International Journal of Environmental Sciences
ISSN: 2229-7359
Vol. 11 No. 19s, 2025
https://theaspd.com/index.php

Cyberbullying And Gender: An Analysis Of Legal Protections For Women On Social Media

Dr. Neha Gupta[1], Ms. Soyonika Gogoi[2]
[1]Assistant Professor , School of Law , Presidency University , Itgalpur, Rajanukunte, Yelahanka, Bengaluru-560064 (Karnataka State), India , neha.gupt@presidencyuniversity.in
[2]Assistant Professor , School of Law , Presidency University , Itgalpur, Rajanukunte, Yelahanka, Bengaluru-560064 (Karnataka State), India , soyonika.gogoi@presidencyuniversity.in

Abstract
Digital platforms, while promoting equal self-expression, have become spaces for exclusionary and violent behaviours, especially against women and girls. Though both genders can face cyber violence, women are more frequently targeted and suffer greater consequences, including physical, psychological, sexual, or economic harm. Cyber violence against women and girls (CVAWG) is often dismissed as trivial, but it stems from deeply ingrained gender inequality. This form of gender-based violence, perpetuated through digital platforms, reflects broader societal issues, where women's safety and dignity continue to be at risk. Cyberbullying, particularly on social media platforms, has emerged as a critical issue in the digital age, disproportionately affecting women. Gender-based cyberbullying often includes threats of violence, sexual harassment, doxxing, and body shaming, which not only undermine women's mental well-being but also deter their participation in online spaces. Despite the severity of the issue, legal protections for women in the digital sphere remain fragmented and inconsistent across jurisdictions.

This paper analyses the intersection of gender and cyberbullying, concentrating on the unique forms of harassment faced by women online and the legal frameworks in place to protect them. The study evaluates the effectiveness of laws like India's Information Technology Act, 2000, and international frameworks such as the EU's GDPR in addressing cyberbullying. It explores the role of social media companies in regulating harmful content, highlighting enforcement gaps and challenges in holding offenders accountable. By analyzing case law, the paper assesses the adequacy of legal protections and recommends reforms. The researcher concludes that while progress has been made, stronger, gender-sensitive policies and proactive actions by social media platforms are necessary to ensure safer digital spaces for women.

Keywords: *Cyberbullying, Online Harassment, Digital Safety, women, social media safety*

1. INTRODUCTION

Social media platforms have become an indispensable part of our everyday lives in the digital age completely transforming how we communicate, share information and create communities. Covering unprecedented terrains of connection and expression, they transcend geographies and social norms that have existed before. But the same tech that allows for those good things to happen online has also made it easier for new types of harassment and abuse. Of these, cyberbullying is a pervasive behaviour with damaging consequences for women and girls in particular.[1]

One of the challenges threatening the safety and welfare of social media users is cyberbullying which can be broadly described as repeated harm inflicted through digital technologies, mainly using electronic forms to deliberately harass or attack some victims with such aggressions. While individuals of all genders can experience cyber violence, research consistently indicates that women and girls are significantly more vulnerable. They face a higher likelihood of being targeted and are often subjected to severe outcomes, including physical, sexual, emotional, and financial harm.[2] Abuse directed at women and girls in online spaces is often underestimated or regarded as merely a virtual concern. In reality, it constitutes a significant form of gender-based violence, facilitated by digital tools and rooted in the persistent social and structural inequalities

between genders. According to data from the National Crime Records Bureau (NCRB), India witnessed an upward trend in cybercrime cases, including incidents of cyberbullying. In 2021, 52,974 cases were reported nationwide, marking a 5.9% rise from the figures recorded in 2020.[3]

This insidious form of cyberbullying not only demonstrates its pervasiveness but also raises considerable questions about the legal protections that women in particular have online. Online violence targeting women and girls has emerged as a critical concern in the digital age. Tragic incidents, such as the suicide of a young woman in Kerala due to sustained online abuse, expose the severe psychological impact of cyber harassment. Women across the globe whether in Pakistan, Spain, or Peru face a range of digital threats, including cyberstalking, gendered hate speech, image-based abuse and doxxing.[4] These forms of violence extend beyond the screen, discouraging women's online presence and undermining their right to free expression, particularly those engaged in activism, journalism, or politics.

According to a World Bank report, only 30% of the world's economies have enacted laws addressing cyber harassment and even fewer have specific provisions to protect women, children, or persons with disabilities.[5] Civil remedies are rare, and just 12% of women globally are covered under cyber sexual harassment legislation.[6] This gap in legal protection highlights an urgent need for comprehensive, gender-sensitive laws and effective enforcement to safeguard digital spaces. Digital innovation is moving quickly, however, many legal frameworks are not keeping up and attempting to cover gaps in protection that organized criminals can easily penetrate. It is necessary to provide a comprehensive examination of the current legal protections afforded women on social media platforms, evaluating where existing laws and policies stand up well and weaknesses failing them.

This paper examines the legal protections available to women against cyberbullying, with a specific focus on social media. It analyses whether current Indian and global frameworks provide adequate protection and explores how these can be strengthened to reflect the gendered nature of online abuse. In addition, the paper analyses the international frameworks such as the EU's GDPR on cyberbullying. The researcher also explores the role of social media companies in regulating harmful content, highlighting enforcement gaps and challenges in holding offenders accountable.

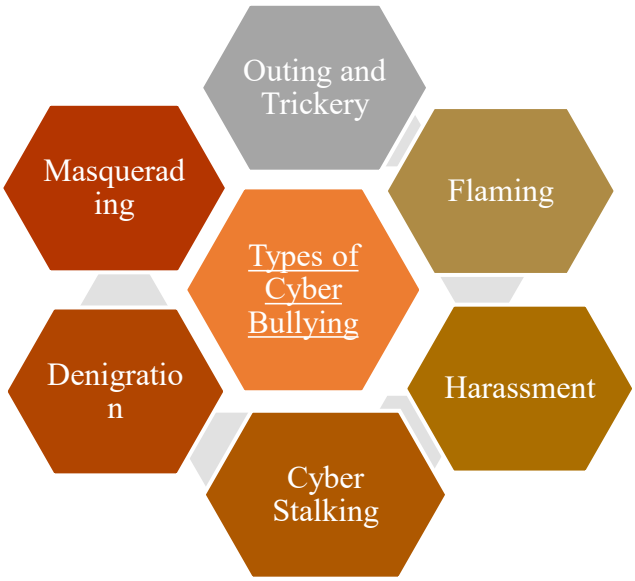
1.1 Types of cyber bullying –

Cyberbullying has become a modern-day crisis, deeply intertwined with the misuse of digital technologies. A significant factor contributing to its growing impact is the general lack of awareness and the absence of strong preventive mechanisms within society. As a result, the number of victims continues to rise steadily. Offenders exploit the anonymity and reach of the internet to engage in acts such as hacking into personal social media accounts, stealing private data, and even assuming false identities. The range of actions available to perpetrators is vast and continually evolving. Cyberbullying manifests in multiple forms, making it a complex and pressing issue in the digital age.[7] Cyberbullying can take on several harmful forms in the digital environment. These include flaming, cyber staling, harassment etc.

The diagram presents seven common forms of cyberbullying. They are -

- Flaming: Posting inflammatory or insulting messages to provoke conflict.
- Harassment: Repeatedly sending offensive or threatening communications.

- Cyberstalking: Persistent monitoring, intimidation, or threats via digital channels.



- Denigration: Spreading false, harmful, or demeaning content about someone.
- Masquerading: Impersonating another person online to send harmful or abusive messages.
- Outing and Trickery: Sharing private or embarrassing information or images without consent.
- Exclusion: Deliberately leaving someone out of an online group or activity.

Together, these categories capture the spectrum of abusive behaviors that can occur in digital environments. These behaviors can cause significant emotional distress and social harm to victims, particularly in environments where support and accountability mechanisms are weak.

1.2 Review of Literature –

1. R. Vasanthi et al. (2024)[8]

This study investigates the emotional and psychological toll of cyberbullying on women, highlighting increased levels of anxiety, depression, and social withdrawal. It emphasizes the lack of awareness and legal literacy as contributing factors to underreporting.

2. Anita Gurumurthy & Nandini Chami (2016)[9]

The authors argue that cyber violence against women in India is structurally rooted in patriarchy and is exacerbated by digital inequality. The study calls for a rights-based and gender-sensitive regulatory approach.

3. UNHRC Special Rapporteur Report (2018)[10]

This report recognizes online abuse as a form of gender-based violence and stresses the responsibility of both states and digital platforms in ensuring online safety for women.

4. World Bank (2022)[11]

In a global assessment, the World Bank's "Women, Business and the Law" initiative identifies gaps in legal frameworks related to cyber harassment, noting that only a fraction of economies provide adequate protections.

1.3 Statement of Problem –

Despite the rapid expansion of digital platforms as tools for self-expression and communication, they have increasingly become spaces where gendered abuse thrives. Women and girls are disproportionately targeted by cyberbullying, experiencing severe psychological, emotional, and sometimes physical harm. This form of

online violence is deeply rooted in systemic gender inequality and often manifests through threats, harassment, doxxing, and sexualised abuse. However, legal frameworks to address such violence remain fragmented, inconsistent and insufficient across national and international jurisdictions. In India, although provisions exist under the Information Technology Act, 2000 and the Indian Penal Code, they lack gender-sensitive perspectives and strong enforcement. Meanwhile, social media platforms continue to operate with vague or inconsistently applied moderation policies, leaving victims vulnerable. Addressing the gaps in both legal protections and platform accountability is essential to ensure that digital spaces are safe, inclusive and equitable for women.

1.4 Scope of the study –

This study focuses on the phenomenon of gender-based cyberbullying, particularly as it affects women in India. It explores how legal frameworks domestic (such as the IT Act, 2000) and international (such as the GDPR) respond to this form of violence. The study also critically examines the role and responsibility of social media platforms in preventing and mitigating cyber harassment. Through doctrinal and case-based analysis, it evaluates the strengths and shortcomings of current legal protections and enforcement mechanisms, with recommendations for reform.

1.5 Objectives of the study –

1. To identify and analyse the specific forms of cyberbullying disproportionately faced by women on digital platforms.
2. To examine the effectiveness and limitations of Indian legal provisions addressing cyberbullying, with a focus on gender justice.
3. To assess relevant international legal instruments and their influence on domestic law and policy.
4. To explore the regulatory responsibilities of social media companies and the effectiveness of their content moderation policies.
5. To propose legal and policy reforms aimed at enhancing gender-sensitive protections in digital spaces.

1.6 Research Questions –

1. What are the specific forms of cyberbullying most commonly directed at women on social media platforms?
2. How adequate are the current legal frameworks in India, particularly the Information Technology Act, 2000, in addressing gender-based cyberbullying?

1.7 Hypothesis –

H1 - What are the specific forms of cyberbullying most commonly directed at women on social media platforms?

H1 - How adequate are the current legal frameworks in India, particularly the Information Technology Act, 2000, in addressing gender-based cyberbullying?

1.8 RESEARCH METHODOLOGY –

This study uses a qualitative doctrinal research method, relying on secondary sources such as statutes, judicial decisions, scholarly articles and international legal instruments. It examines India's legal framework primarily the IT Act, 2000 and the Indian Penal Code alongside international standards like the GDPR and CEDAW to assess how gender-based cyberbullying is addressed. A case-based analysis is also included to evaluate real-life enforcement and legal responses. Additionally, the study reviews social media platform policies to understand their role and accountability in preventing online abuse. This approach supports a critical and comparative understanding of existing gaps and needed reforms.

2. Legal Frameworks And Their Effectiveness In India

India's response to cyberbullying is currently shaped by multiple legal instruments, including the Information Technology Act, 2000, and specific provisions within the Indian Penal Code (IPC), 1860. However, with the recent enactment of the Bharatiya Nyaya Sanhita (BNS) intended to replace the IPC and introduce updated legal principles, it becomes necessary to assess how this new law may strengthen existing safeguards against cyberbullying. This section examines the relevant legal provisions addressing online harassment, considers

the potential impact of the BNS on cybercrime regulation and highlights the ongoing challenges in ensuring comprehensive protection for victims.[12]

2.1 Overview of Relevant Laws

1. Information Technology Act, 2000

Key provisions relevant to cyberbullying include Section 66E, which penalizes the violation of privacy through capturing, publishing, or transmitting images without consent; Section 67, which criminalizes the publication or transmission of obscene material electronically; and Section 72, which addresses breaches of confidentiality and privacy by any person who has secured access to information through unlawful means.[13]

2. Indian Penal Code, 1860

Although the **Indian Penal Code, 1860** predates modern technology, several of its sections are applicable to online harassment. **Section 499** addresses defamation, penalizing the spread of false content intended to damage someone's reputation, an act commonly seen in cyberbullying. **Section 504** covers intentional insult aimed at provoking violence or retaliation, which can occur through threatening or abusive digital messages. **Section 506** pertains to criminal intimidation and includes online threats to a person's safety, reputation, or property.

3. Bharatiya Nyaya Sanhita

The Bharatiya Nyaya Sanhita (BNS), proposed as a modern replacement for the Indian Penal Code, aims to address digital-era crimes more effectively. It introduces clearer legal definitions for online offences like cyber harassment and intimidation, improving enforcement clarity. The BNS also recommends stricter penalties to reflect the seriousness of cyberbullying and to deter offenders. Notably, it emphasizes victim-centric provisions, including access to justice and protection mechanisms. By focusing on the technological dimensions of crime, the BNS seeks to align Indian criminal law with contemporary digital threats.

Despite these legal tools, the current framework lacks specificity when it comes to gendered online abuse. There is no standalone statute dedicated to cyber violence against women. Further, enforcement mechanisms remain limited due to underreporting, inadequate training among law enforcement agencies, and procedural bottlenecks in investigation and prosecution.[14] This gap often leaves victims without timely or effective remedies, perpetuating a cycle of silence and impunity. Strengthening gender-sensitive laws and building institutional capacity are therefore essential steps toward securing safer digital environments for women.

2.2 Recent Judicial Perspective on Cyberbullying in India

In a recent observation, the Supreme Court of India has underlined the growing concern of cyberbullying, particularly its impact on vulnerable groups such as minors. The Court has stressed the necessity for robust enforcement of cyber laws and the deployment of advanced technological tools to curb digital harassment.[15]

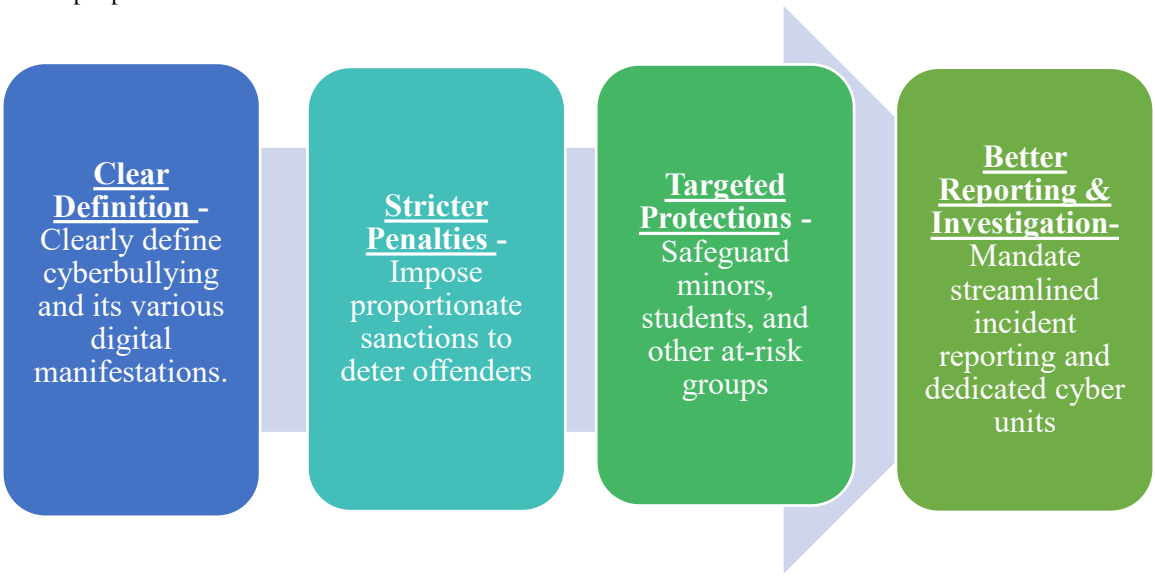
One landmark case in this context is Shreya Singhal v. Union of India[16], where the Supreme Court invalidated Section 66A of the Information Technology Act, 2000, on grounds of vagueness and its potential to infringe on free speech. While the ruling safeguarded fundamental rights, it also recognized the significance of addressing online abuse through precise and constitutionally sound provisions.

2.3 The Need for a Dedicated Cyberbullying Law in India

Although existing laws under the Information Technology Act, 2000 and the Indian Penal Code, 1860 provide some remedies, they fall short of addressing the nuanced and evolving nature of cyberbullying. India lacks a standalone statute that clearly defines cyberbullying, prescribes specific penalties and ensures efficient redressal mechanisms.

The diagram below outlines four essential pillars for an effective cyberbullying law. First, it calls for a precise definition of cyberbullying that covers all forms of online abuse. Second, it mandates proportionate penalties

designed to deter offenders. Third, it emphasizes special protections for vulnerable groups especially minors and students. Fourth, it requires robust reporting and dedicated investigation mechanisms to ensure swift action. Together, these elements form a comprehensive legal framework that safeguards digital rights and holds perpetrators accountable.



3. International Perspectives On Cyberbullying Legislation

The use of international legal instruments is important as the internet and social media platforms are global, and thus such laws determine to a large extent how cyberbullying against women will be responded to globally. Young persons want to know what law they can turn to protect themselves from cyberbullying online: there is no single international treaty establishing such a lawful power, nevertheless, several contain pertinent frameworks and principles. Cyberbullying has become a growing global concern, prompting many nations to establish specific legal responses to tackle online abuse. A review of international legislative trends reveals diverse strategies, ranging from dedicated anti-bullying statutes to broader laws focused on digital safety and harassment. This section examines how different jurisdictions have approached cyberbullying through law, referencing successful legal models, landmark judicial decisions and their relevance to India's ongoing efforts to strengthen its cyber legal framework.

1. United States

In the United States, legal responses to cyberbullying are primarily shaped by individual states rather than federal law. Many states have enacted specific legislation that addresses digital harassment within broader anti-bullying frameworks. For instance, California's Education Code mandates that educational institutions implement policies to prevent and respond to incidents of cyberbullying among students.[17] These policies often include disciplinary measures to hold perpetrators accountable.

A notable judicial precedent in this area is Doe v. Taylor Independent School District[18], where a student faced sustained cyber harassment through emails and social media platforms. The court ruled in favor of the student, affirming that schools bear a constitutional duty to safeguard students from both physical and online abuse. This case reinforced the legal obligation of schools to adopt effective preventive and corrective strategies to ensure a safe learning environment.

2. United Kingdom

The UK addresses cyberbullying within a broader online safety and educational policy framework. Under the Education and Inspections Act 2006, schools are empowered to develop and enforce anti-bullying strategies,

including those targeting online abuse.[19] The law recognizes the evolving nature of bullying and requires schools to intervene proactively.

A significant case in this context is S v. H (2012)[20], where the High Court found that the school failed in its duty of care after a student endured severe cyberbullying, leading to mental health deterioration. The court emphasized the obligation of educational institutions to take timely and appropriate action to protect students from digital harassment.

3. Australia

Australia has adopted both federal and state-level measures to combat cyberbullying. The Criminal Code Amendment (Bullying) Act 2011 criminalizes certain online behaviors that amount to bullying and initiatives like the Safe Schools Program promote inclusive and secure educational environments.[21]

In Khadra v. State of South Australia (2015)[22], the court ruled in favor of a student who suffered physical and emotional distress due to cyberbullying. It was held that schools are responsible for addressing such abuse, even when it occurs outside the physical premises, provided they are aware of the situation. This case affirmed schools' legal responsibility to intervene in instances of digital bullying.

4. European Union

The European Union has made notable progress in regulating online harassment through its comprehensive legal instruments. While the General Data Protection Regulation (GDPR) primarily focuses on protecting personal data, it also contributes indirectly to combating cyberbullying by ensuring individuals' control over their digital identity and enforcing strict standards for the collection, use and dissemination of personal information.[23]

A significant precedent in this area is GC and Others v. M.E. (2019)[24], decided by the European Court of Human Rights. The Court found that a state's failure to shield individuals from persistent harassment, including digital abuse, violated their right to respect for private life under Article 8 of the European Convention on Human Rights. This ruling underscored the duty of member states to establish effective legal remedies against online abuse and harassment.

Examining such international models demonstrates how diverse legal frameworks from dedicated anti-cyberbullying laws to broader digital safety provisions can be effectively enforced to protect victims' rights. As India moves forward with reforms under the Bharatiya Nyaya Sanhita, these global experiences provide meaningful guidance for crafting robust, victim-centric legislation that addresses the complexities of cyberbullying.

4. The Role Of Social Media Platforms In Preventing And Addressing Cyberbullying

Social media platforms have implemented internal policies aimed at curbing digital abuse, including cyberbullying. Despite these efforts, enforcement often remains inconsistent, algorithmically biased, and lacking in transparency. Many platforms prioritize user engagement and content virality over safety, which can exacerbate the spread of harmful material.[25] Content moderation systems frequently overlook cultural nuances, fail to respond adequately to gendered abuse, and offer limited recourse for victims. Women, in particular, face disproportionate levels of abuse on platforms such as X (formerly Twitter), Instagram, and Facebook.

Several incidents illustrate the grave consequences of this regulatory gap. The Bois Locker Room case in India (2020)[26] revealed a private Instagram group where teenage boys shared explicit comments and images of

underage girls without consent. The episode sparked national outrage and raised critical questions about platform accountability, digital literacy and the normalization of online misogyny. In another high-profile example, investigative journalist Rana Ayyub was relentlessly targeted through doxxing, sexualised abuse and coordinated trolling campaigns, often with minimal response from platform moderators.[27] Similarly, climate activist Disha Ravi faced gendered online abuse and threats following her arrest, further highlighting the gendered dimension of digital harassment.[28]

These cases demonstrate that voluntary self-regulation by tech platforms is insufficient. Legal frameworks must enforce timely takedown procedures, implement mandatory transparency reporting and create user-friendly grievance redressal mechanisms. A co-regulatory model, combining statutory oversight with internal platform responsibility, may offer a more balanced and enforceable approach. Without strong legal mandates, social media will continue to be a breeding ground for cyberbullying, particularly against women and minors.

4.1 Gaps and Challenges in the Indian Legal Framework

India's legal response to cyberbullying and online harassment is gradually developing, especially with the introduction of the Bharatiya Nyaya Sanhita and recent updates to the Information Technology Act, 2000. While these reforms mark progress, they fall short of comprehensively addressing the growing complexity of digital abuse. Key challenges remain, including legislative ambiguity, enforcement limitations and deep-rooted socio-cultural obstacles. This section critically examines these persistent gaps and highlights the urgent need for a more coherent, victim-centric legal and institutional approach to combat cyberbullying effectively.

1. **Legislative Inadequacies -** A significant limitation of India's cyber laws lies in the lack of precise legal terminology. Terms like "harassment" or "bullying" are often broadly interpreted due to the absence of specific definitions within the existing statutes. For example, while the Information Technology Act, 2000 includes provisions addressing electronic communication-related offences, it does not clearly define "cyberbullying," resulting in inconsistent application across law enforcement and judicial processes.[29] Additionally, India does not have a dedicated cyberbullying law, unlike several countries that have enacted targeted legislation to address online abuse. Relevant provisions are currently dispersed among multiple legal instruments, such as the Indian Penal Code, the IT Act, and various administrative guidelines related to education.[30] This fragmented framework can confuse victims seeking redress and may discourage them from initiating legal action. Furthermore, the current laws fail to establish victim-oriented safeguards. There is a clear gap in statutory provisions concerning victims' rights, including psychological support, legal aid and access to grievance redress mechanisms.[31] Without institutional support systems such as counselling services or victim advocacy frameworks, survivors often face challenges in both navigating legal proceedings and recovering from the trauma caused by online abuse.

2. **Enforcement Challenges -** One of the critical issues in effectively addressing cyberbullying is the lack of technical expertise and infrastructure within law enforcement. Many officers are not adequately trained to investigate digital crimes and the absence of cyber forensic tools hampers evidence collection and analysis.[32]This often results in weak prosecution and low conviction rates. Additionally, insufficient awareness and sensitivity among officials further limits the impact of existing laws. Cyberbullying is sometimes trivialized, and in certain cases, victim-blaming attitudes may prevent survivors from reporting abuse.[33] Moreover, judicial delays pose another barrier. The slow progression of cases through India's overburdened

courts can prolong victims' trauma and reduce faith in the justice system.[34] Timely justice is essential to ensure that protective laws serve their intended purpose.

3. **Socio-Cultural Barriers** - One of the major obstacles in addressing cyberbullying is the social stigma attached to victims, particularly women. Fear of judgment and reputational damage often discourages individuals from reporting abuse, leading to underreporting and limited legal action against offenders.[35] This isolation perpetuates a culture of silence around digital harassment. Another critical concern is the lack of awareness about legal protections. Many victims especially in rural and semi-urban regions remain unaware of their rights or the procedures to seek redress, which further hinders access to justice.[36] Additionally, the widespread use of social media platforms has intensified cyberbullying. Anonymity, ease of access and rapid content sharing allow perpetrators to act with impunity while making enforcement difficult.[37] These challenges highlight the need for legal reforms, digital literacy programs and victim-support mechanisms tailored to India's socio-technological realities.

4. **Need for Comprehensive Policy Framework** - To effectively address cyberbullying, India requires a unified legal and policy framework that clearly defines offences, outlines accountability for perpetrators and includes robust victim support mechanisms. This must go beyond fragmented laws to integrate legal protections with awareness and counselling services.[38] Equally important is multi-stakeholder collaboration. Government bodies, police, educators, civil society and tech companies must work together to create a safer digital ecosystem. Such collective action can strengthen law enforcement, promote digital literacy and ensure timely victim assistance.[39]

Although India has taken legislative steps to address cyberbullying, major challenges remain. Loopholes in the law, weak enforcement and social stigma continue to hinder effective protection for victims. A dedicated, comprehensive cyberbullying law supported by public awareness, education and institutional training is essential. Strengthening these areas will help create a safer and more inclusive digital space, particularly for vulnerable groups like women and children.

5. CONCLUSION AND RECOMMENDATIONS

As digital technologies continue to advance, our legal systems and public mindset must evolve to meet the growing threat of cyberbullying. This form of abuse not only harms individuals but also weakens the foundation of online communities. India has the opportunity to lead by enacting strong and inclusive laws that respond to the specific challenges of digital harassment and protect those most at risk. Addressing cyberbullying is not just a legislative necessity it is a moral responsibility. Lawmakers, educators and citizens must work collectively to foster a culture rooted in empathy, accountability and digital dignity. Through purposeful reform and public engagement, we can move toward future where online spaces are safer, supportive and respectful for everyone. Now is the time to act and build a digital world where all voices are valued and protected.

The analysis reveals a significant gap between the nature of online abuse faced by women and the scope of existing legal protections. Laws remain gender-neutral on paper but gender-blind in practice. Victim redress mechanisms are weak, and law enforcement often lacks training in handling digital abuse sensitively.

Cyberbullying is a manifestation of offline gender inequalities in digital form. Without robust, gender-sensitive legal frameworks and responsible platform governance, the promise of the internet as a democratic space remains unfulfilled. Protecting women in digital spaces is not just a legal obligation but a societal imperative.

5.1 Recommendations for Legal Reform

To effectively tackle cyberbullying and strengthen India's legal response, a multifaceted set of reforms is essential. These should focus on updating laws, improving enforcement, supporting victims, promoting education and raising public awareness.

1. Legislative changes

- Precise Definition of Cyberbullying: The law should clearly define cyberbullying, including specific behaviours like trolling, doxxing and online humiliation, to ensure consistent legal interpretation.
- Dedicated Legislation: India should consider enacting a standalone law against cyberbullying, similar to frameworks in Australia and New Zealand. This law should outline specific offences, penalties and avenues for victim redress.
- Revising Existing Laws: Amendments to the Information Technology Act, 2000 and the Indian Penal Code should explicitly address cyberbullying and prescribe stricter punishments particularly when minors or cases of mental trauma are involved.
- Compulsory Reporting: Mandate that schools, colleges and online platforms report cyberbullying incidents. This will enhance accountability and help ensure timely action against perpetrators.

2. Strengthening Enforcement Mechanisms

- Specialized Police Training: Introduce targeted training for law enforcement personnel to enhance their ability to investigate cyberbullying cases. This should include instruction in digital evidence handling, online investigative tools and empathetic communication with victims.
- Creation of Cybercrime Divisions: Set up specialized units within police departments that focus solely on cybercrime, including cyberbullying. These teams should be staffed with professionals trained in both cybersecurity and legal procedures.
- Accelerated Legal Proceedings: Promote the establishment of fast-track judicial mechanisms for cyberbullying cases to ensure prompt resolution and reduce victim trauma caused by prolonged delays.

3. Strengthening Victim Support Systems

- Dedicated Helplines and Online Assistance: Launch confidential support channels, such as 24/7 helplines and chat-based services, to offer victims emotional support, legal guidance and help with reporting cyberbullying incidents.
- Access to Counselling and Recovery Services: Ensure victims have access to professional mental health services, including therapy and trauma counselling. Partnerships with NGOs and psychologists can enhance the availability and quality of care.
- Provision of Legal Assistance: Develop specialized legal aid services to assist cyberbullying victims in understanding and pursuing their rights through the justice system.

4. Promoting Cyberbullying Awareness Through Education

- Integrate Digital Safety in School Curriculum: Introduce structured educational modules on cyberbullying in schools to teach students about responsible online behaviour, the consequences of digital abuse and how to seek help if targeted.
- Empower Teachers and School Personnel: Provide specialized training for educators to help them detect early signs of cyberbullying, respond appropriately and create inclusive and safe digital spaces for students.
- Partner with Tech Companies: Collaborate with digital platforms and tech firms to co-develop age-appropriate educational materials and online safety tools that empower young users to navigate the internet securely.

5. Building Public Awareness and Cultural Change

- National Awareness Initiatives: Launch countrywide campaigns to educate the public about the harmful effects of cyberbullying, empower victims to report abuse and spread information on available legal remedies and support services.

- Leverage Social Voices: Engage popular influencers, public figures and local community leaders to advocate for respectful online behaviour and encourage a culture of empathy, inclusion and support for those affected.
- Data-Driven Policy Making: Support studies and data collection on cyberbullying trends across India to better understand the issue and develop informed, evidence-based policies and interventions.

To effectively combat cyberbullying in India, a comprehensive strategy involving legal reform, stronger enforcement, victim support, education and public awareness is essential. Clear legislation and timely enforcement will help ensure accountability, while mental health and legal aid services will support victims. Education and outreach can foster safer digital behaviour. Achieving this vision requires coordinated efforts among government bodies, police, schools, civil society and tech platforms. Such collaboration can create a secure online environment where victims feel empowered to speak up and seek justice.

REFERENCES

1. UNICEF, "How to Stop Cyberbullying," UNICEF, https://www.unicef.org/eca/cyberbullying-what-it-and-how-stop-it (accessed August 25, 2024).European Institute for Gender Equality (EIGE), Cyber Violence Against Women and Girls: Key Terms and Concepts,
2. EIGE, 2017, available at:
3. https://eige.europa.eu/sites/default/files/cyber_violence_against_women_and_girls_key_terms_and_concepts.pdf [accessed 1 July 2025].
4. National Crime Records Bureau (2022) Crime in India 2021: Statistics. Ministry of Home Affairs, Government of India. Available at: https://ncrb.gov.in/en/crime-india-2021 [Accessed 1 July 2025].
5. Bois Locker Room: A Case of Juvenile Misogyny, The Hindu (May 6, 2020).
6. Women, Business and the Law, Protecting Women and Girls from Cyber Harassment: A Global Assessment of Existing Laws, World Bank (2022), https://www.worldbank.org/en/news/feature/2022/03/03/protecting-women-and-girls-from-cyber-harassment.
7. Id.
8. R. Vasanthi et al., Impact of Cyber Bullying on Women Emotional Health, 45 J. ADVANCED ZOOL. 686 (2024), https://jazindia.com/index.php/jaz/article/view/4067/3871.
9. Id.
10. Anita Gurumurthy & Nandini Chami, Digital India: Technology to Transform or Transfix?, 14 IT FOR CHANGE 3 (2016).
11. U.N. Human Rights Council, Report of the Special Rapporteur on Violence Against Women, Its Causes and Consequences, U.N. Doc. A/HRC/38/47 (2018).
12. Women, Business and the Law, Protecting Women and Girls from Cyber Harassment: A Global Assessment of Existing Laws, WORLD BANK (2022), https://www.worldbank.org/en/news/feature/2022/03/03/protecting-women-and-girls-from-cyber-harassment. [1] Prithwish Ganguli, Cyberbullying Legislation in India: Effectiveness and International Perspectives, SSRN (Oct. 28, 2024), https://ssrn.com/abstract=5001936.
13. Information Technology Act, 2000, No. 21, §§ 66E, 67, 72, Acts of Parliament, 2000 (India).
14. Shreya Singhal v. Union of India, (2015) 5 S.C.C. 1 (India); see also National Crime Records Bureau, Crime in India 2021: Statistics, Ministry of Home Affairs, Govt. of India (2022), https://ncrb.gov.in/en/crime-india-2021.
15. Supreme Court Calls for Stronger Enforcement of Cyber Laws to Protect Minors, The Hindu (Apr. 2024).
16. Shreya Singhal v. Union of India, (2015) 5 S.C.C. 1 (India).
17. CAL. EDUC. CODE § 234.1 (West 2023).
18. Doe v. Taylor Indep. Sch. Dist., 15 F.3d 443 (5th Cir. 1994).
19. Education and Inspections Act 2006, c. 40, § 89 (UK).
20. S v. H, [2012] EWHC 2459 (Admin) (Eng.).
21. Criminal Code Amendment (Bullying) Act 2011 (Cth) (Austl.); Safe Schools Coalition Australia, Program Overview (2013).
22. Khadra v. State of S. Austl., [2015] SA/33/15 (Austl.).
23. Regulation (EU) 2016/679 of the European Parliament and of the Council (General Data Protection Regulation), 2016 O.J. (L 119).
24. GC & Others v. M.E., App. No. 2020/18, Eur. Ct. H.R. (2019).
25. UNHRC, Report of the Special Rapporteur on Violence Against Women, Its Causes and Consequences, U.N. Doc. A/HRC/38/47 (2018).
26. Shaikh, Zeeshan, Bois Locker Room: Delhi Police Trace Group Admin, 15 Students Identified, The Indian Express (May 6, 2020), https://indianexpress.com/article/cities/delhi/bois-locker-room-delhi-police-instagram-chat-6394293/.
27. Rana Ayyub, The Cost of Speaking Out, The Washington Post (Jan. 20, 2022), https://www.washingtonpost.com/opinions/2022/01/20/rana-ayyub-trolls-india-harassment/.

28. BBC News, India Climate Activist Disha Ravi Granted Bail, BBC (Feb. 23, 2021), https://www.bbc.com/news/world-asia-india-56163557.
29. Information Technology Act, 2000, No. 21, § 66A (struck down), Acts of Parliament, 2000 (India); see also Shreya Singhal v. Union of India, (2015) 5 S.C.C. 1 (India).
30. Indian Penal Code, 1860, No. 45, Acts of Parliament, 1860 (India); Information Technology Act, 2000, No. 21, Acts of Parliament, 2000 (India).
31. Apar Gupta, Why India Needs a Victim-Centric Cyber Law Framework, The Hindu (Feb. 14, 2023), https://www.thehindu.com/opinion/op-ed/india-cyber-laws-victim-protection.
32. Ministry of Home Affairs, Handbook for Cybercrime Investigation (2022), available at https://www.mha.gov.in.

33. Pawan Duggal, Challenges of Cyber Law Enforcement in India, CYBERLAWS.NET (2023), https://www.cyberlaws.net.
34. Law Commission of India, Report No. 245: Arrears and Backlog: Creating Additional Judicial (wo)manpower (2014).
35. Nupur J. Sharma, Why Cyberbullying Victims Suffer in Silence, The Print (Oct. 5, 2022), https://theprint.in.
36. Ministry of Electronics and Information Technology, Cyber Awareness Handbook for Citizens (2021), https://www.meity.gov.in.
37. National Crime Records Bureau, Crime in India 2021: Cybercrime Statistics, Ministry of Home Affairs (2022), https://ncrb.gov.in.
38. Ministry of Home Affairs, Cyber Safety Handbook for Youth (2022), https://www.mha.gov.in.
39. Apar Gupta, Digital Rights and Cyber Accountability in India, Internet Freedom Foundation (2023), https://internetfreedom.in.