



Cyberbullying Laws in India

Omendra Singh, Ph.D., Department of Law
Brahmanand Degree College, Kanpur, Uttar Pradesh, INDIA

ORIGINAL ARTICLE



Author

Omendra Singh, Ph.D.

E-mail : omsingh81@gmail.com

shodhsamagam1@gmail.com

Received on : 06/04/2026
Revised on : 07/06/2026
Accepted on : 16/06/2026
Overall Similarity : 01% on 08/06/2026



Plagiarism Checker X - Report

Originality Assessment

1%

Overall Similarity

Date: Jun 8, 2026 (07:04 AM)
Matches: 21 / 3438 words
Sources: 3

Remarks: Low similarity detected, consider making necessary changes if needed.

Verify Report:
Scan this QR Code



ABSTRACT

The proliferation of digital technologies has revolutionized communication, yet it has simultaneously facilitated the rise of cyberbullying as a pervasive and complex socio-legal issue. Cyberbullying transcends geographical boundaries and poses significant threats to individual dignity, privacy, and mental health. In India, the legal response to cyberbullying is fragmented, relying on provisions of the Information Technology Act, 2000, the Indian Penal Code, 1860 (now replaced by the Bharatiya Nyaya Sanhita, 2023), and sector-specific legislation such as the Protection of Children from Sexual Offences Act, 2012. This paper critically examines the adequacy of the Indian legal framework, judicial interventions, and enforcement mechanisms in addressing cyberbullying. It undertakes a comparative analysis with legal regimes in the United Kingdom, the United States, and the European Union, highlighting best practices and regulatory innovations. The study concludes that India requires a comprehensive and victim-centric legislative framework to effectively combat cyberbullying while balancing constitutional freedoms.

KEY WORDS

Cyberbullying, Digital Harassment, IT Act, Intermediary Liability, Comparative Law.

INTRODUCTION

The exponential growth of digital technologies and internet penetration has transformed the landscape of human interaction. Social media platforms, instant messaging services, and online forums have created unprecedented opportunities for communication and expression. However, these developments have also facilitated the emergence of cyberbullying as a significant socio-legal concern.

Cyberbullying represents a modern manifestation of harassment, characterized by the use of electronic

communication to intimidate, threaten, or humiliate individuals. Unlike traditional forms of bullying, cyberbullying is not confined by physical boundaries and often operates under the cloak of anonymity, thereby intensifying its impact. The permanence and virality of online content further exacerbate the harm caused to victims.¹

In India, the increasing reliance on digital platforms has been accompanied by a rise in cyberbullying incidents, particularly among adolescents and young adults. Despite this, the Indian legal system lacks a dedicated statute addressing cyberbullying. Instead, the issue is governed through a patchwork of provisions under the Information Technology Act, 2000, the Indian Penal Code, 1860 (now replaced by the Bharatiya Nyaya Sanhita, 2023), and other specialized legislations.

This study lays the foundational framework by examining the concept, nature, and types of cyberbullying, followed by a detailed analysis of the statutory provisions governing such conduct in India.

Concept and Nature of Cyberbullying

Definitional Ambiguity

One of the primary challenges in addressing cyberbullying is the absence of a universally accepted legal definition. Indian statutes do not explicitly define cyberbullying, leading to reliance on academic and judicial interpretations.

Cyberbullying may be understood as: “The use of digital communication technologies to harass, threaten, or harm individuals through repeated and intentional conduct.” This definitional ambiguity results in inconsistent legal responses and difficulties in classification and prosecution.

Essential Elements of Cyberbullying

Cyberbullying generally involves the following elements:

1. **Intentional Conduct:** The act must be deliberate.
2. **Repetition:** Continuous or repeated behavior.
3. **Harm:** Psychological, emotional, or reputational damage.
4. **Use of Technology:** Digital platforms as the medium.

Unlike traditional bullying, repetition may occur through the viral nature of a single post, thereby complicating legal interpretation.

Forms and Manifestations

Cyberbullying manifests in various forms, including:

- **Cyberstalking:** Persistent online tracking and harassment
- **Trolling:** Posting inflammatory or abusive comments
- **Defamation:** Circulating false statements harming reputation
- **Impersonation:** Creating fake profiles
- **Outing and Doxxing:** Sharing private or confidential information
- **Revenge Porn:** Non-consensual sharing of intimate images

Each of these forms intersects with existing legal provisions but lacks unified treatment under a single statute.

Psychological and Social Impact

Cyberbullying has profound consequences, including:

- Anxiety and depression.
- Loss of self-esteem.
- Social isolation.
- Suicidal tendencies in extreme cases.

The impact is often more severe than traditional bullying due to the permanence and public nature of digital content.

Statutory Framework Governing Cyberbullying in India

The Information Technology Act, 2000²

The IT Act serves as the primary legislation addressing cyber offences in India. Although it does not explicitly criminalize cyberbullying, several provisions are relevant.

Section 66C² – Identity Theft

This provision penalizes fraudulent use of another person's identity, including passwords and digital signatures.

Relevance to Cyberbullying

Impersonation through fake social media accounts is a common form of cyberbullying, falling squarely within this provision.

Section 66D – Cheating by Personation

This section criminalizes cheating through impersonation using computer resources.

Application

Used in cases where perpetrators deceive victims through fake online identities.

Section 66E³ – Violation of Privacy

This provision addresses the capture or transmission of private images without consent.

Importance

Critical in cases involving **revenge porn** and unauthorized sharing of intimate content.

Section 67 – Obscene Content

This section penalizes publication or transmission of obscene material in electronic form.

Scope

Covers sexually explicit harassment and offensive content.

Limitations of the IT Act¹²

- Absence of explicit definition of cyberbullying.
- Focus on specific offences rather than holistic harm.
- Reactive rather than preventive approach.

Penal Law Framework: Bhartiya Nyaya Sanhita, 2023¹³

Traditional criminal law provisions supplement cyber law in addressing cyberbullying.

Section 78 – Stalking (Including Cyberstalking)

This provision explicitly recognizes cyberstalking as an offence.

Judicial Interpretation

Courts have interpreted stalking broadly to include persistent online harassment.

Sections 356 – Defamation

These provisions address harm to reputation.

Cyber Context

Online defamation through posts, tweets, and blogs is actionable under these sections.

Sections 351– Criminal Intimidation

These sections criminalize threats intended to cause alarm.

Application

Frequently invoked in cases involving online threats and harassment.

Section 79 – Insulting Modesty of a Woman

This provision is particularly relevant in gender-based cyberbullying.

Judicial Application

In SMC Pneumatics (India) Pvt. Ltd. v. Jogesh Kwatra, the Delhi High Court recognized cyber defamation and granted an injunction against defamatory emails.

Significance

This case marked the judiciary's early acknowledgment of digital harassment under traditional legal provisions.

Protection of Children: The Protection of Children from Sexual Offences Act, 2012

This Act provides robust protection for minors against sexual offences, including those committed online.

Scope and Application

The Act covers:

- Online sexual harassment.
- Child pornography.
- Grooming and exploitation.

Importance in Cyberbullying

Children are particularly vulnerable to cyberbullying. The Act provides:

- Stringent punishments.
- Child-friendly procedures.
- Mandatory reporting obligations.

Intermediary Liability: The Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021¹¹

Digital platforms are required to:

- Remove unlawful content.
- Appoint grievance officers.
- Ensure user safety.

Takedown Mechanism

Content involving nudity or impersonation must be removed within 24 hours upon complaint.

Limitations

- Enforcement challenges.
- Dependence on user complaints.
- Lack of proactive monitoring.

Case Law- Illustrating Cyberbullying Dimensions

Shreya Singhal v. Union of India.

Facts

The petitioner challenged the constitutionality of Section 66A of the IT Act, which criminalized offensive online content.

Issue

Whether Section 66A violated the right to freedom of speech under Article 19(1)(a).

Judgment

The Supreme Court struck down Section 66A as unconstitutional.

Relevance to Cyberbullying

While the judgment protected free speech, it also created a regulatory gap in addressing online abuse. Kalandi Charan Lenka v. State of Odisha.

Facts

The accused created fake profiles and circulated obscene images of the victim.

Judgment

The court recognized cyber harassment as a serious offence affecting dignity and privacy.

Significance

This case highlighted the psychological impact of cyberbullying and the need for strict enforcement.

Critical Observations on the Indian Legal Framework

- **Fragmented Approach:** Multiple laws but no unified framework
- **Reactive Nature:** Focus on punishment rather than prevention
- **Lack of Awareness:** Victims often unaware of legal remedies
- **Judicial Dependence:** Courts play a crucial role in interpretation

Judicial Approach to Cyberbullying in India

The Indian judiciary has played a pivotal role in shaping the legal discourse surrounding cyberbullying. In the absence of a dedicated statutory framework, courts have relied on constitutional principles and existing penal provisions to address digital harassment. Judicial intervention has thus been both interpretative and gap-filling, often balancing competing interests such as freedom of speech and protection of individual dignity.

Constitutional Dimensions: Freedom of Speech vs. Cyber Abuse

Shreya Singhal v. Union of India

Facts

The case arose from a challenge to Section 66A of the IT Act, which criminalized the sending of “offensive” messages through electronic communication. The provision was criticized for its vague terminology, including expressions such as “annoying” and “inconvenient.”

Issues

- Whether Section 66A violated Article 19(1)(a) (freedom of speech and expression).
- Whether the restriction could be justified under Article 19(2).

Judgment

The Supreme Court struck down Section 66A as unconstitutional, holding that:

- The provision was vague and overbroad.
- It had a chilling effect on free speech.
- It failed to meet the test of reasonable restrictions.

Legal Reasoning

The Court emphasized that restrictions on speech must be narrowly tailored and directly related to the grounds specified in Article 19(2), such as public order, defamation, or incitement to an offence.

Relevance to Cyberbullying

While the judgment safeguarded fundamental rights, it inadvertently created a regulatory vacuum in addressing online abuse. The absence of Section 66A has made it more challenging to prosecute certain forms of cyberbullying that do not fall neatly within existing provisions.

Recognition of Cyber Harassment and Privacy Violations

Kalandi Charan Lenka v. State of Odisha

Facts

The accused created fake social media profiles of the victim and circulated morphed obscene images, causing severe mental trauma.

Issues

- Whether such acts constitute offences under the IT Act and IPC.
- Whether cyber harassment violates the victim’s right to dignity and privacy.

Judgment

The court held the accused liable under provisions relating to:

- Identity theft.
- Obscenity.
- Criminal intimidation.

Significance

The case is significant for:

- Recognizing cyber harassment as a serious offence.
- Highlighting the psychological impact of digital abuse.
- Expanding the interpretation of privacy in the digital context.

Doctrinal Contribution

This decision aligns with the broader constitutional recognition of privacy as a fundamental right, as later affirmed in *Justice K.S. Puttaswamy v. Union of India* (2017).

Cyber Defamation and Injunctive Relief

SMC Pneumatics (India) Pvt. Ltd. v. Jogesh Kwatrati

Facts

The defendant sent defamatory emails to the plaintiff's business associates, damaging the company's reputation.

Issues

- Whether defamatory electronic communication constitutes actionable defamation.
- Whether courts can grant injunctions against such acts.

Judgment

The Delhi High Court granted an injunction restraining the defendant from sending further defamatory communications.

Significance

- First Indian case recognizing cyber defamation.
- Established the applicability of traditional defamation laws in digital contexts.

Analytical Insight

The case demonstrates the judiciary's willingness to adapt conventional legal principles to emerging technological challenges.

Emerging Judicial Trends

The Indian judiciary has increasingly recognized:

- Digital dignity as an extension of Article 21.
- The need for platform accountability.
- The importance of victim protection mechanisms.

However, the absence of a unified legal framework results in inconsistent judicial outcomes.

Comparative Legal Analysis

United Kingdom: A Duty-Based Regulatory Model

The United Kingdom adopts a comprehensive and proactive approach to cyberbullying.

Statutory Framework

Key legislations include:

- Malicious Communications Act, 1988.
- Communications Act, 2003.
- Protection from Harassment Act, 1997.

Online Safety Act, 2023

The UK's Online Safety Act, 2023 represents a paradigm shift in regulating online harms.

Key Features

- Duty of Care imposed on platforms.
- Mandatory risk assessment for harmful content.
- Strong regulatory oversight by Ofcom.

Legal Significance

The Act moves from a reactive to a preventive regulatory model, requiring platforms to actively mitigate risks.

Case Illustration

In *R v. Nimmo and Sorley* (2014)x, individuals were prosecuted for sending abusive tweets, demonstrating the applicability of harassment laws to online conduct.

Comparative Insight

The UK model emphasizes:

- Platform responsibility.
- Victim protection.
- Preventive regulation.

United States: Free Speech-Centric Approach

The United States adopts a decentralized and rights-oriented approach, heavily influenced by the First Amendment.

Legal Framework

- Cyberbullying laws vary across states.
- Federal laws address specific offences (e.g., cyberstalking).

Constitutional Constraint

The First Amendment imposes significant limitations on regulating online speech.

Case Analysis

In *Elonis v. United States* (2015)y, the U.S. Supreme Court held that **mere negligence is insufficient** to establish criminal liability for online threats; intent must be proven.

Implications

- High threshold for prosecution.
- Strong protection of free speech.
- Limited scope for regulating offensive content.

Policy Approach

Focus on:

- School-based interventions.
- Awareness programs.
- Civil remedies.

European Union: Rights-Based Regulatory Framework

The European Union adopts a holistic and rights-oriented approach, integrating privacy, data protection, and platform accountability.

General Data Protection Regulation (GDPR)

The GDPR provides:

- Right to privacy.
- Right to erasure ("right to be forgotten").
- Strict data protection obligations.

Digital Services Act (DSA)

The DSA establishes:

- Accountability of online platforms.
- Mechanisms for content moderation.
- Transparency requirements.

Key Features

- Strong emphasis on user rights.
- Cross-border enforcement mechanisms.
- Proactive monitoring obligations.

Case Reference

In *Google Spain SL v. AEPD* (2014)^{1p}, the Court of Justice of the EU recognized the **right to be forgotten**, enabling individuals to request removal of harmful online content.

Comparative Insight

The EU model prioritizes:

- Data protection.
- User autonomy.
- Platform accountability.

Comparative Evaluation

Structural Comparison

Aspect	India	UK	US	EU
Specific Cyberbullying Law	No	Present	Partial	Emerging
Platform Liability	Limited	Strong	Moderate	Strong
Preventive Mechanisms	Weak	Advanced	Moderate	Advanced
Victim Protection	Limited	Strong	Moderate	Strong

Observations

1. **India's Fragmented Approach:** Relies on multiple statutes without coherence.
2. **UK's Preventive Model:** Imposes proactive obligations on platforms.
3. **US Free Speech Priority:** Limits regulatory intervention.
4. **EU Rights-Based Framework:** Balances privacy, dignity, and accountability.

Lessons for India

India can adopt:

- Duty of care principles (UK model).
- Strong data protection norms (EU model).
- Awareness and education strategies (US model).

The preceding parts have demonstrated that India's response to cyberbullying is shaped by a fragmented statutory framework and evolving judicial interpretation. While courts have attempted to bridge legislative gaps, the absence of a coherent and dedicated legal regime continues to undermine effective regulation. This part critically evaluates the structural, doctrinal, and institutional deficiencies in India's approach and proposes a forward-looking reform agenda grounded in comparative insights and constitutional principles.

Structural and Doctrinal Gaps in the Indian Legal Framework

Absence of a Dedicated Cyberbullying Statute

A central weakness in India's legal regime is the lack of a specific statute addressing cyberbullying. Existing laws such as the Information Technology Act, 2000 and the Indian Penal Code, 1860 operate in a piecemeal fashion, addressing isolated aspects such as obscenity, defamation, or identity theft.

This fragmented approach leads to:

- **Doctrinal ambiguity** in classifying offences.
- **Inconsistent application** by law enforcement agencies.
- **Judicial uncertainty** in interpreting overlapping provisions.

Unlike jurisdictions such as the UK, which explicitly recognize online harms, Indian law fails to conceptualize cyberbullying as a distinct legal wrong.

Over-Reliance on Traditional Penal Provisions

The application of conventional criminal law to cyberbullying raises doctrinal concerns. Provisions designed for offline conduct are often ill-suited to the complexities of digital harm, particularly in cases involving anonymity, virality, and cross-platform dissemination.

For instance:

- Defamation law requires proof of reputational harm, which may not capture psychological injury.
- Criminal intimidation provisions require demonstrable threat perception.
- Stalking provisions may not adequately address indirect or collective harassment.

This mismatch reflects a normative lag between law and technology.

Constitutional Tension: Free Speech vs. Harm Prevention

The judgment in *Shreya Singhal v. Union of India* illustrates the inherent tension between regulating harmful speech and protecting constitutional freedoms.

While the decision rightly invalidated vague restrictions, it also exposed the difficulty of crafting narrowly tailored legislation to address cyberbullying without infringing Article 19(1)(a).

This tension manifests in:

- Reluctance to introduce stringent regulations.
- Judicial caution in interpreting online speech offences.
- Regulatory gaps in addressing non-criminal but harmful conduct.

Inadequate Recognition of Psychological Harm

Indian law traditionally prioritizes physical and economic harm, often neglecting psychological injury. Cyberbullying, however, primarily operates through emotional and reputational damage.

The failure to recognize mental harm as a central component results in:

- Under-criminalization of serious conduct.
- Limited remedies for victims.
- Insufficient deterrence.

Weak Intermediary Accountability

Although the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021 impose certain obligations, they remain largely reactive and complaint-driven.

Key limitations include:

- Lack of proactive monitoring requirements.
- Delayed content removal.
- Limited transparency in content moderation.

This contrasts sharply with jurisdictions such as the EU, where platform accountability is more robust and enforceable.

Institutional and Enforcement Challenges

Jurisdictional Complexities

Cyberbullying often involves cross-border elements, raising issues of:

- Territorial jurisdiction.
- Conflict of laws.
- Enforcement of foreign judgments.

Indian authorities face significant challenges in investigating and prosecuting offences involving foreign platforms or perpetrators.

Underreporting and Social Barriers

Victims frequently refrain from reporting cyberbullying due to:

- Social stigma.
- Fear of retaliation.
- Lack of awareness.

This results in a significant gap between incidence and reporting, undermining the effectiveness of legal remedies.

Capacity Constraints in Law Enforcement

Law enforcement agencies often lack:

- Technical expertise.
- Specialized training.
- Adequate infrastructure.

This leads to delays in investigation and low conviction rates.

Normative Evaluation: Towards a Rights-Based Framework

Cyberbullying as a Violation of Fundamental Rights

Cyberbullying implicates multiple constitutional rights, including:

- Right to dignity under Article 21.
- Right to privacy (as recognized in *Puttaswamy*).
- Right to equality under Article 14.

A rights-based approach requires recognizing cyberbullying as a violation of human dignity, rather than merely a criminal offence.

Reconceptualizing Harm in the Digital Age

The legal system must evolve to recognize:

- Emotional and psychological harm.
- Reputational damage in digital spaces.
- Long-term consequences of online abuse.

This requires a shift from tangible harm to intangible harm paradigms.

Policy Recommendations and Reform Agenda

Enactment of a Comprehensive Anti-Cyberbullying Law

India should enact a dedicated statute that:

- Defines cyberbullying comprehensively.
- Differentiates between degrees of harm.
- Provides both civil and criminal remedies.

The law should incorporate:

- Clear definitions.
- Graded penalties.
- Procedural safeguards.

Strengthening Intermediary Liability

Drawing from the EU and UK models, India should:

- Impose a duty of care on platforms.
- Mandate proactive risk assessment.
- Introduce strict timelines for content removal.

Platforms should be required to:

- Publish transparency reports.
- Establish robust grievance mechanisms.

Establishment of Specialized Cyber Courts

Dedicated cyber courts can:

- Ensure speedy adjudication.
- Develop judicial expertise.
- Promote consistency in decisions.

Enhancing Victim Support Mechanisms

A victim-centric approach should include:

- Psychological counseling services.
- Legal aid and assistance.
- Confidential reporting mechanisms.

Promoting Digital Literacy and Awareness

Preventive strategies should focus on:

- Educational programs in schools and universities.
- Public awareness campaigns.
- Training for law enforcement officials.

International Cooperation and Harmonization

India should:

- Strengthen cooperation with foreign jurisdictions.
- Participate in international cybercrime frameworks.
- Harmonize laws with global standards.

Original Contribution: A Hybrid Regulatory Model

This paper proposes a Hybrid Regulatory Model combining:

1. **Statutory Regulation:** Dedicated cyberbullying law.
2. **Platform Governance:** Duty-based obligations.
3. **Judicial Oversight:** Constitutional safeguards.
4. **Preventive Measures:** Education and awareness.

This model seeks to balance:

- Freedom of expression.
- Protection of dignity.
- Technological innovation.

Findings of the Study

The study reveals that:

1. India's legal framework is fragmented and inadequate.
2. Judicial intervention, while significant, is insufficient to fill legislative gaps.
3. Comparative jurisdictions provide valuable models for reform.
4. A rights-based and victim-centric approach is essential.
5. Effective regulation requires integration of legal, technological, and social measures.

CONCLUSION

The conceptual and legal analysis reveals that cyberbullying in India is addressed through a patchwork of statutory provisions and judicial interpretations. While the existing framework provides certain remedies, it lacks coherence, specificity, and preventive mechanisms. The absence of a dedicated legal definition and comprehensive statute creates significant challenges in enforcement and victim protection. This foundational understanding sets the stage for a deeper examination of judicial trends and comparative legal frameworks in the subsequent part of this study.

The judicial approach in India reflects a progressive yet fragmented effort to address cyberbullying. Courts have played a crucial role in interpreting existing laws to protect victims, but the absence of a dedicated statutory framework limits their effectiveness. Comparative analysis reveals that jurisdictions such as the United Kingdom and the European Union have developed more structured and proactive legal mechanisms, while the United States emphasizes constitutional freedoms. These models provide valuable insights for reforming India's approach to cyberbullying. Cyberbullying represents a complex challenge at the intersection of law, technology, and society. India's current legal framework, though functional, is insufficient to address the multifaceted nature of digital harassment. The absence of a dedicated statute, coupled with enforcement challenges and constitutional constraints, necessitates a comprehensive reform strategy.

Drawing from comparative insights and normative analysis, this study advocates for a holistic and forward-looking approach that integrates legal reform, institutional capacity building, and societal awareness. Only through such a multi-dimensional framework can India effectively combat cyberbullying while preserving the fundamental values of a democratic society.

REFERENCE

1. Hinduja, S. & Patchin, J. W. (2015) *Bullying Beyond the Schoolyard*. Corwin Press, Thousand Oaks, CA.
2. Information Technology Act, 2000, S. 66C.
3. Information Technology Act, 2000, S. 66E.
4. SMC Pneumatics (India) Pvt. Ltd. v. Jogesh Kwatra, 2001 (Delhi HC).
5. Shreya Singhal v. Union of India, (2015) 5 SCC 1.
6. Kalandi Charan Lenka v. State of Odisha, 2017 SCC OnLine Ori 384.
7. Justice K.S. Puttaswamy v. Union of India, (2017) 10 SCC 1.
8. R v. Nimmo and Sorley [2014] EWCA Crim 2063.
9. *Elonis v. United States*, 575 U.S. 723 (2015).
10. *Google Spain SL v. AEPD*, Case C-131/12 (CJEU, 2014).
11. Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021. Government of India. <https://www.meity.gov.in>, Accessed on 16/03/2026.
12. Information Technology Act, 2000.
13. *Bhartiya Nyaya Sanhita*, 2023.
