International Journal for Multidisciplinary Research (IJFMR)
E-ISSN: 2582-2160 ● Website: www.ijfmr.com ● Email: editor@ijfmr.com

The Role of Law in Combatting Gender-Based Violence on Social Media and Online Platforms

Nusrat Ali Rizvi

Assistant Professor, Govt. Law College, Gwalior, M.P.

Abstract

The advent of digital platforms has revolutionized communication, but it has also introduced new dimensions of gender-based violence posing significant challenges for legal frameworks worldwide. This study critically discusses at the intersection of digital platforms and gender-based violence, exploring the complexities and legal implications within this context. The study points to the different forms of gender-based violence manifested in the digital environment, which includes cyberstalking, online harassment, and non-consensual dissemination of intimate images. It emphasizes how these violations are so deep-rooted that they have reached every nook and corner, transcended geographical boundaries and affected individuals regardless of their location. Through a comprehensive analysis of existing legal frameworks, the article evaluates the effectiveness of current laws in addressing digital gender-based violence. It identifies gaps and inconsistencies in legal provisions, highlighting the challenges faced by victims in seeking justice. The study also explores the role of digital platforms in perpetuating or mitigating gender-based violence, examining their policies, enforcement mechanisms, and accountability measures. This study further highlights that the fight against digital gender-based violence requires multi-faceted approaches, emphasizing stronger legal protection, greater platform accountability, and increased public awareness. It pushes for the incorporation of international standards and cooperation across nations to more effectively address transnational digital gender-based violence. The article ends with policy recommendations that will enhance legal responses to digital gender-based violence, making the online environment safer, and ensuring justice for victims. This Article advocates for more holistic and victim-centred policies that are grounded in human rights principles to deal with the increasingly alarming scourge of online gender-based violence.

Keywords: Violence, Digital platforms, Gender, Mechanisms, Communication, Policy.

1. Introduction

India, with this rapidly growing Internet user base, has seen growth in online harassment, cyber stalking, revenge porn, and every other form of digital gender-based violence. It is reported by the National Crime Records Bureau, NCRB[1], that, between 2018 and 2020, cybercrimes against women registered a 32% increase in India. So, while offering a platform to express oneself in social media sites, it can also be referred to as places where misogyny, hate speech, and even targeted abuse get bred. Internet anonymity emboldens the offenders and hampers victims in getting redress. Here, law is dually instrumental. First, in

[1] Manral, M.S. (2023) 24% rise in cybercrime in 2022, 11% surge in economic offences: NCRB report, The Indian Express. Available at: https://indianexpress.com/article/india/rise-cybercrime-2022-economic-offences-ncrb-report-9053882/ (Last visited on 06 February 2025).

acting as a deterrent for prospective offenders; and second, to give justice to and rehabilitate victims. Online gender-based violence is not at all a recent issue. Online gender-based violence in India can be understood better through the context of legislative responses made to counter such an emergent trend by Indian jurisprudence. The Information Technology Act, 2000[2], and the subsequent amendments thereof, provide the legal framework for dealing with cybercrimes. Among these is the violation of privacy through capturing and disseminating images without permission under Section 66E of the IT Act, and Section 67 that deals with the publication or transmission of obscene material in electronic form (Ministry of Electronics and Information Technology, 2008). Additionally, the Criminal Law (Amendment) Act, 2013, introduced provisions to address sexual harassment and stalking, both offline and online. These legal provisions reflect an acknowledgment of the evolving nature of gender-based violence in the digital age. However, the effectiveness of these laws is often hindered by challenges in implementation. One major issue is the underreporting of online gender-based violence due to social stigma, fear of retaliation, and lack of awareness about legal remedies. Moreover, the enforcement of cyber laws in India is hampered by inadequate training of law enforcement officials, jurisdictional complexities, and the slow pace of the judicial process. The absence of a gender-sensitive approach in dealing with the cybercrime case compounds the problem further, often leading to victim-blaming and secondary trauma. For example, the study conducted by the Internet Freedom Foundation shows that most women fear to report online abuse because police and law enforcement agencies trivialize online abuse issues. Another critical issue here is the role of social media platforms themselves. Platforms like Facebook, Twitter, and Instagram have community guidelines and reporting mechanisms, though the enforcement is extremely inconsistent and inadequately done. Recently, the government of India has made a new law called the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021[3] that will hold the intermediaries responsible for the content available on the social media platforms, but there has been a lot of criticism that this will bring over-censorship and curtail freedom of expression. Combating gender-based violence on social media and other online platforms calls for a multifaceted strategy that includes improvement of the legal framework, enhanced enforcement mechanisms, and collaboration among the government, civil society, and technology companies. Public awareness campaigns and digital literacy programs would help users operate in online spaces safely and report abuse. Further, the transnational feature of online platforms automatically opens up jurisdictional challenges, as content hosted in outside India servers may fall beyond the Indian law book. The challenges raised above necessitate a holistic and comprehensive framework to frame a law that takes into consideration the specifics of online gender-based violence but ensures robust implementation mechanisms. In the Indian scenario where social media usage is rapidly growing, there is a pressing need to balance what the regulation of harmful contents calls for with the basic liberties of freedom of speech and expression or privacy. At a time when India is facing both challenges of deep-entrenched gender inequalities and the rapid digitization of society, it must adapt a legal system that is responsive, inclusive, and forward-looking. By addressing the gaps in existing laws, enhancing enforcement mechanisms, and fostering collaboration among stakeholders, However, legal measures alone are not sufficient; they must be complemented by broader societal efforts to promote gender equality and challenge the norms that enable violence. Only through a multifaceted and

[2] The Information Technology Act, 2000 (Act 21 of 2000).
[3] Ministry of Electronics and Information Technology, Intermediary Guidelines and Digital Media Ethics Code, 2021

collaborative approach can we hope to eradicate gender-based violence in all its forms, both online and offline.

2. Review of Literature

Gender-based violence on social media and online platforms has emerged as a significant concern in India, with the proliferation of digital technologies and increased internet penetration. The anonymity and reach of online spaces have exacerbated issues such as cyberstalking, online harassment, revenge porn, and hate speech, disproportionately affecting women and marginalized genders. This literature review examines the role of law in addressing Gender-based violence in the Indian context, highlighting legal frameworks, challenges, and recommendations for effective intervention. India has enacted several laws to combat online Gender-based violence, including the Information Technology Act, 2000 (IT Act), and its amendments, which criminalize cyber offenses such as cyberbullying, identity theft, and the dissemination of obscene material. Section 66A of the IT Act, though struck down by the Supreme Court in 2015 for being vague and unconstitutional, was initially aimed at regulating offensive online communication. The Protection of Women from Domestic Violence Act, 2005[4], and the Bhartiya Nyaya Sanhita (BNS)[5] provisions, such as Section 78 (stalking) and Section 79 (insulting the modesty of a woman), also provide legal recourse for victims of online harassment. However, scholars like Dhir (2019)[6] opine that such laws usually do not address the specifics of online Gender-based violence because they were not tailored for the virtual world. A major legislation after the Nirbhaya case was the Criminal Law (Amendment) Act of 2013. Still, it is not implemented due to issues such as lack of knowledge among people regarding awareness of such crimes, underreporting, and judicial slowness. Varghese and Kumar (2020)[7] also researched on the same theme and presented a clear indication of the lack of digital literacy in law enforcement agencies, which bars effective investigation and prosecution of cybercrimes. Moreover, the absence of a gender-sensitive approach in legal frameworks reveals victim-blaming and secondary trauma for survivors. This only adds to the problem, as such platforms operate according to global policies that might not consider Indian legal standards. In fact, scholars like Singh and Tripathi argued in 2021 that there is an urgent need for tech companies to be more accountable for local laws and quick removal of such contents. The draft Personal Data Protection Bill, 2019, and the proposed Digital India Act aim to address these gaps by introducing data privacy regulations and enhancing online safety. However, concerns remain about the potential misuse of these laws to curtail freedom of expression. Civil society organizations and activists have played a crucial role in advocating for stronger legal protections and raising awareness about online Gender-based violence. Campaigns like "MeToo" have brought forth the issue of digital harassment and compelled lawmakers to respond to this. However, according to Ghosh and Sharma, 2022, the interlinkage of caste, class, and gender will further increase vulnerabilities in most instances and thus call for an inclusive approach by law. where India has led in legislation against online gender-based violence, the gaps remain huge in terms of implementation, awareness, and inclusivity. Future research should focus on the development of gender-sensitive legal frameworks, digital literacy, and collaboration among stakeholders toward a safer cyberspace for all.

[4] The Criminal Law (Amendment) Act, 2013 (Act 13 of 2013).
[5] Bharatiya Nyaya Sanhita, 2023 (45 of 2023).
[6] A. Dhir, Cyber Law in India: A Critical Analysis 23 (Oxford University Press 2019).
[7] Sesha Kethineni, Murugesan Srinivasan & Suman Kakar, Combating Violence against Women in India: Nari Adalats and Gender-Based Justice, 26 Women & Criminal Justice 281 (2016).

3. Purpose of Study

The purpose of this study is to explore the role played by the law in dealing with and mitigating gender-based violence in the digital sphere, focusing particularly on the Indian context. This research will critically assess the current Indian legal framework that was conceptualized to tackle online gender-based violence. This includes examining the efficacy of laws such as the Information Technology Act, 2000, the Indian Penal Code (IPC), and recent amendments like the IT (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021. The study aims to assess whether these legal provisions are sufficient to address the unique challenges posed by online platforms, including the anonymity of perpetrators, the cross-jurisdictional nature of the internet, and the rapid dissemination of harmful content. Furthermore, it will also look into the mechanisms of enforcing these laws. This includes, among others, the role played by law enforcement agencies, the judiciary, and social media in ensuring accountability and justice for the victims. One of the objectives of the research is to focus on the existing gaps and inadequacies within the legal framework. The study also aims to provide actionable recommendations for policymakers, legal practitioners, and civil society organizations to strengthen the legal response to online gender-based violence. This includes advocating for gender-sensitive legislation, improving access to justice for survivors, and promoting digital literacy to empower users to navigate online spaces safely.

4. Methodology

The research methodology employed is primarily doctrinal, relying on legal texts, judicial precedents, legislative frameworks, and policy documents.

Primary Sources: The research examines constitutional provisions, statutes, rules, and regulations governing cyber laws and gender justice in India. Apart from this, relevant Supreme Court and High Court judgments interpreting legal provisions related to online gender-based violence will also be studied.

Secondary Sources: The research further covers academic literature, reports of national and international organizations and policy papers on digital safety and gender-based violence. Secondary sources like legal articles, Newspaper and Magazine Articles, Social site, Internet websites will be covered to analyse in detail how the law works towards curbing gender-based violence on digital platforms in India.

5. Understanding Gender-Based Violence on Digital Platforms

Gender-based violence on digital platforms refers to harmful acts directed at individuals based on their gender, facilitated through online technologies. This form of violence disproportionately affects women, girls, and gender-diverse individuals, taking various forms such as cyberstalking, online harassment, doxxing, non-consensual sharing of intimate images, and deepfake abuse.

5.1 Definition and Types of Digital Gender based violence

Digital Gender-Based Violence describes harmful actions that are strategically targeted at people because of their gender and facilitated through digital platforms such as social media, messaging apps, email, and other online spaces. Threats, harassment, non-consensual sharing of intimate images, and other forms of abuse that aim to control, shame, or harm individuals, especially women and marginalized genders, are all examples.

Types of Digital Gender-Based Violence[8]

1. **Cyber stalking –** The recurrent use of internet tools to surveil, bully, or blackmail a person. This leads to fear or intimidation.
2. **Online harassment –** The recurrence of hate mails, threats, or insults with the intention to intimidate someone through their gender.
3. **Doxxing** – Public broadcasting of private and personal information including home address or phone number meant to intimidate an individual.
4. **Non-Consensual Sharing of Intimate Images (Revenge Porn) –** Distributing private, sexual content without consent, often as an act of revenge or coercion.
5. **Deepfake Abuse**[9] **–** Using AI to create fake explicit images or videos of someone without their consent.
6. **Sexual Exploitation and Grooming –** Coercing or manipulating individuals, especially minors, into sexual activities online.
7. **Impersonation and Identity Theft –** Creating fake profiles or using someone's identity to defraud, harass, or spread false information.
8. **Misogynistic Hate Speech –** Spreading sexist or misogynistic content that incites violence or discrimination against a particular gender.
9. **Trolling and Cyberbullying –** Posting offensive, provocative, or degrading comments aimed at humiliating or discrediting individuals.
10. **Technology-Facilitated Coercive Control –** Using digital tools to monitor or control someone's online activity, often in abusive relationships.

In India, these types of abuse are highly prevalent and directed towards women mainly for expressing an opinion, joining public discourse or even for merely existing online. A 2020 report of the Cyber Peace Foundation indicated that 76 percent of women have experienced online harassment in India and therefore it sets out the size of the issue.

5.2 Prevalence and Impact of Digital gender-based violence in India

1. **Cyberbullying and Online Harassment:** Women and girls in India are disproportionately targeted by online harassment, including cyberstalking, trolling, and abusive messages. A 2020 study by the Internet Freedom Foundation (IFF) found that 60% of women internet users in India reported experiencing some form of online harassment. According to the National Crime Records Bureau (NCRB) 2021 report, cybercrimes against women, including cyberstalking and bullying, increased by 36% from the previous year. According to the annual report of the National Crime Records Bureau (NCRB) released, crimes against women rose 4% in 2022 compared to 2021. The report said 4,45,256 cases of crime against women were registered in 2022, an increase of 4% compared to 4,28,278 in 2021[10].
2. **Non-Consensual Sharing of Intimate Images:** The non-consensual sharing of intimate images, often referred to as "revenge porn," is a growing concern. A 2019 report by the Cyber Peace Foundation highlighted that 90% of victims of non-consensual pornography in India are women.

[8] Smitee Kumari & Amit Chawla, Role of Media in Portraying Gender Biasness in Indian Politics: A Review Based Study, 10 International journals of science and research 12(2023).
[9] Sarkar, S. (2023). Women survivors' experiences of and responses to technology-facilitated sexual violence. https://doi.org/10.5204/thesis.eprints.242462.
[10] National Crime Records Bureau (NCRB). (2021), Crime in India 2020: Statistics.

3. **Social media: Sexual Harassment:** A 2021 survey by Amnesty International India found that 23% of women in India reported having experienced online abuse or harassment on platforms such as Twitter, often involving gendered slurs and threats of sexual violence.
4. **Victimhood of the Marginalized:** Women in the marginalized Dalit, Muslim, and LGBTQ+ communities face cumulative forms of digital violence. For example, Dalit women often receive casteist slurs and threats on social media platforms. This has been noted by Equality Now in its 2022 report on Digital Gender-Based Violence.

Impact of Digital Gender-Based Violence

1. **Psychological and Emotional Trauma:** Victims of DGBV often experience anxiety, depression, and fear. A study by the Digital Empowerment Foundation (2021) found that 70% of women who faced online harassment reported a decline in their mental health.
2. **Chilling Effect on Freedom of Expression:** Many women self-censor or withdraw from online spaces due to fear of harassment. A 2020 report by UNESCO noted that 30% of women in India reduced their online presence after experiencing abuse.
3. **Social and Professional Consequences:** DGBV can lead to social ostracization, damage to reputation, and even loss of employment. For example, women in public-facing roles, such as journalists and activists, are often targeted to silence their voices.
4. **Legal and Institutional Challenges**: Despite laws like Section 66E of the Information Technology Act (2008) and the Criminal Law (Amendment) Act (2013), enforcement remains weak. Many victims face barriers in reporting due to stigma, lack of awareness, and inadequate support systems.

5.3 Case Studies and Examples

Case Study 1: Online Harassment and Cyberstalking

For example, in 2017, a woman in Delhi said she was being stalked and harassed on the internet by a man who had obtained her contact details from a mutual friend. The man sent her unsolicited explicit messages, created fake social media profiles to defame her, and threatened to share her private photos online. Despite filing a complaint under Section 354D (stalking) of the Indian Penal Code (IPC) and the Information Technology (IT) Act, the case faced delays due to inadequate cybercrime investigation mechanisms. This case highlights the challenges women face in seeking justice for cyberstalking and online harassment. The lack of awareness about legal remedies and the slow judicial process often discourages victims from pursuing cases.

Case Study 2: Non-Consensual Sharing of Intimate Images (Revenge Porn)

Example: In 2019, a college student from Mumbai became a victim of revenge porn when her ex-boyfriend uploaded intimate images of her on multiple pornographic websites without her consent. The images went viral, leading to severe emotional distress and social ostracization. The victim filed a complaint under Section 66E (violation of privacy) and Section 67A (publishing sexually explicit material) of the IT Act. However, the images continued to circulate online due to the lack of effective content removal mechanisms. This case underscores the need for stronger enforcement of laws and better cooperation between law enforcement agencies and tech companies to remove non-consensual intimate content promptly.

Case Study 3: Trolling and Hate Speech Against Women Journalists

Example: In 2021, Rana Ayyub, a prominent Indian journalist, faced relentless online abuse, including rape threats and communal slurs, after she criticized the government's handling of a particular issue. The abuse was amplified by coordinated trolling campaigns on Twitter and other platforms. Despite reporting

the abuse to the platforms and filing police complaints, the perpetrators often remained anonymous or faced minimal consequences. This case illustrates how women in public roles, particularly journalists and activists, are targeted with gendered hate speech and threats to silence their voices. The anonymity provided by digital platforms often emboldens perpetrators. Case Study

4: Online Sexual Exploitation of Minors

Example: In 2020, a nationwide investigation uncovered a network of online predators targeting minor girls through social media platforms like Instagram and Facebook. The perpetrators posed as teenage boys to gain the trust of their victims, coerced them into sharing explicit images, and later blackmailed them for money or more content. The case led to the arrest of several individuals under the Protection of Children from Sexual Offences (POCSO) Act and the IT Act. This case highlights the vulnerability of minors to online sexual exploitation and the need for greater awareness and preventive measures, including digital literacy programs for children and parents.

Case Study 5: Gender-Based Hate Speech on Social Media

For instance, in 2022, a Dalit woman activist was hit with a barrage of casteist and sexist slurs on Twitter after speaking up against caste-based discrimination. The abuse came with sexual threats along with the derogatory remarks over her identity. She reported the incidents, but the action from the side of the platform was slow, and most abusive accounts were left active. This case demonstrates the intersectionality of digital GBV, where gender-based violence is compounded by caste, class, or religious identities. It also highlights the inadequacy of social media platforms in addressing hate speech effectively. 6. Legal Frameworks Addressing Digital Gender based violence in India

India has developed a legal framework that combines existing laws with specific provisions for digital crimes. Gender-based violence on social media and online platforms has emerged as a significant concern in India, with the proliferation of digital technologies and internet access. Women and marginalized genders often face harassment, cyberstalking, non-consensual sharing of intimate images, and hate speech online. The Indian legal framework has evolved to address these challenges, but gaps remain in effectively combating gender-based violence in the digital sphere. This analysis evaluates the legal provisions in India concerning online gender-based violence, effectiveness, and the challenges in their implementation.

6. Important Legal Frameworks Addressing Digital Gender-based Violence in India

1. **Information Technology Act, 2000 (IT Act):** The IT Act is the primary legislation for cybercrimes in India. It contains provisions that address digital gender-based violence:

- **Section 66E:** Penalizes the violation of privacy by capturing, publishing, or transmitting images of a person's private areas without consent. Punishment includes imprisonment up to three years or a fine of up to ₹2 lakh.
- **Section 67:** It prohibits the publication or transmission of obscene material in electronic form. This even includes the dissemination of explicit content without consent. The punishment ranges from imprisonment for up to three years and fine up to ₹5 lakh in case of first conviction.
- **Section 67A:** It targets the specific offense of publication or transmission of sexually explicit material. The punishment extends to imprisonment for up to five years and a fine of up to ₹10 lakh.
- **Section 67B:** Addresses child pornography and sexually explicit content involving children, with stringent penalties.

2. **Bhartiya Nyaya Sanhita, 2023**

Several sections of the BNS are used to prosecute digital gender-based violence which are as follows:

- **Section 75 BNS:** Defines sexual harassment, including making sexually coloured remarks or showing pornography. Punishment includes imprisonment up to three years or a fine.
- **Section 78 BNS**: Criminalizes stalking, including cyberstalking. Punishment includes imprisonment up to three years for the first offense and up to five years for subsequent offenses.
- **Section 356 BNS:** Address defamation, which can be applied to cases of online character assassination or false accusations.
- **Section 79 BNS:** Penalizes words, gestures, or acts intended to insult the modesty of a woman, including online harassment.

3. Protection of Children from Sexual Offences (POCSO) Act, 2012

The POCSO Act addresses sexual offenses against children, including those committed online. It criminalizes the use of digital platforms to exploit children sexually, with stringent penalties for offenders.

Criminal Law (Amendment) Act, 2013

This amendment introduced stricter provisions for sexual offenses, including those committed online. It expanded the definition of rape and sexual assault to include acts facilitated by digital means.

Indecent Representation of Women (Prohibition) Act, 1986

This Act prohibits indecent representation of women through advertisements, publications, or other means, including digital platforms. Violations can result in imprisonment up to two years and fines.

The Digital Personal Data Protection Act, 2023

Though basically a data protection Act, the implications of the Act are important for Digital Gender-based violence by regulating the collection, storage, and processing of personal data and aims to prevent unauthorized use of data that might be used to harass or exploit. The Government of India has also introduced regulatory mechanisms such as the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021, mandating social media platforms to take proactive measures against harmful content. These rules require intermediaries to remove offensive content within 24 hours upon receiving complaints related to nudity, morphed images, or gender-based abuse.

Despite these legal safeguards, challenges remain in effective enforcement due to lack of awareness, underreporting, and jurisdictional issues. Strengthening digital literacy, sensitizing law enforcement agencies, and encouraging swift legal recourse are essential steps toward a safer online environment for women.

7. Gaps and Inconsistencies in Current Legal Frameworks

The rise of social media and online platforms has exacerbated gender-based violence in digital spaces, including cyberstalking, online harassment, doxing, and non-consensual image sharing. Despite India's legal provisions to address such issues, gaps and inconsistencies persist, undermining the effectiveness of legal recourse for victims.

Gaps in Legal Provisions

India has several laws that indirectly address online gender-based violence, including the Information Technology (IT) Act, 2000, BNS, 2023, and the Protection of Women from Domestic Violence Act, 2005. However, none comprehensively cover the evolving nature of gender-based cybercrimes.

- Narrow Scope of the IT Act, 2000: Although Section 66E penalizes violation of privacy and Section 67 criminalizes obscene content transmission, such provisions do not explicitly address gendered cyber violence like deepfake pornography or cyberflashing (IT Act, 2000). The lack of specific offenses targeting gendered abuse leaves victims vulnerable.

- Inadequate BNS Provisions: Sections 78 (stalking), 356 (criminal defamation), and 79 (word, gesture, or act intended to insult the modesty of a woman) are used to prosecute online Gender based violence (BNS 2023). However, these sections are often ineffective due to challenges in enforcement and the reluctance of law enforcement agencies to take online offenses seriously.
- Jurisdictional and Enforcement Challenges: Digital crimes transcend geographical boundaries, making jurisdiction a major hurdle. Online platforms operate internationally, and cooperation between Indian law enforcement and global tech companies remains inconsistent, often resulting in delayed action or non-compliance with takedown requests.

Inconsistencies in Implementation

- **Lack of Clear Definition of Online Gender Based Violence:** A legal definition does not exist in the case of online gender-based violence, resulting in inconsistent laws and judicial discretion, which, at times, leads to cases being underreported and dismissed.
- **Delayed Legal Proceedings:** Victims of online gender-based violence often face prolonged legal battles, discouraging them from seeking justice. The lack of specialized cybercrime units across all states further exacerbates the delay in addressing complaints.
- **Platform Accountability:** While the IT (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021, impose due diligence obligations on social media platforms, their implementation remains inconsistent. Many platforms fail to respond adequately to complaints of online harassment, often citing freedom of speech as a defence.

Despite these legal gap and inconsistencies, several other challenges hinder the effective combatting of online gender-based violence in India. First, the lack of awareness among women about their legal rights and the mechanisms for reporting online abuse is a significant barrier. Many victims are unaware of the existence of cyber cells or the process of filing complaints under the IT Act or IPC. Second, the anonymity afforded by social media platforms complicates the identification and prosecution of offenders. Perpetrators often use fake accounts or virtual private networks (VPNs) to evade detection. While Section 69A of the IT Act allows the government to block content and issue takedown orders, the process is often slow and bureaucratic. Third, the burden of proof and the stigma associated with reporting online Gender based violence deter victims from seeking legal recourse. It forces women who experience cybercrime to remain silent due to victim-blaming and social isolation. Moreover, the law enforcement of existing laws is often inconsistent. Police officers lack proper training in dealing with cybercrime cases, leading to deficient investigations and low conviction rates. Further, the judiciary is overburdened, and cases take a lot of time to be resolved.

8. Recommendations for Strengthening the Legal Framework:

To effectively combat online gender-based violence, India's legal framework must be strengthened and implemented more effectively.

First, there is a need for specialized cybercrime units with trained personnel to handle cases of online harassment. Second, awareness campaigns should be conducted to educate women about their legal rights and the reporting mechanisms available to them. Third, social media platforms must be held accountable for enforcing their community guidelines and providing timely redressal to victims. Collaboration between the government, civil society, and tech companies is essential to develop effective strategies for combating online gender-based violence. Finally, the legal framework should be updated to address emerging forms

of online abuse, such as deepfakes and doxxing. A comprehensive law specifically targeting online gender-based violence, with clear definitions and stringent penalties, would provide a stronger deterrent.

9. The Role of Indian Judiciary in Combatting Gender-Based Violence on Social Media and Online Platforms

In India, the judiciary has addressed the role of law in combating gender-based violence on social media and online platforms through several notable cases and pronouncements:

1. Suhas Katti v. Tamil Nadu (2004)

This case marked India's first conviction under Section 67 of the Information Technology Act, 2000, which penalizes the publication or transmission of obscene material in electronic form. The accused was found guilty of posting obscene, defamatory, and harassing messages about a woman in a Yahoo message group, leading to his conviction. This judgment underscored the applicability of existing laws to address online harassment and set a precedent for future cases involving cyber harassment.

2. Bulli Bai Case (2022)

In this incident, photos of prominent Muslim women were uploaded without consent on the "Bulli Bai" app, where they were subjected to a mock auction.

The app was hosted on the platform GitHub. Mumbai Police arrested the individuals who developed the app. They charged those involved with the various sections of the Indian Penal Code, which included provocative acts for promoting enmity between groups and insulting the modesty of a woman. This case shows that the judiciary has understood the depth of online gender-based harassment as well as the need to bring the online platform accountable.

3. Aparna Bhat v. State of Madhya Pradesh (2021) The Supreme Court of India addressed entrenched patriarchal and misogynistic attitudes in judicial proceedings related to gender-based violence. The Court held that judges must not make any comments that reflect gender stereotypes or question the character of survivors. This pronouncement, although unrelated to online platforms, reinforces the judiciary's commitment to combating gender-based violence and ensuring sensitivity in such cases.

4. Shreya Singhal v. Union of India (2015) The Cout Declared Section 66A of the IT Act unconstitutional but recommended that the government should have formulated better laws to curb online harassment.

5. Prajwala Case (2018) Supreme Court of India ordered internet companies and law enforcement agencies to take stringent measures against online sexual harassment.

6. Facebook v. Union of India (2020) The Court Examined intermediary liability and the need for platforms to proactively address online violence.

The Supreme Court noted the global efforts to hold social media platforms accountable for the spread of disruptive messages and hate speech. The Court highlighted the need for such platforms to be responsible, given their potential to influence public opinion. This observation underscores the judiciary's recognition of the role of social media in perpetuating gender-based violence and the necessity for regulatory measures. These judgments and orders illustrate the Indian judiciary's changing stance in dealing with gender-based violence in the cyber world, by stressing the implementation of existing law, the importance of judicial processes being sensitive to the issues at hand, and the responsibility of online service providers.

10: Conclusion

Law plays a critical but developing role in the prevention of gender-based violence on social media and online platforms in India. While legislative frameworks such as the Information Technology (IT) Act,

2000, Bhartiya Nyaya Sanhita, 2023 (BNS) and recent amendments like the IT Rules, 2021 provide a foundation for addressing online abuse, enforcement remains a challenge. The intersection of technology and gender justice demands stronger legal provisions, better implementation, and sensitization among law enforcement agencies. Further, judicial interventions, such as the Supreme Court's stance in Shreya Singhal v. Union of India (2015), which struck down Section 66A of the IT Act for its ambiguity, reflect the ongoing efforts to balance free speech and protection against online harassment. However, online gender-based violence continues to persist due to anonymity, lack of digital literacy, and inadequate reporting mechanisms. This includes strengthening cyber laws with a gender-sensitive approach, improving reporting mechanisms, and fostering collaborations between law enforcement, social media companies, and civil society organizations to make digital spaces safer. Legislative reforms must be accompanied by digital awareness campaigns and stronger accountability measures for tech platforms. As India moves towards a more digitally inclusive society, addressing online gender-based violence through robust legal frameworks and proactive governance remains an urgent necessity.

References

Books & Journals

1. Dhir, A. (2019), Cyber Law in India: A Critical Analysis. Oxford University Press.
2. Varghese, R., & Kumar, S. (2020), "Challenges in Combating Cyber Violence Against Women in India." Journal of Gender Studies, 29(4), 456-470.
3. Singh, P., & Tripathi, R, (2021). "Social Media and Gender-Based Violence: A Study of Indian Context." Indian Journal of Law and Technology, 17(2), 123-140.
4. Ghosh, S., & Sharma, M, (2022). "Intersectionality and Online Harassment: A Case Study of Indian Women." Feminist Media Studies, 22(3), 567-582.
5. Chami, N. (2021), Platform accountability for gender-based cyber violence: An analysis of the Indian legal-policy landscape & IT for Change.
6. Banerjee, A. (2023), Cyber Violence and Women in India: Legal and Social Responses. Oxford University Press.
7. Chakraborty, S., & Bose, R. (2022), Digital Safety and Gender-Based Cyber Crimes: Indian Perspectives. Cambridge Scholars Publishing.
8. Dhawan, S. (2020), Cybercrime Against Women in India: A Critical Analysis. Journal of Human Rights and Social Work, 5(3), 234-245.
9. Singh, R. (2019), Online Harassment and the Law: A Study of Indian Legal Framework. Indian Journal of Gender Studies, 26(2), 178-195.
10. IMPRI Impact and Policy Research Institute (2024), Ending Online Violence Against Women in India: Calling for an Inclusive, Comprehensive, and Gender-Sensitive Law and Policy Framework.
11. Internet Democracy Project, (2013), "Keeping women safe"? Gender, online harassment and Indian law.
12. Chadha, K. (2021), "Regulating Social Media in India: Balancing Accountability and Freedom." Economic and Political Weekly, 56(25), 18-22.
13. Internet Freedom Foundation, (2021), The Impact of IT Rules 2021 on Digital Rights in India.

Act, Report and Cases

1. National Crime Records Bureau (NCRB). (2021). Crime in India 2020: Statistics.
2. Cyber Peace Foundation. (2020), Online Harassment in India: A Report on the Prevalence and Impact

of Cyber Violence Against Women.
3. National Crime Records Bureau (NCRB) Cyber Crime Report, 2022.
4. United Nations Women Report on Online Gender-Based Violence (2021).
5. Ministry of Electronics and Information Technology, Intermediary Guidelines and Digital Media Ethics Code, 2021.
6. Legal Bites, (2019). Legal Framework on Cyber-Violence Against Women.
7. The Information Technology Act, 2000 (Act 21 of 2000).
8. Bhartiya Nyaya Sanhita, 2023 (45 of 2023).
9. Protection of Children from Sexual Offences Act, 2012.
10. Criminal Law (Amendment) Act, 2013 (Act 13 of 2013).
11. Prajwala vs Union of India (2018) SC 1043.
12. Facebook v. Union of India (2020) SC 2260).
13. Shreya Singhal v. Union of India, (2015) SC 1523