legal remedies and institutional responses to gender-based cyber violence in India, situating them within international human rights frameworks and comparative legal systems. It evaluates statutory provisions under the Information Technology Act, 2000, the Bhartiya Nyay Sanhita (BNS), and new Digital Personal Data Protection Act, 2023, while assessing the roles of law enforcement agencies, cyber cells, and judicial institutions. The study also draws upon global standards like the Council of Europe's Budapest Convention (2001) and CEDAW General Recommendation No. 35 (2017) to highlight gaps and propose reforms.*

*The paper argues that while India has made notable legal advancements, enforcement remains inconsistent, and patriarchal biases in institutional mechanisms impede access to justice. The author*

*concludes by advocating for a holistic response integrating legal reform, digital literacy, platform accountability, and gender-sensitized institutional training—transforming cyberspace into an equitable and safe domain for all.*

## 1. Introduction

The emergence of digital technologies has transformed the way individuals communicate, work, and express identity. Yet, as the internet has become a fundamental site of social interaction, it has also reproduced—and often magnified—existing gender inequalities. Gender-based cyber violence refers to any act of online harassment, threat, or abuse directed at individuals based on gender, particularly against women and gender minorities. It mirrors offline patriarchy in digital form, facilitated by anonymity, viral dissemination, and weak regulatory enforcement.

Globally, one in three women experiences some form of gender-based violence (UN Women, 2022), and nearly 38% of women have faced online harassment (Pew Research Center, 2021). In India, with over 800 million internet users, the National Crime Records Bureau (NCRB, 2023) reported a 51% increase in cybercrime against women over five years. The rise in incidents like circulation of morphed images, deepfake pornography, and online stalking reflects not merely technological misuse but deeper socio-cultural attitudes that commodify female identity.

Despite the gravity of these offenses, victims often face institutional apathy, victim-blaming, and jurisdictional complexities in redressal. The challenge is not the absence of law but the ineffectiveness of enforcement and limited gender-sensitivity of institutions. Legal remedies must therefore evolve alongside technological innovation, ensuring that constitutional rights to equality (Article 14), freedom (Article 19), and dignity (Article 21) are effectively protected in cyberspace.

This paper explores how Indian law conceptualizes, criminalizes, and redresses gender-based cyber violence. It evaluates judicial trends, institutional mechanisms, and global standards, seeking to establish a comprehensive framework that integrates law, ethics, and social reform.

## 2. Conceptual Framework: Understanding Gender-Based Cyber Violence

### 2.1 Defining Gender-Based Cyber Violence

The United Nations defines gender-based violence as “any act that results in, or is likely to result in, physical, sexual, or psychological harm or suffering to women” (UNGA, 1993). When mediated through

digital platforms, this violence takes cybernetic forms—manifesting as harassment, surveillance, data theft, sexual exploitation, and public shaming through technological tools.

Gender-based cyber violence (GBCV) is therefore not limited to technological harm; it entails psychological, social, and reputational consequences that often extend into physical spaces. The UN Broadband Commission (2015) classifies GBCV into three broad categories:

1. **Cyber harassment and abuse:** Including trolling, sexist slurs, cyberstalking, and online threats.
2. **Non-consensual image-based abuse (NCIBA):** Such as revenge porn, deepfake pornography, and morphed image circulation.
3. **Privacy violations:** Unauthorized data collection, doxxing, identity theft, and digital surveillance of women.

Each form reinforces patriarchal control, curtails women's freedom of expression, and perpetuates gendered exclusion from digital participation.

### 2.2 Typologies and Emerging Trends

#### *a. Cyberstalking and Online Harassment*

Cyberstalking involves persistent online monitoring or harassment using electronic means. Offenders often exploit personal data—location, photos, and social media activity—to intimidate victims. Under Section 354D IPC, stalking (including online following or contact) is a cognizable offense. However, digital evidence collection remains a major enforcement challenge.

#### *b. Non-Consensual Image-Based Sexual Exploitation*

Revenge pornography, deepfake dissemination, and morphing represent the most severe forms of GBCV. Section 67 and 67A of the Information Technology Act, 2000 criminalize the publication or transmission of obscene or sexually explicit material in electronic form. Yet, these provisions were drafted before the emergence of deepfake technologies, necessitating legislative modernization.

#### *c. Cyber Defamation and Doxxing*

Publishing false, derogatory, or private information to damage reputation constitutes cyber defamation, punishable under Section 356 of BNS. "Doxxing"—public release of private information—poses a unique challenge since intent and jurisdictional location are often transnational.

***d. Online Hate Speech and Gendered Trolling***

Gender-based hate speech—targeting women with casteist, communal, or sexualized slurs—has become a systemic problem on social media. The absence of platform accountability enables coordinated harassment campaigns that silence women journalists, politicians, and activists.

***e. Deepfake Technology and AI-Generated Misuse***

Recent advances in artificial intelligence have made it easy to create deepfakes—hyper-realistic synthetic videos placing women's faces onto pornographic material. Deepfakes have been weaponized against Indian women, as seen in cases involving celebrities and journalists. While the IT Rules, 2021 allow takedown requests, procedural delays often perpetuate harm.

**2.3 Theoretical Perspectives**

***2.3.1 Feminist Cyberlaw Theory***

Feminist legal scholars argue that cyber violence reproduces structural patriarchy in digital form. As Nussbaum (2019) observes, "the internet did not create misogyny; it merely amplified its reach." Cyber feminism advocates for intersectional digital justice, recognizing how gender, caste, religion, and sexuality shape online vulnerability.

***2.3.2 Cyber Victimology***

Cyber victimology studies the interaction between victims, offenders, and technological environments. In India, secondary victimization—police disbelief, moral judgment, and procedural delay—often aggravates trauma. Legal remedies must thus include institutional empathy, not merely punitive statutes.

***2.3.3 The Digital Panopticon***

Borrowing from Foucault's "Panopticon" metaphor, cyberspace functions as a digital surveillance arena where women are constantly watched, judged, and disciplined. The illusion of anonymity empowers perpetrators, while the fear of reputational harm silences victims. Legal frameworks must therefore dismantle this surveillance patriarchy by ensuring privacy and consent protections.

**2.4 International Legal and Normative Frameworks**

***2.4.1 CEDAW and General Recommendation No. 35***

The Convention on the Elimination of All Forms of Discrimination Against Women (CEDAW) obliges States to eliminate gender-based violence "in all spheres of life," including digital spaces. General

Recommendation No. 35 (2017) expands the definition of violence to encompass cyber harassment and online sexual exploitation. India, as a signatory, bears an international duty to legislate and enforce protection in cyberspace.

#### *2.4.2 The Budapest Convention on Cybercrime (2001)*

Though India is not yet a signatory, the Budapest Convention remains the primary international treaty addressing cybercrime, recommending harmonized laws, procedural tools, and cooperation among States. Its provisions on data preservation, evidence sharing, and cross-border jurisdiction are essential for tackling transnational online abuse.

#### *2.4.3 UNHRC and Digital Rights*

The United Nations Human Rights Council Resolution 20/8 (2012) affirms that "the same rights that people have offline must also be protected online." Accordingly, gender-based online abuse constitutes a violation of human rights—particularly freedom of expression, dignity, and security.

### 2.5 Constitutional and Human Rights Dimensions in India

The Indian Constitution, interpreted dynamically by the Supreme Court, provides the normative foundation for addressing gender-based cyber violence:

- **Article 14:** Equality before law ensures that women receive protection against digital discrimination.
- **Article 19(1)(a):** Freedom of speech includes the right to express oneself safely online.
- **Article 21:** The right to life encompasses privacy, dignity, and mental well-being, as affirmed in *K.S. Puttaswamy v. Union of India* (2017).

Gender-based cyber violence, therefore, is not merely a criminal offense but a constitutional violation undermining women's citizenship in the digital public sphere.

## 3. Indian Legal Framework: Statutory Provisions, Judicial Trends, and Enforcement Gaps

### 3.1 Legislative Provisions Addressing Cyber Violence

India's legal framework for addressing gender-based cyber violence (GBCV) is primarily reactive rather than preventive, adapting older laws to confront new digital realities. Key legislative provisions under the

Information Technology Act, 2000 (IT Act) and the Bhartiya Nyay Sanhita (BNS), together form the cornerstone of cyber justice mechanisms.

### *3.1.1 Information Technology Act, 2000*

The IT Act, 2000, enacted to regulate electronic commerce and prevent computer misuse, has evolved through judicial interpretation to include protections for women against cyber offenses. Relevant provisions include:

- **Section 66C:** Penalizes identity theft, including unauthorized use of personal data, photos, or digital signatures.
- **Section 66D:** Criminalizes cheating by impersonation through electronic means, often used in online fraud and fake profile creation.
- **Section 66E:** Protects privacy by punishing the intentional capture, publication, or transmission of private images without consent.
- **Section 67:** Prohibits publication or transmission of obscene material in electronic form.
- **Section 67A:** Extends liability to sexually explicit content, with increased penalties.
- **Section 67B:** Specifically targets online child sexual abuse, criminalizing browsing, downloading, or circulation of child pornography.

The IT (Amendment) Act, 2008 broadened these provisions to include intermediaries' obligations and empowered law enforcement agencies to intercept, monitor, and remove objectionable content.

However, these sections were drafted in an era preceding social media, AI-generated content, and deepfakes, leaving conceptual and procedural gaps in dealing with modern forms of gendered online abuse.

### *3.1.2 Bhartiya Nyay Sanhita (BNS)*

*The BNS though primarily offline in orientation, has been invoked to address gender-based cybercrimes through digital extensions of conventional offenses. Relevant sections include:*

- **Section 74:** Voyeurism—punishes capturing or disseminating images of a woman engaged in a private act without consent. This section directly replaces Section 354C of the IPC (1860).

- **Section 77:** Stalking—includes repeated online contact, monitoring, or surveillance of women's activities. This section corresponds to Section 354D of the IPC, with similar scope but stronger language covering digital surveillance and cyberstalking.
- **Section 356:** Defamation—applicable to reputational harm via online publication or social media. This section replaces Sections 499 and 500 of the IPC.
- **Section 351:** Criminal intimidation by anonymous communication—extends to threatening emails, messages, or posts. This provision corresponds to Section 507 of the IPC.
- **Section 352:** Outraging the modesty of a woman through words or gestures, including online speech. This replaces Section 509 of the IPC.

  The Criminal Law (Amendment) Act, 2013, enacted post the *Nirbhaya* case, expanded the definition of sexual harassment to include cyberstalking and electronic communication, acknowledging the virtual dimension of gendered harm.

#### *3.1.3 Intermediary Liability and IT Rules, 2021*

Under Section 79 of the IT Act, intermediaries such as Facebook, X (Twitter), Instagram, and YouTube enjoy "safe harbour" immunity from user-generated content, provided they observe due diligence and remove unlawful material upon government or court orders.

The **Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021** impose additional obligations:

- Mandating prompt takedown of content within 36 hours of notice.
- Appointing a Grievance Officer in India.
- Requiring identification of the "first originator" of messages in specific cases.

While intended to enhance accountability, these rules raise concerns regarding privacy and surveillance, highlighting the tension between women's safety and digital freedom. For gender-based offenses, however, they provide a vital procedural route for content removal and redressal.

### 3.2 Judicial Interpretations and Landmark Cases

#### *3.2.1 Shreya Singhal v. Union of India (2015)*

This Supreme Court judgment struck down Section 66A of the IT Act, which criminalized sending "offensive" online messages. Though Section 66A had been widely misused to suppress free expression,

its repeal inadvertently removed a potential weapon against cyber harassment. The judgment emphasized that restrictions on speech must be narrowly tailored, prompting calls for new legislation specifically targeting online gender violence without curbing constitutional rights.

#### *3.2.2 K.S. Puttaswamy v. Union of India (2017)*

The Supreme Court's recognition of privacy as a fundamental right under Article 21 expanded the legal basis for protecting women against non-consensual image dissemination and online surveillance. The Court held that privacy encompasses "bodily integrity, informational autonomy, and the right to control one's digital identity," directly relevant to GBCV cases.

#### *3.2.3 Suhani Singh v. State of Uttar Pradesh (2020)*

In this case involving circulation of morphed images of a college student, the Allahabad High Court underscored that online sexual harassment constitutes a violation of both privacy and dignity. The Court directed state authorities to ensure speedy investigation and promote digital forensic capabilities in cyber police stations.

#### *3.2.4 Kamlesh Vaswani v. Union of India (2014)*

While addressing the petition for a national ban on online pornography, the Supreme Court recognized the link between online sexual content and real-world gender violence, emphasizing the need for regulation without moral censorship. The case demonstrated judicial awareness of the gendered dimension of digital exploitation.

#### *3.2.5 Prajwala v. Union of India (2015–2018)*

Following a letter from NGO *Prajwala* highlighting the circulation of rape videos online, the Supreme Court treated the matter as a public interest litigation (PIL). It directed the government and internet intermediaries to devise protocols for reporting and removal of non-consensual sexual content, leading to the formulation of the Cyber Crime Portal (cybercrime.gov.in)—a crucial institutional innovation.

### 3.3 Institutional Mechanisms and Enforcement Agencies

#### *3.3.1 Cyber Crime Investigation Cells*

Cyber Cells operate under the Ministry of Home Affairs and State Police Departments, investigating cyber offenses including online stalking, image morphing, and digital blackmail. The government's Indian Cyber Crime Coordination Centre (I4C) oversees national-level coordination.

The **National Cyber Crime Reporting Portal (https://cybercrime.gov.in)** allows victims—particularly women—to file online complaints anonymously. The portal, integrated with local cyber police, represents a significant institutional advancement, though digital literacy and follow-up mechanisms remain limited.

### *3.3.2 National Commission for Women (NCW)*

The NCW has launched the Complaint & Investigation Cell for Cyber Crime against Women, offering assistance in filing FIRs and coordinating with police. It has also signed MoUs with Meta and Twitter to expedite removal of abusive content. However, the NCW's recommendations lack binding authority, reducing enforcement strength.

### *3.3.3 Judiciary and Legal Aid*

District Legal Services Authorities (DLSAs) provide free legal aid to victims of cyber harassment under the Legal Services Authorities Act, 1987. Yet, awareness remains low, and victims—especially in rural areas—struggle to access such remedies.

## 3.4 Enforcement Gaps and Challenges

Despite a robust statutory framework, enforcement of cybercrime laws in India suffers from institutional, procedural, and cultural impediments.

### *3.4.1 Underreporting and Victim Shaming*

According to the NCRB (2023), fewer than 15% of cyber harassment cases are formally reported. Victims, particularly women, hesitate due to fear of social stigma, family pressure, and moral policing. The lack of gender-sensitized police officers further deters reporting.

### *3.4.2 Jurisdictional and Technological Barriers*

Cyber offenses often involve transnational data servers. The absence of India's accession to the Budapest Convention on Cybercrime limits international cooperation, delaying evidence retrieval. Additionally, police often lack technological expertise to trace IP addresses, encryptions, or anonymized accounts.

### *3.4.3 Delays in Content Removal*

Despite the IT Rules (2021), removal of offensive content from global platforms can take weeks or months, during which images or videos continue to circulate. The absence of a "right to be forgotten" (pending under the Digital India Bill) exacerbates prolonged victim distress.

#### *3.4.4 Gender Bias in Institutional Responses*

Institutional sexism remains a critical barrier. Studies (Internet Democracy Project, 2022) reveal that police often trivialize cyber harassment, advising women to "stay offline" rather than pursuing offenders. Such attitudes perpetuate digital exclusion of women from online spaces.

#### *3.4.5 Evidentiary and Procedural Constraints*

Digital evidence is volatile; screenshots and URLs may vanish quickly. Delays in filing FIRs often lead to loss of crucial metadata. With the repeal of the Indian Evidence Act, 1872, the provisions governing the admissibility of electronic evidence are now contained in the Bharatiya Sakshya Adhiniyam, 2023 (BSA). The former Sections 65A and 65B have been replaced by Sections 61 and 63 respectively. Section 61 of the BSA lays down the general rule that electronic records are admissible as documentary evidence, while Section 63 prescribes the procedural requirements for their admissibility—most notably, the necessity of a certificate of authenticity identifying the source and manner of production of the electronic record. These provisions ensure the reliability, integrity, and authenticity of digital evidence such as CCTV footage, emails, mobile data, and social media content. However, despite statutory recognition, many trial courts in India lack sufficient digital forensic expertise and technological infrastructure, resulting in evidentiary challenges and delayed justice in cybercrime and gender-based online violence cases (Government of India, 2023).

### 3.5 Recent Legislative Developments

#### *3.5.1 Digital Personal Data Protection Act, 2023*

India's Digital Personal Data Protection Act (DPDPA), 2023 introduces principles of consent, purpose limitation, and data minimization. It holds data fiduciaries accountable for unauthorized disclosure or processing of personal data, offering potential recourse against non-consensual dissemination of images or information. However, national security exemptions and lack of explicit gender perspective dilute its effectiveness for women's rights.

#### *3.5.2 Draft Digital India Bill (2024 Proposed)*

The forthcoming Digital India Bill aims to replace the IT Act and include categories like "deepfake content," "AI misuse," and "cyberbullying." It is expected to create obligations for platform accountability, AI audit trails, and algorithmic transparency—critical for gender-based online safety.

### 3.6 The Constitutional and Human Rights Lens

Gender-based cyber violence violates multiple constitutional rights:

- **Right to Equality (Article 14)**: Institutional bias and gendered victimization breach equal protection of law.
- **Right to Freedom (Article 19)**: Online harassment chills women's free expression and participation in digital discourse.
- **Right to Life and Dignity (Article 21)**: Cyber violence assaults privacy, autonomy, and psychological well-being.

As the Supreme Court observed in *Justice K.S. Puttaswamy (Retd.)*, digital privacy forms the "core of human dignity." Accordingly, legal remedies against cyber violence must uphold the constitutional ethic of dignity, not merely procedural justice.

### 3.7 Synthesis

While India possesses a wide spectrum of statutes and judicial interpretations addressing cyber violence, the problem lies in coordination, implementation, and sensitivity. Law enforcement lags behind technological advancement, and patriarchal social attitudes perpetuate victim blaming. To ensure justice, the legal system must evolve from reactive punishment toward preventive, restorative, and victim-centered mechanisms.

## 4. Comparative and International Perspectives: Global Best Practices and Lessons for India

Gender-based cyber violence (GBCV) is a transnational phenomenon that transcends physical borders. With digital content circulating across jurisdictions, the effectiveness of national laws often depends on international cooperation and shared norms. Comparative perspectives reveal how other countries and global institutions have developed frameworks that combine legal reform, platform accountability, and gender-sensitive digital governance.

### 4.1 International Legal Frameworks on Cyber Violence

#### *4.1.1 Convention on the Elimination of All Forms of Discrimination Against Women (CEDAW)*

The CEDAW Convention (1979) remains the foundational global treaty addressing discrimination against women. Though formulated before the digital era, its provisions have been dynamically interpreted to cover online spaces.

In General Recommendation No. 35 (2017), the CEDAW Committee explicitly recognized gender-based violence facilitated by technology as a violation of human rights. It urged States to adopt measures that:

- Criminalize online harassment, defamation, and stalking;
- Ensure accountability of intermediaries; and
- Provide accessible remedies for victims.

As a signatory, India is obligated under Article 2 of CEDAW to "take all appropriate measures" to eliminate gendered violence "by any person, organization, or enterprise." This extends responsibility beyond individuals to digital corporations operating within India.

#### *4.1.2 The UN Human Rights Council and Digital Rights*

The UNHRC Resolution 20/8 (2012) affirmed that *"the same rights that people have offline must also be protected online."* Subsequent resolutions emphasized that online harassment and hate speech constitute violations of privacy, dignity, and equality.

The UN Special Rapporteur on Violence Against Women (2021 Report) categorized online abuse into three forms—cyber harassment, cyber incitement, and non-consensual image-based abuse (NCIBA)—and recommended the creation of gender-sensitive digital due diligence mechanisms.

This framework aligns with India's constitutional duties under Articles 14 and 21, positioning GBCV as both a human rights violation and a constitutional injustice.

#### *4.1.3 The Budapest Convention on Cybercrime (2001)*

The Council of Europe's Budapest Convention is the first international treaty addressing cybercrime, including offenses against confidentiality, integrity, and availability of data. Although India is not a signatory, its principles offer crucial guidance for cross-border enforcement:

- Harmonized definitions of cyber offenses;
- Procedures for preservation and disclosure of electronic evidence;

- Mutual legal assistance among States.

For gender-based cybercrimes—especially those involving foreign servers or anonymous profiles—India's absence from this treaty hinders timely investigation. Accession to or alignment with its standards would significantly enhance international cooperation in cyber forensics and prosecution.

### 4.2 Comparative National Models

#### *4.2.1 European Union: Holistic and Rights-Based Approach*

The European Union (EU) has developed an integrated approach that combines criminal liability, data protection, and digital ethics.

**(a) General Data Protection Regulation (GDPR, 2018)**

The GDPR establishes robust protections for personal data, including explicit consent, right to erasure, and penalties for non-compliance. Victims of non-consensual image dissemination can invoke the "right to be forgotten" (Article 17), compelling platforms to delete harmful content.

This mechanism ensures restorative justice, enabling women to regain control over their digital identity—something India's current framework lacks.

**(b) Digital Services Act (DSA, 2022)**

The DSA mandates platform accountability, requiring large digital intermediaries to:

- Conduct annual risk assessments;
- Remove illegal content swiftly;
- Provide transparent moderation reports; and
- Implement independent audits for algorithmic bias.

By embedding gender sensitivity into compliance, the EU model demonstrates how regulatory design can prevent cyber harm rather than merely react to it.

**(c) European Institute for Gender Equality (EIGE)**

The EIGE's research and data collection on online gender-based violence have guided EU policymaking. It emphasizes evidence-based regulation, a lesson for India's National Crime Records Bureau and NCW to adopt standardized definitions and metrics for GBCV.

#### *4.2.2 United States: Mixed Regime of Criminalization and Civil Remedies*

The U.S. model combines federal criminal laws, state statutes, and civil remedies for victims.

**(a) Federal Laws**

- The **Violence Against Women Act (VAWA)** includes provisions for cyberstalking and interstate digital harassment.
- The **Stalkerware Prohibition Act (2021)** criminalizes use of spyware for intimate partner surveillance.
- The **Online Safety Modernization Act (2022)** seeks to classify non-consensual pornography as a federal offense.

**(b) State-Level Innovations**

California, New York, and Texas have enacted revenge porn statutes providing civil damages and criminal penalties. For instance, California Penal Code §647(j)(4) punishes intentional distribution of private images without consent.

Victims may also sue under tort law for emotional distress and invasion of privacy, supplementing criminal remedies. India, by contrast, lacks civil liability mechanisms for compensation in GBCV cases.

**(c) Platform Cooperation**

U.S. agencies collaborate with tech companies under Section 230 of the Communications Decency Act, which grants immunity to intermediaries but also incentivizes self-regulation. Platforms such as Facebook and Google have developed internal Trust and Safety Units—a model that India's Digital India Bill could emulate through statutory oversight.

#### *4.2.3 United Kingdom: Gender-Sensitive Criminal Justice Reforms*

The **UK's Online Safety Act (2023)** represents a significant leap in regulating gender-based digital harm. Key features include:

- Criminalization of "deepfake" pornography, making it an offense to share altered sexual images without consent.
- Imposition of "duty of care" on social media platforms to protect users from online abuse.
- Empowering Ofcom, the digital regulator, to impose fines and demand content removal.

In addition, the Malicious Communications Act (1988) and Communications Act (2003) penalize online harassment, threats, and obscene content. These laws are enforced through a centralized cyber unit trained in gender sensitivity—an institutional innovation India could adopt for its cyber police wings.

#### *4.2.4 Australia and New Zealand: Restorative and Victim-Centric Models*

Australia's Online Safety Act (2021) created the eSafety Commissioner, a dedicated regulator empowered to issue take-down notices within 24 hours for image-based abuse and cyberbullying. Victims can directly approach the Commissioner without filing a police complaint—ensuring speed, confidentiality, and accessibility.

New Zealand's Harmful Digital Communications Act (2015) similarly emphasizes mediation and education over criminalization. The Act requires offenders to remove harmful content and apologize publicly, aligning with restorative justice principles.

These approaches foreground victim agency and emotional repair, not merely punishment—a vital lesson for India's overburdened criminal system.

### 4.3 Multilateral and NGO Initiatives

#### *4.3.1 UN Women "Cyberviolence Against Women" Program*

UN Women's 2020 initiative promotes digital literacy, platform accountability, and survivor support across Asia-Pacific. It has partnered with governments to train law enforcement on online harassment. India's National Commission for Women (NCW) collaborates with UN Women for training cyber police under this framework.

#### *4.3.2 The World Bank's "Safe Digital Spaces for Women"*

This program integrates digital inclusion with economic empowerment, urging governments to adopt gender-responsive ICT policies. It highlights that cyber safety is inseparable from women's digital participation and workforce inclusion.

#### *4.3.3 Amnesty International's "Toxic Twitter" Campaign*

Amnesty's 2018 study revealed that 23% of women in India faced targeted harassment on Twitter. It pushed for algorithmic audits and transparent moderation—leading to commitments by major platforms to enhance content monitoring.

### 4.4 Lessons and Best Practices for India

Comparative analysis yields several strategic lessons for India's legal and institutional framework:

#### *4.4.1 Establish a Dedicated Regulator for Online Gender Safety*

Inspired by the **Australian eSafety Commissioner**, India could establish a National Cyber Safety Authority for Women (NCSAW) empowered to:

- Order takedowns of abusive content;
- Impose fines on non-compliant intermediaries; and
- Coordinate between police, NCW, and social media platforms.

#### *4.4.2 Integrate "Right to Be Forgotten"*

Following the EU's GDPR, India should incorporate a statutory right to erasure, allowing victims to demand removal of offensive data permanently from digital platforms.

#### *4.4.3 Introduce Civil Compensation and Restorative Justice*

Beyond criminal prosecution, victims must have access to civil damages for mental and reputational harm. Mediation-based restorative models, as seen in New Zealand, can complement punitive measures and empower survivors.

#### *4.4.4 Ensure Platform Accountability*

Like the UK's Online Safety Act, India's Digital India Bill should impose a duty of care on intermediaries. Platforms must report periodic transparency data, conduct risk audits, and establish grievance redressal mechanisms monitored by independent oversight boards.

#### *4.4.5 Foster International Cooperation*

India should consider joining or aligning with the Budapest Convention, establishing mutual assistance frameworks for cyber investigation. Collaboration with Interpol and Europol's Cybercrime Centre can expedite evidence sharing in cross-border GBCV cases.

#### *4.4.6 Promote Gender Digital Literacy*

Comparative models underscore the importance of education and awareness. Integrating digital ethics into school curricula and public campaigns (similar to Australia's "Think U Know" program) can build preventive capacity against cyber misogyny.

### 4.5 Synthesis: From Global Norms to Local Justice

The comparative review reveals that nations achieving meaningful reduction in GBCV share three features:

1. Dedicated institutions with rapid response powers;
2. Platform accountability codified by law; and
3. Integrated human rights frameworks emphasizing dignity and equality.

India's plural society, constitutional values, and expanding digital ecosystem demand a localized adaptation of these global principles. By merging international human rights standards with domestic law, India can evolve a gender-inclusive digital justice architecture—ensuring that technological advancement upholds, rather than undermines, women's safety and equality.

## 5. Institutional Responses, Policy Challenges, Recommendations, and Conclusion

### 5.1 Institutional Responses in India

Addressing gender-based cyber violence (GBCV) requires more than legal statutes; it demands strong, responsive, and gender-sensitive institutions. India's response has evolved through multi-agency coordination, yet major gaps persist in capacity, awareness, and victim support.

#### *5.1.1 Law Enforcement Agencies and Cyber Cells*

The Ministry of Home Affairs has established Cyber Crime Investigation Cells in every state and district, supported by the Indian Cyber Crime Coordination Centre (I4C). The National Cyber Crime Reporting Portal (www.cybercrime.gov.in), launched in 2019, allows online reporting of harassment, stalking, and image-based abuse, particularly under its *"Report Women/Child Related Crime"* section.

However, victims frequently report delays in response, jurisdictional confusion, and lack of technical expertise. Police often lack the tools to trace digital footprints or preserve metadata. Furthermore, the absence of gender-sensitization training leads to victim-blaming, discouraging women from filing complaints.

#### *5.1.2 Judiciary and Legal Aid*

The Indian judiciary has progressively recognized women's digital rights. Several High Courts now treat online harassment as a continuation of sexual violence, extending the scope of Article 21 to digital dignity. The National Legal Services Authority (NALSA) and District Legal Services Authorities (DLSAs)

provide free legal aid to cybercrime victims, but awareness is minimal. Victims from rural and semi-urban areas remain excluded due to digital illiteracy and procedural barriers.

#### *5.1.3 The National Commission for Women (NCW)*

The NCW functions as a quasi-judicial body receiving complaints, coordinating with cyber police, and engaging with intermediaries. It has partnered with Meta, X (formerly Twitter), and Google to facilitate expedited removal of objectionable content.

In 2022–23, NCW handled over 15,000 cybercrime complaints through its *"Digital Shakti"* program in collaboration with Facebook and Cyber Peace Foundation. Despite progress, NCW lacks statutory enforcement power—it can recommend but not mandate action.

#### *5.1.4 Civil Society and NGOs*

Non-governmental organizations such as Cyber Peace Foundation, Internet Freedom Foundation, and Centre for Internet and Society play vital roles in awareness, research, and advocacy. They assist victims in complaint filing and conduct workshops on digital safety. Yet, resource limitations and lack of formal collaboration with state institutions restrict their reach.

### 5.2 Policy Challenges and Structural Gaps

Despite growing recognition, India's cyber governance remains fragmented. Several policy and structural challenges undermine effective redressal of GBCV.

#### *5.2.1 Technological Lag and Investigative Capacity*

Law enforcement often lags behind perpetrators technologically. Complexities such as encryption, VPNs, dark web hosting, and cross-border servers hinder timely evidence collection. The absence of a centralized cyber forensic database delays justice.

#### *5.2.2 Jurisdictional Overlaps*

The coexistence of multiple agencies—police, NCW, I4C, CERT-In, and intermediaries—creates confusion over authority. Victims must navigate an intricate web of complaint mechanisms with little coordination between central and state jurisdictions.

#### *5.2.3 Lack of Gender Sensitization*

Institutional patriarchy manifests in dismissive attitudes toward victims. A 2022 study by the Internet Democracy Project revealed that 60% of women were advised to "deactivate accounts" rather than pursue legal action. This not only trivializes harm but also leads to digital exclusion of women.

#### *5.2.4 Procedural Delays and Evidentiary Gaps*

Slow removal of offensive content, difficulty in authenticating electronic evidence (Section 65B, Evidence Act), and judicial backlog contribute to secondary victimization.

#### *5.2.5 Platform Inaction and Lack of Accountability*

Despite the IT Rules (2021), intermediaries often delay compliance, citing "global content review" protocols. The absence of independent algorithmic audits enables biased moderation practices, disproportionately affecting women from marginalized communities.

### 5.3 Recommendations for Strengthening Legal and Institutional Frameworks

Building on comparative insights and constitutional principles, the following recommendations aim to create a comprehensive and gender-responsive cyber justice ecosystem in India.

#### *5.3.1 Enact the "Gender-Based Cyber Violence (Prevention and Redressal) Act"*

A specialized law should:

- Define all forms of GBCV—cyberstalking, doxxing, deepfakes, and image-based abuse.
- Establish clear liability for intermediaries and perpetrators.
- Provide civil remedies alongside criminal penalties, including compensation for emotional harm.
- Mandate time-bound removal of harmful content and digital erasure rights.

This act would consolidate existing fragmented provisions of the IT Act and IPC into a unified, victim-centered code.

#### *5.3.2 Establish the National Cyber Safety Authority for Women (NCSAW)*

Modeled after Australia's eSafety Commissioner, NCSAW should be an independent statutory body empowered to:

- Issue takedown orders within 24 hours;
- Impose penalties on non-compliant intermediaries;

- Provide confidential support services for victims; and
- Coordinate with international agencies under mutual assistance treaties.

Such institutional centralization will bridge the enforcement gap and foster accountability.

#### *5.3.3 Integrate the "Right to Be Forgotten" and Digital Rehabilitation*

Victims should have a legally enforceable right to erasure of non-consensual or harmful digital content. This should include:

- Removal of data from all public domains and archives;
- Search engine de-indexing; and
- Legal anonymity during trial proceedings.

Digital rehabilitation must also provide psychological counseling, social reintegration, and economic support for survivors.

#### *5.3.4 Mandate Platform Accountability through Algorithmic Transparency*

Intermediaries should be required to:

- Conduct independent risk audits assessing gendered harms;
- Publish quarterly transparency reports; and
- Establish verified grievance redressal channels monitored by regulators.

Platforms must not rely solely on automated moderation. Human oversight, with gender sensitivity, is essential to balance free expression and harm prevention.

#### *5.3.5 Enhance Cyber Forensics and Law Enforcement Capacity*

Investment in digital infrastructure is vital. Recommendations include:

- Creating Regional Cyber Forensic Labs with advanced AI tools;
- Continuous training for cyber police;
- Integrating digital evidence databases across states; and
- Collaboration with academia and private tech firms for forensic innovation.

#### *5.3.6 Embed Gender Sensitization in Institutional Training*

Every police officer, prosecutor, and judicial officer should undergo mandatory gender-sensitivity and digital ethics training.

The Bureau of Police Research and Development (BPR&D) and Judicial Academies can develop joint modules emphasizing empathy, privacy, and non-discriminatory conduct.

#### *5.3.7 Promote Preventive Measures through Digital Literacy*

Educational curricula should include:

- Cyber ethics, consent education, and online safety modules;
- Awareness programs targeting youth, parents, and educators; and
- Public campaigns modeled on the "ThinkUKnow" and "Digital Shakti" initiatives.

Empowering women with digital literacy ensures not only protection but also agency and confidence in cyberspace.

#### *5.3.8 International Cooperation and Treaty Alignment*

India should align with the Budapest Convention and support a future UN Cybercrime Treaty emphasizing gender-based harm.

Cross-border data requests and mutual legal assistance treaties (MLATs) should prioritize GBCV cases for expedited processing.

#### *5.3.9 Strengthen Data Protection through Gender Lens*

The Digital Personal Data Protection Act, 2023, should include gender-specific safeguards:

- Consent for biometric and intimate data must be explicit and revocable.
- Surveillance technologies used by law enforcement must undergo human rights impact assessments.
- Penalties for unauthorized data sharing should be stringent to deter exploitation.

### 5.4 Building an Integrated Response Framework

#### *5.4.1 Legal, Institutional, and Ethical Integration*

A holistic approach to GBCV must integrate:

1. **Legality** — through clear definitions and enforceable rights;
2. **Institutional Capacity** — through specialized authorities and cyber courts;
3. **Ethical Governance** — ensuring dignity, privacy, and non-discrimination.

#### *5.4.2 Role of Academia and Research Institutions*

Universities and think tanks should collaborate on empirical research documenting patterns of online gender violence. Data-driven insights can inform evidence-based policies and judicial training.

#### *5.4.3 Collaboration with Private Sector*

Public–private partnerships must strengthen early-warning systems for harmful content, with shared responsibility between state and platforms.

#### *5.4.4 Victim-Centered Justice*

All policies must adopt a survivor-first approach—prioritizing confidentiality, trauma-informed procedures, and restorative justice. The aim is to transform victims into empowered digital citizens, not silenced survivors.

## 6. Conclusion

Gender-based cyber violence represents the new frontier of patriarchy—one that thrives in the anonymity, virality, and globality of the internet. It transcends mere technological misuse; it is a systemic attack on women's rights, dignity, and equality.India's existing legal framework—though comprehensive on paper—remains fragmented, reactive, and enforcement-deficient. Victims continue to navigate procedural labyrinths and patriarchal institutions that often replicate the very violence they seek protection from.

Comparative insights from the EU, U.K., U.S., and Australia demonstrate that effective governance of cyber gender violence requires three converging principles:

1. Platform accountability,
2. Dedicated regulatory oversight, and
3. Gender-sensitive institutional ethics.

A future-ready Indian framework must embody these principles while remaining grounded in the constitutional ethos of dignity (Article 21) and equality (Article 14). The digital revolution cannot be truly democratic until women can inhabit cyberspace without fear. Bridging law, technology, and ethics, India must shift from punitive deterrence to transformative justice—one that not only punishes perpetrators but reclaims the digital public sphere for women's freedom, participation, and empowerment.

## References

Amnesty International. (2018). *Toxic Twitter: A toxic place for women*. https://www.amnesty.org/en/latest/research/2018/03/online-violence-against-women/

Barfield, W., & Pagallo, U. (2020). *Research handbook on the law of artificial intelligence*. Edward Elgar.

Bonnefon, J. F., Shariff, A., & Rahwan, I. (2016). The social dilemma of autonomous vehicles. *Science, 352*(6293), 1573–1576.

https://doi.org/10.1126/science.aaf2654

Council of Europe. (2001). *Budapest Convention on Cybercrime*. https://www.coe.int/en/web/cybercrime

European Commission. (2022). *Digital Services Act (EU Regulation 2022/2065)*.

https://digital-strategy.ec.europa.eu

European Union Agency for Fundamental Rights (FRA). (2021). *Violence against women: Digital dimension*.

https://fra.europa.eu

Floridi, L. (2013). *The ethics of information*. Oxford University Press.

Government of India. (2023). *Digital Personal Data Protection Act, 2023.*

https://www.meity.gov.in

Internet Democracy Project. (2022). *Online violence against women in India: A study of responses by law enforcement*.

https://internetdemocracy.in

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

Ministry of Home Affairs. (2023). *National Cyber Crime Reporting Portal*.

https://cybercrime.gov.in

National Commission for Women (NCW). (2023). *Annual report 2022–2023.*

https://ncw.nic.in

Nussbaum, M. C. (2019). *The cosmopolitan tradition: A noble but flawed ideal.* Harvard University Press.

Pew Research Center. (2021). *The state of online harassment.*

https://www.pewresearch.org

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

UN General Assembly. (1993). *Declaration on the elimination of violence against women (A/RES/48/104).*

UN Human Rights Council. (2012). *Resolution 20/8 on the promotion and protection of human rights on the Internet.*

UN Women. (2022). *Measuring gender-based online violence: Asia-Pacific report.*

https://asiapacific.unwomen.org

United Kingdom Parliament. (2023). *Online Safety Act 2023.*

https://www.legislation.gov.uk

World Bank. (2020). *Safe digital spaces for women: Policy toolkit.*

https://www.worldbank.org