TECHNOLOGY-FACILITATED GENDER-BASED VIOLENCE IN INDIA: CYBERBULLYING, DEEPFAKES, AND THE LAW

Dr. Shradha Sharma, Assistant Professor, School of Law, Bennett University

ABSTRACT

Digital technologies have transformed communication, work, and education, but they have also created new spaces for violence. Women and minor girls are disproportionately targeted through cyberbullying, deepfake pornography, image-based abuse, cyberstalking, and other forms of technology-facilitated gender-based violence (TF-GBV). Global estimates suggest that about one in ten women have already experienced some form of cyber violence since the age of 15, and that girls and young women are among the biggest targets of online abuse.

Recent research shows that non-consensual sexually explicit deepfakes now constitute the overwhelming majority of deepfake videos online and overwhelmingly target women, adding a new layer of psychological harm and reputational risk. In India, National Crime Records Bureau (NCRB) data indicate a steady rise in cyber-crime and crimes against women, signalling that online violence is part of a broader continuum of gendered harm.

This paper examines cyberbullying, deepfakes, and online gender-based violence against women and minor girls through a socio-legal lens. It (i) conceptualises key forms of technology-facilitated violence, (ii) situates them within international human rights standards, (iii) analyses the Indian legal framework (IT Act, IPC, POCSO, intermediary rules, and data protection law), (iv) discusses enforcement challenges and illustrative cases, and (v) proposes legal, policy, and institutional reforms. The paper argues that existing laws, while not wholly inadequate, are fragmented and reactive. A comprehensive, victim-centred and techno-social approach—integrating law reform, platform accountability, digital literacy, and gender-transformative education—is essential to meaningfully protect women and girls in the digital age.

Keywords: Cyberbullying, Deepfakes, Online Gender-Based Violence, Women, Minor Girls, India, Technology-Facilitated Violence, Image-Based Abuse.

1. Introduction

The expansion of internet penetration and smartphone access has dramatically altered social and economic life in India and across the globe. Yet this digital transformation has also intensified old hierarchies and forms of domination. Gender-based violence—already one of the most pervasive human rights violations worldwide now has a powerful digital dimension.[1]

International and regional bodies note that women and girls experience online violence in multiple forms: cyberstalking, non-consensual sharing of intimate images, doxing, deepfake pornography, cyberbullying, and coordinated misogynistic trolling.[2] These harms are not "virtual" in their impact; they produce concrete psychological, social, educational, and economic consequences.[3]

For minor girls, the stakes are often higher. Adolescents navigate identity, sexuality, and peer relationships in heavily mediatised environments. Cyberbullying and image-based abuse can lead to school avoidance, self-harm, or long-term mental health issues.[4]

In India, the steady rise in crimes against women and cyber-crime reported by the National Crime Records Bureau (NCRB) underscores the urgency of examining technology-facilitated gender-based violence as a socio-legal problem rather than a purely technological one.[5]

This paper seeks to provide a structured socio-legal analysis of this phenomenon, with a particular focus on cyberbullying, deepfakes, and online gender-based violence against women and minor girls.

2. Conceptual and Theoretical Framework

2.1 Technology-Facilitated Gender-Based Violence (TF-GBV)

Technology-facilitated gender-based violence refers to any act of gender-based violence that is committed, assisted, aggravated, or amplified by the use of digital technologies—such as social media, instant messaging, email, gaming platforms, or AI tools.[6]

---

[1] UN General Assembly, *Declaration on the Elimination of Violence against Women* (1993)
[2] UN Women, *Online Violence Against Women and Girls* (2015).
[3] Danielle Citron, *Hate Crimes in Cyberspace* (Harvard University Press, 2014).
[4] UNICEF, *Ending the Torment: Tackling Bullying from the Schoolyard to Cyberspace* (2016).
[5] National Crime Records Bureau, *Crime in India 2023.*
[6] UNFPA, *Technology-Facilitated Gender-Based Violence* (2020)

Common forms include:

- Cyberbullying and online harassment
- Cyberstalking and doxxing (publishing personal information)
- Non-consensual sharing of intimate images ("revenge porn", though the term is contested)
- Deepfake pornography and morphed images
- Online threats of rape or physical violence
- Online grooming of children and sextortion

TF-GBV is rooted in the same patriarchal norms and power inequalities that underpin offline violence; digital tools simply extend its reach, speed, and permanence.[7]

2.2 Cyberbullying: Gendered Patterns

Cyberbullying is generally defined as intentional and repeated aggression carried out by a group or individual using electronic forms of contact against a victim who cannot easily defend themselves. Across OECD countries, girls report higher levels of cyberbullying victimisation than boys.[8]

A UNICEF poll across 30 countries found that one in three young people have been victims of online bullying, with substantial proportions reporting that cyberbullying leads them to skip school.[9] When gender-disaggregated, several studies show that girls and young women report higher rates of online harassment and are more likely to face sexualised abuse.

2.3 Deepfakes and Image-Based Abuse

Deepfakes are hyper-realistic but synthetic images, videos, or audio recordings generated using deep learning techniques that depict a person doing or saying something they never did. While

[7] Nancy Fraser, 'Rethinking the Public Sphere' (1990) 25 *Social Text* 56
[8] OECD, *Education at a Glance* (2021)
[9] UNICEF, *Global Poll on Cyberbullying* (2019)

deepfake technologies have benign applications in art and entertainment, their most prevalent use is now in sexually explicit content.[10]

Research suggests that non-consensual pornography constitutes around 96–98% of deepfake videos online, and women are overwhelmingly targeted in such material. Deepfake pornography thus functions as a form of image-based sexual abuse, not mere "erotic content".[11]

For minor girls, the threshold for harm is even lower: ordinary school photos, social media selfies, or class pictures can be harvested and morphed, often by peers, and circulated via closed messaging groups, creating enduring reputational and psychological damage.[12]

2.4 Online Gender-Based Violence as a Continuum

International studies emphasise that online and offline violence form a continuum rather than discrete categories.[13] The Economist Intelligence Unit's global study across 45 countries found that 85% of women have experienced or witnessed online violence, and many reported that online abuse spills over into offline threats and stalking.

Conceptually, therefore, cyberbullying and deepfake-based abuse should be understood as part of broader structures of gender inequality, rather than as isolated or purely "digital" phenomena.

3. Global and Indian Empirical Landscape

3.1 Global Trends

Key global findings include:

- An estimated one in ten women has experienced some form of cyber violence since the age of 15.[14]
- Plan International found that 58% of girls have experienced online harassment, with

[10] Henry Ajder et al, *The State of Deepfakes* (Deeptrace, 2019)
[11] Clare McGlynn & Erika Rackley, 'Image-Based Sexual Abuse' (2017) 37 *Oxford Journal of Legal Studies* 534
[12] OECD, *PISA 2018 Results (Volume III): What School Life Means for Students' Lives* (2019)
[13] WHO, *Violence Against Women Prevalence Estimates* (2021)
[14] UN Broadband Commission, *Cyber Violence Against Women and Girls* (2015)

many reporting that online abuse is more pervasive than street harassment.

- UNFPA and UN Women highlight that a very high proportion of women report that technology-facilitated violence adversely affects their wellbeing, safety, and participation in public life.

3.2 India: Crimes Against Women, Children, and Cyber-Crime

India's NCRB "Crime in India" reports show both an overall increase in crimes against women and a parallel surge in cyber-crime. NCRB data indicate over 4.45 lakh cases of crimes against women in 2022, with further increases in 2023.[15]

In terms of cyber-crime, the 2023 report records about 86,420 cyber-crime cases, a rise of over 30% from 2022, with a cyber-crime rate increase from 4.8 to 6.2 per lakh population. Among the motives, "causing disrepute", "extortion", and "personal revenge" are significant, all of which are relevant to gender-based online abuse.[16]

Although NCRB's classification does not always isolate deepfake or non-consensual image-based offences, civil society reports and media investigations reveal an uptick in morphed image circulation, sextortion, and deepfake pornography targeting women and girls.

A recent case from Lucknow, for instance, involved BA students allegedly editing and circulating obscene morphed images of women via fake Instagram accounts, leading to arrest under cyber-crime provisions. Such instances, while anecdotal, illustrate how easily accessible editing and AI tools are being weaponised in social and educational spaces.

4. International Normative Framework

4.1 CEDAW and General Recommendations

The Convention on the Elimination of All Forms of Discrimination against Women (CEDAW) obliges States to eliminate discrimination and violence against women in all spheres, including those emerging in digital environments.[17] General Recommendation No. 35 clarifies that

[15] NCRB, *Crime in India 2023*
[16] Internet Freedom Foundation, *Deepfakes and the Law in India* (2023)
[17] CEDAW, General Recommendation No. 35 (2017)

gender-based violence against women includes acts committed in digital contexts and requires States to prevent, investigate, punish, and provide reparations.

4.2 Regional Standards

The Council of Europe's Istanbul Convention and its thematic reports explicitly address cyber-violence and the digital dimension of violence against women, urging States to criminalise various forms of online abuse and ensure effective remedies, including swift content removal and platform obligations.

While India is not a party to these regional instruments, they provide persuasive guidance for law reform and judicial interpretation.

4.3 UN Resolutions and Policy Guidance

UN Women, UNFPA, and other UN entities have issued briefs and policy guidance on online violence against women and girls, emphasising the need for multi-stakeholder responses involving States, platforms, and civil society.[18]

5. Indian Legal Framework

5.1 Information Technology Act, 2000 and Rules

Key provisions relevant to cyberbullying and deepfake-related abuse include:[19]

- **Section 66E** – Punishes violation of privacy through intentional capturing, publishing, or transmitting images of a person's private areas without consent.
- **Section 66D** – Addresses cheating by personation using computer resources, relevant to fake profiles and impersonation accounts.
- **Sections 67, 67A, 67B** – Penalise publication or transmission of obscene, sexually explicit content and child sexual abuse material (CSAM).

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

[18] UN Human Rights Council Res 38/5 (2018)
[19] Information Technology Act, 2000

Rules, 2021 impose due-diligence obligations on intermediaries, requiring them to remove or disable access to unlawful content upon receiving actual knowledge or court/government orders, and to enable reporting mechanisms for users, including complaints relating to nudity or sexual content.[20] (Platform-level compliance and over-broad takedowns remain contentious.)

5.2 Indian Penal Code (IPC)

Several IPC provisions can be invoked in cases of online gender-based violence:

- **Section 354A** – Sexual harassment;
- **Section 354C** – Voyeurism;
- **Section 354D** – Stalking, including monitoring of a woman's use of the internet or email;
- **Section 499–500** – Defamation, relevant for reputational harm from false allegations;
- **Section 506** – Criminal intimidation;
- **Section 509** – Word, gesture, or act intended to insult the modesty of a woman.

These provisions, though drafted with offline contexts in mind, have been applied to online harassment and circulation of morphed images.[21]

5.3 POCSO Act, 2012

The **Protection of Children from Sexual Offences (POCSO) Act** is crucial where minor girls are targeted:

- It criminalises the use of children for pornographic purposes (Sections 13–15)[22], including storage, dissemination, and browsing of such material.
- It introduces mandatory reporting obligations for institutions and individuals who

[20] IT (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021
[21] *Shreya Singhal v Union of India* (2015) 5 SCC 1
[22] Protection of Children from Sexual Offences Act, 2012

become aware of offences, which has implications for schools and platforms hosting child-targeted content.

5.4 Data Protection and Privacy

The **Digital Personal Data Protection Act, 2023 (DPDPA)** introduces a consent-based framework for the processing of personal data, with enhanced protections for children's data. Misuse of personal data for deepfake creation, doxxing, or non-consensual dissemination potentially engages both data protection and criminal law obligations.

However, the Act is not specifically designed as a TF-GBV instrument. Its effectiveness depends on how "harm" and "unlawful processing" are interpreted and enforced in cases involving image-based abuse.

6. Gaps and Challenges in the Current Framework

6.1 Fragmentation and Lack of Deepfake-Specific Offences

Although a combination of IT Act, IPC, and POCSO provisions can be applied to deepfake pornography and cyberbullying, there is no explicit statutory recognition of "synthetic media" or "deepfakes" in Indian criminal law. By contrast, some jurisdictions (for example, the UK and parts of Australia) are moving towards dedicated offences for sexually explicit deepfakes and non-consensual synthetic intimate imagery.

This lack of specificity complicates investigation and prosecution, especially where perpetrators argue that "no real nudity" occurred because the image is "fake".

6.2 Anonymity, Jurisdiction, and Cross-Border Platforms

Perpetrators can easily use VPNs, foreign servers, or anonymous accounts to create and disseminate abusive content. Cross-border data access requests are slow, and platforms may be headquartered outside India. This creates delays in identifying offenders and preserving evidence.

6.3 Under-Reporting and Victim-Blaming

Social stigma, fear of reputational damage, and victim-blaming attitudes deter many women

and minor girls from reporting. UN and regional studies stress that online abuse is often trivialised and dismissed as "not real" or "harmless banter", despite strong evidence of psychological and social harm.[23]

For minor girls, parental reactions can also be punitive (restrictions on device use, blaming dress or behaviour), further discouraging disclosure.

6.4 Institutional Capacity and Digital Literacy

Police, prosecutors, and judicial officers may lack specialised training in handling digital evidence, identifying deepfakes, or working with traumatised child survivors. At the same time, schools and colleges often lack robust cyber-safety policies or complaint mechanisms.

Digital literacy gaps persist—many girls and women lack knowledge about privacy settings, reporting tools, or legal remedies.

7. Impact on Women and Minor Girls

7.1 Psychological and Health Impacts

UN and regional reports consistently associate online violence with anxiety, depression, PTSD symptoms, and in severe cases, suicidal ideation—particularly among young women and girls.[24]

Deepfake pornography and non-consensual image-sharing are particularly devastating because of their permanence and the difficulty of erasing content once it has spread.[25]

7.2 Educational and Professional Consequences

For minor girls, cyberbullying and image-based abuse can lead to absenteeism, school drop-out, and reduced participation in classroom and extracurricular activities.

For adult women—especially those in public life, such as journalists, activists, and

[23] UN Special Rapporteur on Violence Against Women, *Report on Online Violence Against Women and Girls* UN Doc A/HRC/38/47 (2018)
[24] World Health Organization, *Violence Against Women* (2021)
[25] Nicola Henry and Anastasia Powell, 'Technology-Facilitated Sexual Violence: A Literature Review of Empirical Research' (2018) 19 *Trauma, Violence & Abuse* 195

politicians—online harassment creates a chilling effect on speech and participation. Studies documenting online hate and disinformation targeting female parliamentarians in Asia-Pacific and other regions suggest that digital hostility can deter women from entering or remaining in politics.

7.3 Economic and Reputational Harm

Victims may lose employment opportunities, suffer career stagnation, or face discrimination due to reputational damage caused by false allegations or manipulated sexual content. Deepfakes, precisely because they appear "real", can severely undermine credibility and trust.

8. Platform Responsibility and Algorithmic Dimensions

Social media and content-sharing platforms are major sites of TF-GBV. Key concerns include:

- **Amplification by algorithms:** Engagement-driven recommender systems may inadvertently promote sensational or abusive content, including misogynistic trolling.
- **Inadequate reporting and redress:** Complex complaint processes, opaque moderation standards, and inconsistent enforcement disproportionately affect victims who lack legal or technical support.
- **Lack of age-appropriate design:** Platforms frequented by minors may not implement robust age-verification, default privacy settings, or AI-based detection of grooming and sextortion.

The World Bank's assessment of cyber-harassment stresses that addressing violence against women and girls online requires integrating platform design, data-driven risk assessments, and regulatory obligations with broader gender equality policies.

9. Reform Proposals and Policy Recommendations

9.1 Substantive Law Reform

1. **Explicit Criminalisation of Deepfake-Based Abuse**
    - Introduce dedicated provisions in the IPC or IT Act to criminalise creation,

distribution, and threats to distribute non-consensual synthetic intimate images, with aggravated penalties where victims are minors.

- Clarify that "real" nudity is not a prerequisite; the harm lies in unauthorised sexualised representation and privacy invasion.

2. **Recognition of Technology-Facilitated Gender-Based Violence**

   - Statutorily recognise TF-GBV as a form of gender-based violence, to facilitate better data collection, targeted policies, and survivor-centred remedies.

3. **Civil Remedies and Protection Orders**

   - Strengthen civil law remedies allowing rapid injunctions, content takedown, and damages.

   - Consider specialised digital protection orders (similar to restraining orders) for victims of cyberstalking and online harassment.

9.2 Procedural and Enforcement Measures

1. **Fast-Track Takedown and Preservation of Evidence**

   - Mandate time-bound takedown (e.g., within 24 hours) of obviously unlawful non-consensual sexual content upon verified complaint, balanced with procedural safeguards against misuse.

   - Require platforms to preserve metadata and logs for investigation while protecting user privacy.

2. **Capacity-Building for Law Enforcement and Judiciary**

   - Continuous training on digital forensics, deepfake detection tools, and trauma-informed interviewing of survivors (especially children).

   - Develop specialised cyber-crime units with gender-sensitised approaches.

3. **Improved Data and Classification**

- NCRB and similar bodies should introduce specific categories for deepfakes, image-based abuse, and online gender-based violence to enable better policy, research, and monitoring.

9.3 Platform Governance

1. **Stronger Due-Diligence Obligations**

   - Refine intermediary rules to explicitly address deepfakes, synthetic media, and TF-GBV, including obligations to deploy detection tools and human review for flagged content.

   - Encourage or mandate "safety-by-design" features—default privacy for minors, friction before sharing intimate content, and clear education prompts around consent.

2. **Transparency and Independent Audits**

   - Require periodic transparency reports disaggregating data on gender-based online abuse, response times, and outcomes.

   - Allow independent researchers to access anonymised platform data (under safeguards) to study patterns of TF-GBV.

9.4 Education, Prevention, and Support Services

1. **Digital Literacy and Rights Education**

   - Integrate cyber-safety, consent, and gender equality modules in school and university curricula.

   - Provide age-appropriate guidance for minor girls on privacy settings, reporting mechanisms, and supportive adult contacts.

2. **Parental and Teacher Training**

   - Conduct training for parents and educators on recognising signs of online abuse, responding supportively, and utilising legal/reporting mechanisms.

3. **Helplines and Counselling**

    - Strengthen national and state-level cyber-crime helplines (such as 1930), and ensure they are equipped to handle gender-based online violence cases with sensitivity.

    - Provide accessible psychological counselling and legal aid for survivors, including tele-counselling services.

4. **Gender-Transformative Campaigns**

    - Public awareness campaigns that challenge victim-blaming, promote bystander intervention online, and encourage responsible digital citizenship among boys and men.

10. Conclusion

Cyberbullying, deepfakes, and online gender-based violence against women and minor girls are not marginal or emerging issues; they are central challenges in contemporary digital societies. Global and Indian evidence demonstrates that women and girls bear a disproportionate burden of technology-facilitated abuse, with serious impacts on their health, dignity, education, economic opportunities, and democratic participation.

India's legal framework provides several entry points for redress—through the IT Act, IPC, POCSO, and emerging data protection norms—but these instruments remain fragmented and reactive. They were not drafted with AI-driven deepfakes and platform-mediated harassment in mind.

To move from piecemeal responses to a coherent strategy, reforms must:

- Explicitly recognise deepfake-based abuse and TF-GBV in law,
- Impose clear responsibilities on platforms,
- Build institutional capacity and improve data, and
- Invest in preventive, educational, and psychosocial interventions.

Ultimately, safeguarding women and minor girls online requires more than technical fixes; it demands sustained efforts to dismantle the gendered power relations that normalise abuse—offline and online alike.