International Journal of Information Movement *Vol. 10 Issue I* *(May 2025)*
Website: www.ijim.in *ISSN: 2456-0553 (online)* **Pages 90-96**

COMBATTING CYBERBULLYING IN INDIA: A CRITICAL LEGAL ANALYSIS

Dr. Pooja
(Assistant Professor)
Vaish College of Law, Rohtak
Email: advocatepoojarao@gmail.com

Abstract
Cyberbullying has become a very serious and complex form of online harassment as an outcome of high rise in use of internet worldwide. The Indian Legal, institutional, and policy framework for combating cyberbullying is critically examined in this research paper, revealing significant gaps in legislation, enforcement, and victim protection. Although "the Information Technology Act of 2000", "the Bhartiya Nyaya Sanhita of 2023", and "the Protection of Children from Sexual Offences (POCSO) Act of 2012" offer partial remedies, they still not adequately cover the complete area of psychological, reputational, and emotional harm that is caused by online harassment.
In this paper leading judicial pronouncements, such as the "Shreya Singhal v. Union of India" and "Puttaswamy v. Union of India", are discussed which has brought India's digital rights jurisprudence. Underreporting, a lack of digital forensic infrastructure, intermediary non-compliance, and procedural delays are all highlighted as enforcement issues.
A dedicated anti-cyberbullying statute, the establishment of a National Cyber Safety Authority, mandatory redressal mechanisms in educational establishments, and enhanced platform accountability are among the recommendations. The paper comes to the conclusion that cyberbullying is not just a technological or legal issue; rather, it is a human rights issue that calls for an integrated approach that combines legal reform, digital literacy, victim support, and regulatory enforcement to make the digital environment safer for everyone.

Keywords: anti-cyberbullying, Cyber Safety

1.0 Introduction

The internet has changed human interaction, education, expression, and governance in the digital age. However, it has also opened up new opportunities for harm, one of which is cyberbullying, which is now widespread and has a negative psychological impact. Utilizing platforms like social media, messaging services, and online forums to harass, threaten, or humiliate individuals, frequently anonymously, is known as cyberbullying. The repercussions range from reputational damage to mental health crises, particularly for vulnerable groups like students, women, LGBTQ+ people, and children.
There are more than 800 million internet users in India for whom it is facing challenges in regulating and preventing online harassment. However, the frequency of the incidents of cyberbullying is increasing at a very high speed, the statute remains inadequate and fragmented and no specific law on cyberbullying. The actual number of incidents is still not known because of not reporting it as there is low digital literacy, not adequate enforcement mechanism and the legal definition is precise. However, legal provisions are there under existing statutes like Information Technology Act, 2000 and Bhartiya Nayay Sanhita, 2024 but they do not cover all the emerging aspects of cyber harassment.

1.1 Understanding Cyberbullying

Cyberbullying is a form of online abuse which is intentional and done repeatedly over internet or social media platforms causing psychological hard to the target. It includes a variety of activities, which are

- Trolling: Posting highly offensive and heating content to provoke others.
- Morphing: Editing and misusing the original images of the person to defame him/her.
- Revenge Porn: Sharing private pictures and videos of someone without his/her consent.
- Cyberstalking: tracking someone online and sending fearful messages to others repeatedly.
- Impersonation: Creating fake profiles to abuse others
- Doxxing: Revealing someone's personal information publicly without his/her consent.
- Online Shaming: Humiliating someone publicly on internet.

Cyberbullying is such an act which can affect the persons of all age groups; however, women and teenagers are

most vulnerable. The National Crime Records Bureau (NCRB) reports shows that women are the most affected from cybercrimes, Especially the crimes under stalking, obscenity and blackmail.

2.0 Social and Psychological Impact of Cyberbullying:

Cyberbullying is a virtual crime with real and more severe consequences than that of the conventional crimes, because these crimes are of permanent nature. Mainly following are the mental impacts of cyberbullying:

- Depression and Anxiety
- Suicidal tendency
- Sleep disturbances
- Feeling of withdrawal
- Shelf harm tendencies
- Lack of appetite, etc.

3.0 Indian Statute for Combatting Cyberbullying

There is not specific law in India to directly deal with cyberbullying, in spite of increasing instances of cyber abuse. However, there are provisions of "Information Technology Act, 2000," "the Bhartiya Nyaya Sanhita, 2023 (BNS)", and "the Protection of Children from Sexual Offences (POCSO) Act, 2012" which cover some of the aspects of cyberbullying.

The Information Technology Act, 2000

The IT Act, 2000 specifically formed with the object of facilitating electronic commerce and dealing with cybercrimes. However, the act is silent about any specific definition of cyberbullying, though several provisions are there to tackle related issues, which are:

- **"Section 66C** – Punishes identity theft (e.g., creating fake social media accounts).
- **Section 66D** – Addresses cheating by personation using computer resources.
- **Section 66E** – Criminalizes the violation of privacy through unauthorized capture, publishing, or transmission of images.
- **Section 67, 67A, 67B** – Penalize publishing or transmission of obscene, sexually explicit material, including child sexual abuse material".[1]

These are the provisions which are usually invoked in the cases of Online threats, morphing, revenge porn and circulating obscene material. However, the act fails to cover the crimes like verbal and emotional abuse like trolling, exclusion, shaming etc.

The "Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021", issued under Section 79, impose compliance duties on platforms such as Facebook, Instagram, and WhatsApp. These include requirements for:

- Appointing grievance redressal officers in India
- Time-bound content takedown
- Reporting offences that threaten the dignity of women

Still, there is lack of enforcement machinery and not specific definition of cyberbullying, clear rules for procedural aspects are not there and challenges remains in the ground.

3.1Bhartiya Nyaya Sanhita, 2023 (BNS)

The BNS, 2023 has replaced the Indian Penal Code, 1860, and contained many important provisions to cover different cyber crimes including cyberbullying. The important provisions are as under:

- **Section 74** – Criminal intimidation (earlier IPC Section 503)
- **Section 77** – Word, gesture or act intended to insult the modesty of a woman (earlier IPC Section 509)
- **Section 79** – Stalking, including cyberstalking (earlier IPC Section 354D)
- **Section 356** – Defamation (earlier IPC Sections 499–500)
- **Section 352** – Anonymous criminal intimidation (earlier IPC Section 507)

These provisions are being used frequently in many complaints related to cyber crimes prevalent these days like online stalking, vulgar comments, impersonation, threatening messages etc. However, these sections were not framed taking in view the cyberspace, so it has found difficult in some cases to apply such sections in

[1] The Information Technology Act, 2000

modern cybercrimes.

POCSO Act, 2012

When the act of cyberbullying is done with children, it attracts "the Protection of Children from Sexual Offences Act, 2012 (POCSO)". The important sections in this regard are as follows:

- **"Section 11** – Sexual harassment of children
- **Section 13** – Use of a child for pornographic purposes
- **Section 14** – Possession or distribution of child sexual abuse material"[2]

When cyberbullying of students involves the dissemination of personal photos, obscene messages, or body shaming, educational institutions frequently face difficulties. Cyber safety advisories from the CBSE and NCERT are non-binding and do not impose statutory obligations on schools.

3.2 Digital Personal Data Protection Act, 2023

The DPDPA, 2023 has an object of regulating and controlling the personal data processing and Strengthening user control in cyberspace. However, it does not aim to address cyberbullying directly, it only gives the users a right to withdraw consent and provides directions for data fiduciaries to maintain safety of the data. But, where there is an act of unauthorized disclosure of personal data covering cyberbullying, this act may provide some civil remedies providing the compensation and injunction.

3.3 Judicial approach towards Cyberbullying

Due to the absence of a specific anti-cyberbullying statute, judicial interpretation has had a significant impact on India's response to cyberbullying. In order to guarantee justice in cases involving digital harassment, the Indian judiciary has frequently used inventive interpretations of "the Information Technology Act of 2000", "the Bhartiya Nyaya Sanhita of 2023", and constitutional rights. The cases involving cyberbullying are the subject of this section's in-depth analysis of significant verdicts and prevailing patterns.

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

The landmark judgement decided by the Apex Court resulted in the repeal of Section 66A of the IT Act, which made it illegal to send electronic messages that were "grossly offensive." The provision was frequently used in cases of cyberbullying, particularly those involving abuse, threats, or trolling, despite its widespread misuse to restrict free speech. According to the Court, Section 66A's language violated Article 19(1)(a) of the Constitution because it was ambiguous, overly broad, and arbitrary. Even though this decision was a turning point in the field of digital expression, it left out a useful tool for people who have been bullied emotionally but not sexually, but it didn't suggest a new law.

***3.5 Kusum Sharma v. State of Haryana*, (2020 SCC OnLine P&H 1849)**

The Punjab and Haryana High Court dealt with cyberstalking and harassment of a woman via sexually explicit messages and fake social media profiles in this case. The court ordered the police to find the IP addresses, highlighting the need for platform cooperation and technical expertise in cyber forensics. Sections 74 and 77 of the Bhartiya Nyaya Sanhita previously Sections 503 and 509 of "the Indian Penal Code as well" as Section 67A of the IT Act were the grounds for the accused's charges. The judgment emphasized that cyber harassment is a violation of Article 21's right to dignity and must be taken seriously, particularly when women are the targets.

***3.6 XYZ v. State of Madhya Pradesh*, 2022 (Name anonymized for victim privacy)**

This case involved the leak of intimate photographs of a college student by her ex-boyfriend on messaging groups. The victim went to the court and asked for both criminal action and injunctive relief to have the content removed. In addition to Sections 356 BNS (defamation) and 79 (stalking), the court cited Sections "66E, 67, and 67A of the IT Act". Importantly, in accordance with the 2021 Intermediary Rules, the Court instructed social media platforms to take immediate action. Even in the absence of a verdict in the trial, this case demonstrated that judges are willing to grant interim digital protection.

***3.7 Re: Harassment of Journalists*, Suo Motu PIL, Delhi High Court (2023)**

The targeted online harassment of female journalists, including doxxing, rape threats, and communal slurs, was

[2] the Protection of Children from Sexual Offences Act, 2012

taken up by the Delhi High Court on its own. It asked the Union Government and the Delhi Police to provide a report on the IT Rules, 2021-related actions taken. The court made the observation that anonymous trolls' digital targeting of dissenting voices is a modern form of silence that is against India's constitutional ethos of pluralism and free debate. The PIL emphasized the judiciary's increasing focus on the relationship between online abuse and democratic rights, despite the fact that no final directives were issued.

***3.8 Sabu Mathew George v. Union of India*, (2017) 2 SCC 514**

Although this Supreme Court decision did not specifically deal with cyberbullying, it dealt with search engine liability for advertisements that violated "the Pre-Conception and Pre-Natal Diagnostic Techniques (PCPNDT) Act". The Court ordered Microsoft, Google, and Yahoo to actively block content that is offensive. In subsequent cyberbullying cases, this precedent has been cited to argue that intermediaries have a duty of care, particularly when the content violates constitutional or statutory rights. The case laid the groundwork for platforms' positive responsibilities to safeguard vulnerable populations.

3.9 Challenges in Enforcement and Reporting of Cyberbullying in India

In spite of legislative efforts and judicial recognition of cyberbullying's seriousness, India's effective enforcement remains a significant obstacle. Underreporting, delayed justice, and impunity for perpetrators are frequently the outcomes of the combination of technological complexity, jurisdictional obstacles, and institutional limitations.

1. **Underreporting and Victim Hesitancy:** The most common problem of cyberbullying is not reporting the act by the victim. The main reasons for the same may be:
    - Public Humiliation and blaming of the victim
    - Lack of knowledge of the statute
    - Fear of non-responsiveness of the police
    - Issue of Gender sensitivity

"A 2021 study by **Cyber Peace Foundation** revealed that nearly **60% of cyberbullying victims in India did not report incidents** due to concerns over stigma and inaction."

2. **Technological Complexity and Forensic Delays:** The use of fake accounts, encrypted messaging apps, foreign servers, and anonymous browsing tools in cyberbullying cases makes it difficult to technologically identify the perpetrators. For enforcement to be successful:
    - Advanced cyber forensic units
    - The timely preservation of digital footprints and metadata
    - Permission from the law to access server logs and IP addresses

Thus, there is lack of training to the police and less digital forensic capability in rural areas, there is delay in evidence collection resulted into failure of prosecution.

3. **Lack of Cooperation from Intermediaries:** As per the IT Rules, 2021, there is a duty of the intermediaries like google, telegram, meta etc. to comply with the regulations which most of the time fails. Following issues come up usually:
    - Delay in deleting the problematic content
    - Legal notices not answered on time
    - Jurisdictional issues
    - No claim by the companies to protect the data by denying the IP Logs
4. **Jurisdictional and Procedural Loopholes:** Because cyberbullying is a crime without borders, it can be hard to figure out which court to go to based on where the content was made, accessed, or hurt the victim. Although in digital space, this is ambiguous, "Section 177 of the Code of Criminal Procedure (CrPC)" permits trial in the local area where the offense occurred. Moreover, there is no clarity of the procedure under the Bhartiya Nyaya Sanhita, 2023 which in turn,
    - Wrong classification of cyberbullying as making it civil defamation
    - If there is light obscenity, police does not register the FIR
    - There is less understanding of cybercrimes, the chargesheets are inadequate
5. **Inadequate Grievance Redressal at Institutional Level:** The National Cyber Crime Reporting Portal gives a centralized platform for reporting crimes over cyberspace, but there are few lacunae,
    - The coordination between the local police and central portal is very poor.
    - Response time is not same all over the country

- Ther are so many anonymous complaints, which the machinery fail to act upon.

Additionally, there are no legally binding internal mechanisms in place for educational establishments and workplaces to address complaints of cyberbullying, particularly those involving staff, students, or faculty. Implementation is advisory and not required, despite the UGC and CBSE guidelines' emphasis on internal committees.

6. **Lack of Victim-Centric Approach:** In India we are less sensitive towards the victim and have right based framework which is followed for cyberbullying too. We focus mainly on the punishment without:
    - Opting for psychological counselling or rehabilitation of the victim
    - Ensuring the safety for future by giving protection from future abuse.
    - Opting for restorative justice.

Many victims of verbal and reputational bullying are unprotected because courts rarely order monetary compensation or platform-level monitoring unless physical harm or sexual elements are involved.

7. **Absence of a Dedicated Law:** In India, the absence of a distinct Anti-Cyberbullying Law contributes to interpretive ambiguity. Judges and lawyers frequently create legal gray areas as a result of having to adapt existing statutes to accommodate contemporary abuse patterns. India still lacks specific cyberbullying or digital abuse laws, unlike Australia, the United Kingdom, and South Korea.

4.0 Recommendations for Reform in Indian Law to Combat Cyberbullying

It is evident that a comprehensive and coherent legal response to cyberbullying is urgently required, given the analysis of India's fragmented statutory framework, enforcement difficulties, and comparative best practices discussed earlier. In order to improve India's ability to combat cyberbullying in a victim-centered, rights-based, and technologically adaptive manner, this section offers a set of actionable legal, institutional, and policy recommendations.

1. **Enactment of a Dedicated Anti-Cyberbullying Law:** There is immense need of having a specific statute in India to combat cyberbullying, which should:
    - Clear definition of cyberbullying with clear terms like trolling, doxxing, cyberstalking and emotional abuse
    - The psychological harm suffered by the victim should also be considered for legal action, even there is no obscenity or sexual content.
    - The punishment must be classified differently on the bases of repetition, severity and victim vulnerability.
    - Restorative mechanism like injunction, counselling etc. should be incorporated.
2. **Establishment of a National Digital Safety Authority:** India should create a separate National Cyber safety Authority and give following powers to it:
    - Delete Highly harmful contents from internet within 24-48 hrs.
    - If the intermediaries and platforms do not comply, impose penalties on them
    - Maintenance of as a complaint mechanism which is highly confidential, to cover the complaints of children and women.
    - Annual transparency report should be published on cyber abuse.
3. **Strengthening Platform Accountability and IT Rules:** Amendments should be made in the provisions of "Intermediary Guidelines and Digital Media Ethics Code, 2021", which are inconsistent. Which are,
    - Proactive monitoring of the repeat offenders must be done.
    - Independent Grievances Redressal Cells must be established on the platforms.
    - For failing to remove reported content within specified timeframes, impose tiered penalties.
    - Require accounts involved in complaints to adhere to protocols for identity verification.
    - Children, journalists, activists, and women should be given special protections, including non-consensual image protections.

4. **Procedural and Police Reforms: "**Bhartiya Nyaya Sanhita, 2023 and the Information Technology Act, 2000" must be enforced efficiently and following upgradations must be made:
    - Every Police station at district level must have a Cybercrime desks.
    - Police personnel, advocates and judges must be trained regularly on digital forensics and emotional abuse indicators.
    - For handling the complaints on cyberbullying and preserving the evidences there should be a Standard Operating Procedures (SOPs)
    - The procedure must be heard by fast-track courts.
5. **School and University Mandates:** Binding obligations must be imposed on educational institutions from mere advisory:
    - Cyberbullying policies must be mandatory at school level with proper protocols.
    - In Universities Internal Digital Safety Committees must be established.
    - In school curriculum digital citizenship education must be compulsorily.
    - Peer to peer bullying must be solved with parity whether its offline or online.
6. **Civil Remedies and Psychological Support:** Cyberbullying should have civil liability recognized by Indian law, such as:
    - Financial compensation for reputational harm, mental anguish, or job loss.
    - On the same platform, requests for public apologies or corrections.
    - Including victim counseling and psychological support into the legal process.
    - Victims of cyberbullying, particularly those under the age of 18 and those with low incomes, should receive free legal assistance from the authorities in charge of legal aid.
7. **Role of Judiciary in Developing Digital Jurisprudence:** Until new legislation is passed, courts must continue to interpret existing laws to increase digital security. Some suggestions are:
    - Recognizing that emotional abuse and damage to reputation warrant judicial intervention.
    - issuing interim digital protection orders in a manner comparable to domestic violence protection orders.
    - Establishing protocols for victim anonymity in cases involving gender-based bullying, children, or students.

5.0 Conclusion:

Cyberbullying has emerged as one of the most pressing and harmful forms of online abuse in the evolving digital ecosystem, affecting people of all ages, genders, locations, and socioeconomic classes. Despite being somewhat responsive, India's existing legal and institutional frameworks lack the specificity, coherence, and enforcement capacity required to address cyberbullying's complexities.

This critical analysis makes it abundantly clear that India's response is still reactive, fragmented, and inadequately enforced. Limited tools are provided by "the Information Technology Act of 2000, the Bhartiya Nyaya Sanhita of 2023", and special laws like POCSO; their implementation is hampered by technological illiteracy, confusion among jurisdictions, and institutional inertia. The void has been partially filled by judicial activism, but even significant cases like Shreya Singhal have not resulted in complete legislative reform.

It is past time for India to place a high value on the safety and dignity of its digital citizens, particularly children, women, and members of minority groups, who continue to be at a disadvantage. Cyberbullying is more than just a technological problem; it is a human rights issue that necessitates legislative bravery, institutional innovation, and social change. Cyberbullying can only be effectively combated and the promise of digital freedom cannot be undermined by digital harm without a comprehensive framework that includes legal reform, digital literacy, platform regulation, and psychological support.

6.0 References

Statutes & Regulations:

1. Information Technology Act, 2000
2. Bhartiya Nyaya Sanhita, 2023
3. Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021
4. Digital Personal Data Protection Act, 2023
5. Protection of Children from Sexual Offences (POCSO) Act, 2012

Cases:

6. *Shreya Singhal v. Union of India*, (2015) 5 SCC 1
7. *Justice K.S. Puttaswamy v. Union of India*, (2017) 10 SCC 1
8. *Kusum Sharma v. State of Haryana*, 2020 SCC OnLine P&H 1849
9. *XYZ v. State of Madhya Pradesh*, 2022 (Unreported)
10. *Sabu Mathew George v. Union of India*, (2017) 2 SCC 514

Reports & Surveys:

11. Cyber Peace Foundation, *Cyberbullying in India Survey Report*, 2021
12. Save The Children, *Protecting Children in Cyberspace: A National Audit Report*, 2022
13. Internet and Mobile Association of India (IAMAI), *Digital in India Report*, 2023