

GENDER-BASED CYBER VIOLENCE: A STUDY OF LEGAL REMEDIES AND JUDICIAL RESPONSES IN INDIA

MD JIYAUDDIN^{1*} AND DEBAMOY PAL¹

Gender-Based Cybercrime poses the biggest danger to the growing Digital Ecosystem in India. Unfortunately, females, girls, and others who do not conform to gender normativity are victimized at much larger rates for the aspects of Online Harassment, Stalking, Impersonation, File Abuse through Intimate Images and Coercion within the Digital Space. India passed the DPDP Act 2023 and its rules in 2025 will be the formalisation of this Act into the Indian Legal Framework. The DPDP Rules will also create additional scope for legal interpretations of Gender Based Cyber Crimes from a gendered perspective under the newly re-instating structure of the Indian Cybercrime Law BNS by amending the sections of the IT Act 2000 to include a new intermediary and Digital Media Ethics Code as established per the IT Rules of 2021, ultimately culminating in the newly established DPDP Act. The authors explore how the Indian Judiciary, so far, is demonstrating the expansion of the scope of Judicial Protection available to Victims of Gender Based Cyber Crime and subsequently how it is recommending establishing a Minimum Threshold of Digital Justice for Victims within the Indian Jurisdiction.

Introduction

As the world moves further and further into a digital age, there is continuous change in how we interact with one another socially, how much involvement we have in our daily lives and the various ways we can access information through technological means. The continued growth of the internet, inexpensive smart phones and the various social media sites that now exist have created a digital world for everyone to use in their public and private life. With these new changes, there have been new and more complicated forms of suffering created through these advancements, especially for women, girls and gender minorities¹. Cybercrime based on gender is one of the fastest-growing concerns in the new digital world of India. Many who have already experienced structural inequalities in the offline world are also the most likely to be victimized by acts of cybercrime including

online stalker, impersonation, intimate image abuse, cyber harassment or digital coercion². Technology is a driving force of violence within our society. The Criminal Justice System of India has gone through a major change since 2021 with the creation of the Bharatiya Nyaya Sanhita (BNS) which replaces the earlier British Indian Penal Code. The current BNS includes many features of crimes committed using information technology, such as stalking, sexual harassment, voyeurism, and intimidation, although some of these terms are not defined in the legislation itself. Due to the rapid rise of deep fake technology and encrypted online communications, investigating cybercrimes has become increasingly complicated by increasingly complex regulatory frameworks and a growing number of legal issues being created in the process of regulating these issues. This research will provide a comprehensive analysis of what is referred to as Gender Based Cyber Crimes, the enactment of legislation on this topic under the BNS, the Information Technology Act (IT Act), the Intermediaries Rules, and the Data Protection and Privacy (DPDP) Act, and the relevant relationships

¹ Assistant Professor, School of Law, Brainware University, Kolkata, India.

* Corresponding Author: mjn.law@brainwareuniversity.ac.in

between these statutes, along with case law from the Supreme Court of India, that define the limits of internet security and user protection for users of the internet in India. In addition, this research will demonstrate that the establishment of an Effective Digital Justice System in India is only attainable with a progressive paradigm shift in how to approach the rights of and protections of victims of gender-based cybercrimes, as the basis for the creation of an Integrated Digital Governance Framework in India³.

Nature And Emerging Forms of Gender-Based Cyber Violence

The rise of Gender-Based Cyber Violence across India is leading to a further disintegration of India's Digital Space. Gender-Based Cyber Violence consists of any type of harmful digital activity that is perpetrated against an individual based on gender, and as such, it typically perpetuates current manifestations of inequality that already exist within society⁴. The occurrence of Gender-Based Cyber Violence assists in sustaining and perpetuating the already existing economic inequities that exist between different genders, as it provides the means for a person to perpetrate a harmful act on someone in an anonymous, quick and global manner. The repercussions of Gender-Based Cyber Violence will generally have the most harmful impact on women, girls, and other Genders/identity-diverse groups, who will suffer long-term emotional, social and psychological damage⁵.

Legal Framework In India

Bharatiya Nyaya Sanhita (BNS), 2023: Section 78 - Stalking can refer to either the old-fashioned way of using a phone or computer to track someone's activities or movements, but stalking also includes many different types of cyber-stalking activity carried out through using electronic devices to perpetrate on the target⁶.

Section 74 - Sexual Harassment (Online & Electronic Sexual Harassment/Solicitation and Sexual Communications). Sending/soliciting sexually suggestive communications using any electronic means (IM/e-mails/text messages) constitutes Sexual Harassment.

Section 77 - Voyeurism is an act of capturing an individual without knowledge or consent for sexual pleasure. This may be capturing 'nude' or 'suggestive' images/video/audio without consent.

Section 351 - Criminal Intimidation covers the use of NCII for threatening or intimidation purposes.

Section 356 - Defamation prohibits individuals from making known to any non-employer false statements about another⁷.

Information Technology Act (IT Act), 2000

- Sections 66C/66D - Identity Theft and Cheating by Personation; Identity theft and catfishing [8].
- Section 66E - Violation of Privacy; Photographing/Recording Private Parts Without Consent.
- Sections 67, 67A, and 67B - Distribution and Hosting of Obscene Material; Additional Protection for Child Sexual Abuse Material.

Information Technology Rules (IT Rules), 2021

- Require all intermediaries to establish grievance redressal and display internet-based grievance officers⁹.
- Intermediaries must take down content within a defined timeframe that includes content that violates NCII and sexual violence.

Digital Personal Data Protection (DPDP) Act of 2023 and Regulations of 2025, as per the DPDP, stipulate

- Duties of custodians: Protection of personal data through "reasonable security safeguards"; Limitations on the use of collected personal data; Limiting the number of collected data to the minimum required for fulfilling a specific purpose.
- Operational Functionality of DPDP (2025): Implementation of process duties, mismanagement penalties based on data breaches¹.

Problems and Implementation Gaps

Gender-responsive is not typically provided by many law enforcement agencies, especially those without a dedicated unit for investigating cybercrimes. Many police agencies also lack the necessary training for officers to gather digital evidence, resulting in delays in the collection and processing of digital evidence for criminal investigations, and thus compounding victims' trauma. Most published studies and practitioner opinion justifies the assertion that there are still few successful prosecutions of online gender-based crimes, and that enforcement responses to such crimes are inconsistent or inadequate in many countries¹⁰. Jurisprudence regarding NCII produced by judges can be helpful; however, there is a need for a more standardized approach to addressing instances of NCII as a result of the use of statutory clarity⁹.

Conclusion

Rapidly Rising Gender-Based Online Violence (GBOV) in India is causing harm to Women and Gender Minority (LGBTQ) populations by reducing Their Rights to Respect, Dignity, and Autonomy. Increasing Availability of Digital Platforms has led to a corresponding Increase in the Number of Incidents of Digital Harassment, Digital Stalking, Doxxing and Image Technical Abuse which Serve to Increase the Offline Gender Disparities that Exist. Laws for Legal Recourse Exist in the IT Act of 2000, the Drafted Bharatiya Nyaya Sanhita and the Data Protection and Privacy Bill of 2023; however, there are still challenges to Effective Implementation due to constant Evolution of Cyber Violence and Lack of Systems of Institutional Support and Capacity to Effectively Address Cyber Violence. The establishment of an Empowered Environment for Survivors of Sexual Assault (Victims of Cyber Violence) will depend upon Strengthening the Enforcement of Existing Judgments, Creation of Survivor Centric Systems (Victim Focused), Sensitivity and Empathy of Judicial

Officers and Creation of Enhanced Technology Solutions. □

References

1. B. N. Ray, *Int. J. Cyber Criminol.* **11**, 23–39 (2017).
2. S. Henry and A. Powell, *Violence Against Women* **21**, 617–638 (2015).
3. A. McGlynn, E. Rackley, and R. Houghton, *J. Law Criminol.* **58**, 26–45 (2017).
4. N. K. Sharma and S. Chatterjee, *J. Indian Law Rev.* **4**, 112–130 (2020).
4. P. Duggal, *Comput. Law Secur. Rev.* **34**, 102–115 (2018).
5. S. Singh, *Indian J. Gender Stud.* **27**, 45–63 (2020).
6. M. Tripathi and R. Gupta, *Int. J. Info. Sec.* **19**, 211–229 (2020).
7. S. R. Sharma, *Int. J. Law Policy Rev.* **9**, 51–66 (2020).
8. P. Duggal, *Cyber Security Law* (Routledge, New Delhi, 2021), pp. 205–225.
9. N. K. Sethi, *Women and Cybercrime* (Sage, New Delhi, 2019).
10. T. Solove and D. Citron, *Hate Crimes in Cyberspace* (Harvard University Press, Cambridge, 2014).