

Cyberbullying and Online Harassment: Legal Remedies in India

Edgar Rajdayal Allan

Student, Presidency School of Law, Department of Law, Bangalore, India

edgar_allan@hotmail.com

I. ABSTRACT

The rapid expansion of digital communication technologies has fundamentally transformed social interaction while simultaneously creating new avenues for abuse, intimidation, and harassment. Cyberbullying and online harassment have emerged as serious socio-legal concerns in India, particularly affecting women, children, and vulnerable communities. These forms of abuse range from cyberstalking, trolling, doxxing, identity theft, revenge pornography, and defamatory communications to coordinated digital intimidation campaigns. Despite the growing prevalence of cyber abuse, India lacks a dedicated statutory framework specifically addressing cyberbullying. Instead, legal remedies are dispersed across the Information Technology Act, 2000, the Bharatiya Nyaya Sanhita/Indian Penal Code, the Protection of Children from Sexual Offences Act, intermediary guidelines, and constitutional protections.

This paper critically examines the legal architecture governing cyberbullying in India, analyses judicial responses, evaluates enforcement challenges, and identifies significant legislative gaps. Through doctrinal analysis, case law evaluation, and comparative legal perspectives, the paper argues that India's fragmented legal system inadequately addresses the multidimensional harms caused by cyberbullying. The paper concludes by proposing comprehensive legislative reforms, specialized enforcement mechanisms, and policy interventions to establish an effective victim-centric framework.

Keywords—*Cyberbullying, Online Harassment, Information Technology Act, Cyber Law, Digital Rights, Intermediary Liability, India*

II. TABLE OF CONTENTS

- Introduction
- Conceptual Framework: Cyberbullying and Online Harassment
- Evolution of Cyber Law in India
- Constitutional Dimensions
- Statutory Legal Framework
 - Information Technology Act, 2000
 - Bharatiya Nyaya Sanhita / Indian Penal Code
 - POCSO Act
 - Digital Personal Data Protection Act, 2023
 - Intermediary Guidelines and Digital Media Ethics Code
- Important Judicial Decisions
- Challenges in Enforcement
- Comparative Jurisprudence
- Policy Recommendations
- Conclusion
- References

III. INTRODUCTION

The digital revolution has dramatically altered communication, education, business, and governance. India, with over 800 million internet users, is among the largest digital populations globally. However, this technological growth has been accompanied by a corresponding rise in cyber-enabled abuse. Cyberbullying, once considered a social issue, has now become a major legal and human rights concern.

Cyberbullying refers to repeated or intentional harmful behavior conducted through digital means, including social media platforms, instant messaging applications, gaming networks, emails, and online forums. Unlike traditional harassment, cyberbullying is characterized by:

- Persistent accessibility to victims
- Potential anonymity of offenders
- Rapid dissemination of harmful content
- Cross-jurisdictional complexities
- Permanent digital footprints

Victims often suffer severe psychological, emotional, social, and economic consequences, including depression, anxiety, reputational damage, and even suicide.

India has witnessed increasing incidents involving:

- Cyberstalking of women

- Revenge pornography
- Online child harassment
- Fake social media profiles
- Sextortion
- Defamatory campaigns
- Deepfake exploitation

Despite this, Indian law continues to rely on a patchwork of statutory provisions rather than a singular, cohesive anti-cyberbullying law.

IV. CONCEPTUAL FRAMEWORK: CYBERBULLYING AND ONLINE HARASSMENT

After the text edit has been completed, the paper is ready for the template.

A. Definition

Cyberbullying can be broadly defined as:

“The intentional and repeated harm inflicted through the use of computers, mobile phones, and other electronic devices.”

Online harassment includes any digital conduct intended to threaten, humiliate, intimidate, stalk, or abuse another person.

B. Major Forms

1) Cyberstalking

Repeated monitoring, unwanted communication, or surveillance using electronic means.

2) Trolling

Posting inflammatory or abusive content to provoke emotional distress.

3) Doxxing

Publishing private or identifying information without consent.

4) Revenge Pornography

Sharing intimate content without authorization.

5) Identity Theft

Using another person's credentials to impersonate them online.

6) Child Cyberbullying

Harassment or exploitation of minors via online platforms.

V. EVOLUTION OF CYBER LAW IN INDIA

India's cyber law regime began with the enactment of the Information Technology Act, 2000, primarily to regulate e-commerce and digital signatures. However, subsequent amendments expanded its scope to criminalize various cyber offences.

Key milestones:

- 2000: IT Act enacted
- 2008: Major amendments introduced cybercrime provisions
- 2015: Section 66A struck down in *Shreya Singhal v. Union of India*

- 2021: Intermediary Guidelines strengthened platform accountability
- 2023: Digital Personal Data Protection Act enacted

Although these developments improved digital governance, none comprehensively define or regulate cyberbullying.

VI. CONSTITUTIONAL DIMENSIONS

Cyberbullying implicates multiple constitutional rights:

Article 14 – Equality Before Law

Victims are entitled to equal legal protection against digital abuse.

Article 19(1)(a) – Freedom of Speech

Free speech protections must be balanced against abusive expression.

Article 19(2)

Reasonable restrictions apply to defamatory, obscene, or harmful online conduct.

Article 21 – Right to Life and Personal Liberty

Judicial interpretation includes:

- Right to privacy
- Dignity
- Mental well-being
- Reputation

Landmark Case:

Justice K.S. Puttaswamy v. Union of India (2017) recognized privacy as a fundamental right, strengthening protections against digital invasions.

VII. STATUTORY LEGAL FRAMEWORK

VII.1 Information Technology Act, 2000

Section 66C – Identity Theft

Punishes fraudulent use of passwords, digital signatures, or unique identification.

Section 66D – Cheating by Personation

Targets online impersonation and fraudulent deception.

Section 66E – Violation of Privacy

Addresses capturing or transmitting private images without consent.

Section 66F – Violation of Privacy

Addresses capturing or transmitting private images without consent.

Section 67 - Punishes publication or transmission of obscene material.

Section 67A - Covers sexually explicit content.

Section 67B - Protects children from sexually exploitative content.

VII.2 Bharatiya Nyaya Sanhita / IPC Provisions

Section 354D IPC – Stalking

Includes online monitoring and harassment.

Section 499/500 IPC – Defamation

Applicable to false online publications harming reputation.

Section 507 IPC – Anonymous Criminal Intimidation

Relevant for anonymous digital threats.

Section 509 IPC

Protects women from insulting communications.

Section 292 IPC

Addresses obscene material.

VII.3 Protection of Children from Sexual Offences Act, 2012

POCSO increasingly interacts with cyber law where minors face:

- Sextortion
- Grooming
- Sexual exploitation
- Child Pornography / CSEAM

VII.4 Digital Personal Data Protection Act, 2012

Provides safeguards against misuse of personal data, unauthorized sharing, and privacy violations, indirectly strengthening anti-cyberbullying protection.

VII.5 Intermediary Guidelines, 2021

These rules mandate due diligence by platforms, including:

- Content takedown obligations
- User grievance mechanisms
- Traceability obligations (in certain cases)
- Cooperation with law enforcement

VIII. IMPORTANT JUDICIAL DECISIONS

VIII.1 Shreya Singhal v. Union of India (2015) 5 SCC 1

Held:

Section 66A IT Act unconstitutional due to vagueness and chilling effect on speech.

Significance:

- Strengthened free speech
- Created enforcement gap for offensive online speech

VIII.2 State of West Bengal v. Animesh Boxi (2018)

Facts:

Non-consensual sharing of intimate images.

Held:

Court recognized severe psychological consequences and imposed strict punishment.

Principle:

Digital sexual exploitation violates dignity and privacy.

VIII.3 Just Rights for Children Alliance v. S. Harish (2024)

Held:

Possession/viewing/storage of child sexual exploitative material constitutes punishable offence.

Principle:

Purposive child protection approach.

VIII.4 K.S. Puttaswamy v. Union of India (2017)

Principle:

Privacy includes digital autonomy and informational control.

IX. CHALLENGES IN ENFORCEMENT

IX.1 Lack of Dedicated Legislation

Fragmented legal remedies create confusion.

IX.2 Jurisdictional Complexities

Cyber offences often transcend state and national boundaries.

IX.3 Evidentiary Challenges

- Anonymous accounts
- VPN usage
- Encryption
- Electronic evidence admissibility under Section 65B
- Evidence Act

IX.4 Underreporting

Victims fear stigma, retaliation, or lack of institutional support.

IX.5 Platform Non-Compliance

Intermediaries may delay takedowns or resist disclosure requests.

IX.6 Deepfakes and Emerging Technologies

Existing law struggles with AI-generated harassment.

X. COMPARATIVE JURISPRUDENCE

United Kingdom

- Malicious Communications Act
- Online Safety Act

Australia

- eSafety Commissioner system
- Rapid content removal powers

United States

- State-level cyberbullying statutes
- Strong free speech constraints

Comparative Insight:

India lacks:

- Uniform cyberbullying definition
- Specialized victim redressal body
- Expedited takedown systems

XI. POLICY RECOMMENDATIONS

XI.1 Dedicated Cyberbullying Legislation

India should enact a comprehensive statute that:

- Defines cyberbullying
- Categorizes offences
- Prescribes graded punishments
- Protects adults and minors

XI.2 Specialized Cyberbullying Cells

Dedicated police and judicial units should handle such complaints.

XI.3 Platform Accountability Reform

Stricter obligations for:

- Real-time reporting
- Time-bound removals
- Transparency reports

XI.4 Educational Reforms

Mandatory digital citizenship education in schools and colleges.

XI.5 Victim Support Systems

- Psychological counseling
- Legal aid
- Online complaint portals

XI.6 AI and Deepfake Regulation

Specific legal provisions targeting synthetic abuse.

XII. CONCLUSION

Cyberbullying and online harassment are no longer peripheral digital concerns; they represent serious violations of dignity, privacy, and safety. India's current legal framework, though partially effective, remains fragmented, reactive, and insufficiently specialized. Judicial innovation has attempted to bridge statutory gaps, but piecemeal interpretation cannot substitute for comprehensive legislative reform.

A robust cyberbullying law must balance:

- Freedom of expression
- Privacy rights
- Victim protection
- Platform accountability
- Technological realities

As India advances toward deeper digital integration, ensuring safe cyberspaces is essential for constitutional governance, social justice, and human dignity.

XIII. SELECT REFERENCES

1. Information Technology Act, 2000 (India).
2. Bharatiya Nyaya Sanhita, 2023 / Indian Penal Code, 1860.
3. Protection of Children from Sexual Offences Act, 2012.
4. Digital Personal Data Protection Act, 2023.
5. *Shreya Singhal v. Union of India*, (2015) 5 SCC 1.
6. *Justice K.S. Puttaswamy v. Union of India*, (2017) 10 SCC 1.
7. *State of West Bengal v. Animesh Boxi*, (2018).
8. *Just Rights for Children Alliance v. S. Harish*, 2024 INSC 716.
9. Law Commission of India Reports on Cyber Law.
10. Ministry of Electronics and Information Technology, Government of India Reports.