

CYBERBULLYING: LEGAL CHALLENGES AND SOLUTIONS IN THE DIGITAL ERA

Shagun Sharma^{*}
Dr. Pooja Sood^{**}

ABSTRACT

The rapid expansion of digital technology has fundamentally transformed social interaction, shifting substantial dimensions of everyday life from offline to online space and, with that shift, giving rise to a distinctive form of harassment now widely termed cyberbullying. The COVID-19 pandemic considerably intensified this problem, with both adolescents and adults experiencing increased online abuse and the severe physical, emotional and psychological harm it inflicts. This paper critically examines the legal framework governing cyberbullying in India, situating the Information Technology Act, 2000, its 2008 amendment, and the relevant provisions of the Bharatiya Nyaya Sanhita, 2023 within a comparative survey of international legal standards from the United States, Canada and Australia. It traces judicial engagement with online harassment from the Supreme Court's landmark invalidation of Section 66A of the Information Technology Act in Shreya Singhal v. Union of India through to the Delhi High Court's more recent recognition, in 2025, that cyberbullying can inflict psychological trauma comparable to physical violence, particularly upon children. The paper identifies persistent structural obstacles to effective enforcement, including offender anonymity, cross-border jurisdictional limitation, inconsistent enforcement practice and the continuing absence of a statutorily defined offence of cyberbullying in Indian law, and it proposes reform directed at closing this definitional and enforcement gap without compromising the constitutional guarantee of free expression Shreya Singhal itself vindicated.

KEYWORDS: Cyberbullying; Online Harassment; Information Technology Act; Digital Safety; Cybercrime Law.

1. INTRODUCTION

Cyberbullying has emerged, over the past decade, as one of the most pressing concerns accompanying the expanding use of digital technology. Classical bullying is understood as unethical conduct rooted in an unequal distribution of power between individuals, whether adolescent or adult, in which a comparatively weaker victim bears the resulting harm.¹ Cyberbullying denotes the specific instance of this conduct carried out through modern technology: the intentional, malicious harassment, intimidation or defamation of a person through social media platform or messaging application, encompassing conduct such as spreading false rumour, issuing threat, and impersonation. The prevalence of cyberbullying has risen in step with growing internet reliance, and individuals across every age group, children, teenager and adult alike, remain vulnerable to it. The term was first coined by Bill Belsey, whose work helped

^{*} Research Scholar, Department of Laws, Panjab University, Chandigarh.

^{**} Chairperson & Associate Professor, University Institute of Legal Studies, PUSSGRC, Hoshiarpur.

¹ Dan Olweus, *Bullying at School: What We Know and What We Can Do 9-14* (Blackwell 1993).

establish cyberbullying as a distinct object of study and policy concern in the digital age.

Cyberbullying differs materially from its traditional counterpart precisely because of the medium through which it operates: unlike bullying confined to physical space, cyberbullying occurs in a virtual environment that is frequently harder to detect and correspondingly harder to control. The internet, notwithstanding its considerable benefit, exposes users to a range of associated risk, online harassment, phishing, cyber fraud, voyeurism, cyberstalking and cyberbullying among them, and offenders exploit digital platforms not merely to express hostility toward a victim but to convey communication specifically calculated to intimidate, humiliate or harass. The scale at which such communication can now travel, from one person to another, from one person to many, or from many to many across the globe simultaneously, has transformed what was once a localised social harm into a considerably more pervasive and difficult-to-contain one, and the continual emergence of new communication technology, from early SMS and email through to contemporary social media and messaging platform, has correspondingly expanded the toolkit available to those inclined to misuse it.

1.1 Objectives of the Study

This study aims to analyse the legal definition, nature and distinguishing feature of cyberbullying relative to other forms of online abuse, including how different legal systems categorise cyberbullying as either a criminal or civil wrong, and to examine the existing legal framework governing cyberbullying at both the national and international level, with a view to identifying reform capable of closing the gaps that framework presently exhibits.

1.2 Research Methodology

This study adopts a doctrinal and analytical methodology, drawing on both primary and secondary legal source. Primary source include statutory law, case law and judicial pronouncement addressing cyberbullying and related online harm; secondary source, including books, journal article, official report and online publication, are reviewed to supply the comparative and policy context this paper's analysis requires.

1.3 Scope

This paper confines its analysis to cyberbullying as a distinct category of online harm, drawing comparative material from the United States, Canada and Australia specifically, and examines Indian statutory and judicial development through August 2026. It does not undertake a comprehensive survey of cybercrime law generally, addressing adjacent offence, financial fraud and cyberterrorism among them, only where directly relevant to the cyberbullying-specific analysis this paper undertakes.

2. THE EVOLUTION AND NATURE OF CYBERBULLYING

The word bully traces to the 1530s, and the concept it denotes has always presupposed both a bully and a victim, with the bully engaging in direct, verbal or indirect practice intended to harass the victim physically or mentally. A significant driver of bullying's persistence and evolution, researchers suggest, lies in a competitive impulse to establish dominance over perceived rivals.² Research indicates that a substantial majority of teenagers, roughly four in five by some estimate, have experienced cyberbullying at some point, a finding of particular concern given adolescence's status as a formative developmental stage. A multinational study conducted across twenty-eight countries in 2005 documented considerable cross-national variation in bullying prevalence and its associated harm, confirming both the phenomenon's consistency across cultural context and the meaningful differences national policy and social condition can produce in its severity.

Bullying's early, predominantly physical form carried genuine harm, but cyberbullying, enabled by social media and other virtual platform, has achieved a considerably wider reach and, in many documented instance, a correspondingly more severe impact. Cyberbullies have developed numerous techniques for confronting and demeaning their targets, techniques whose underlying intention, whether pursued for amusement, gratification or revenge, remains directed at damaging the victim's sentiment, emotional wellbeing and public image across the social media environment the offender and victim share.

Contemporary typology generally distinguishes several recurring forms cyberbullying takes: flaming, involving hostile, aggressive online exchange; harassment, involving repeated, targeted offensive messaging; denigration, involving the circulation of harmful or false statement about a person; impersonation, involving the fraudulent adoption of another's online identity; outing and trickery, involving the disclosure of private information obtained through deception; exclusion, involving deliberate removal from an online group or community; and cyberstalking, involving persistent, threatening surveillance and contact.³ Each form carries distinct evidentiary and enforcement characteristic, a distinction India's own statutory framework, examined in this paper's Section 5, does not presently draw with any consistency, leaving prosecutors and courts to map each specific fact pattern onto provisions drafted for adjacent, but not identical, conduct.

² Christina Salmivalli, *Bullying and the Peer Group: A Review*, 15 *Aggression & Violent Behav.* 112 (2010).

³ Nancy E. Willard, *Cyberbullying and Cyberthreats: Responding to the Challenge of Online Social Aggression, Threats, and Distress* 5-12 (Research Press 2007).

3. THE PSYCHOLOGICAL, SOCIAL AND LEGAL IMPACT OF CYBERBULLYING

Cyberbullying's negative impact extends across the individual, societal and legal domain simultaneously. Victims, spanning children, adolescent and adult alike, commonly experience psychological distress, anxiety, depression and, in the most severe documented instance, suicidal ideation. The anonymity many perpetrators enjoy, combined with the speed at which harmful content can circulate, compounds the difficulty victims face in securing timely justice, and the resulting strain on social relationship, academic and professional performance, and overall wellbeing can prove considerable and lasting.⁴ At a broader societal level, cyberbullying challenges prevailing social norm, disrupts social harmony and fosters a culture of online hostility whose consequence extend well beyond any individual victim.

From a legal perspective, cyberbullying's inherently cross-border character presents a distinctive enforcement obstacle, complicating both the practical enforcement of law and the prosecution of offenders operating from a jurisdiction distinct from the victim's own. Legal systems must simultaneously balance protection for free expression against the imperative of victim protection, and social media platforms continue to struggle with the practical challenge of moderating user-generated content effectively at the scale contemporary platforms operate. Addressing these accumulated harm requires a genuinely global, harmonised response, encompassing robust statutory framework, cross-border legal cooperation, expanded digital literacy and continued technological innovation directed at detecting and preventing cyberbullying before it inflicts lasting harm.

Empirical research on adolescent mental health specifically has documented a measurable association between sustained cyberbullying victimisation and elevated risk of clinical depression, anxiety disorder and, in the most severe case, suicidal ideation and attempt, an association researchers attribute in part to cyberbullying's distinctive persistence: unlike a physical bullying episode confined to a specific time and place, cyberbullying content can remain accessible indefinitely, be repeatedly re-encountered by the victim, and continue circulating among peers long after the original act of posting.⁵ This persistence dimension distinguishes cyberbullying's psychological profile meaningfully from that of traditional bullying, and it supplies part of the doctrinal justification the Delhi High Court articulated in the 2025 decision this paper's Section 6.3 examines, recognising that the harm digital harassment inflicts does not diminish merely because it lacks physical contact.

⁴ Sameer Hinduja & Justin W. Patchin, *Bullying, Cyberbullying, and Suicide*, 14 *Archives Suicide Res.* 206 (2010).

⁵ Sameer Hinduja & Justin W. Patchin, *supra* note 6.

3. THE PSYCHOLOGICAL, SOCIAL AND LEGAL IMPACT OF CYBERBULLYING

Cyberbullying's negative impact extends across the individual, societal and legal domain simultaneously. Victims, spanning children, adolescent and adult alike, commonly experience psychological distress, anxiety, depression and, in the most severe documented instance, suicidal ideation. The anonymity many perpetrators enjoy, combined with the speed at which harmful content can circulate, compounds the difficulty victims face in securing timely justice, and the resulting strain on social relationship, academic and professional performance, and overall wellbeing can prove considerable and lasting. At a broader societal level, cyberbullying challenges prevailing social norm, disrupts social harmony and fosters a culture of online hostility whose consequence extend well beyond any individual victim.

From a legal perspective, cyberbullying's inherently cross-border character presents a distinctive enforcement obstacle, complicating both the practical enforcement of law and the prosecution of offenders operating from a jurisdiction distinct from the victim's own. Legal systems must simultaneously balance protection for free expression against the imperative of victim protection, and social media platforms continue to struggle with the practical challenge of moderating user-generated content effectively at the scale contemporary platforms operate. Addressing these accumulated harm requires a genuinely global, harmonised response, encompassing robust statutory framework, cross-border legal cooperation, expanded digital literacy and continued technological innovation directed at detecting and preventing cyberbullying before it inflicts lasting harm.

Empirical research on adolescent mental health specifically has documented a measurable association between sustained cyberbullying victimisation and elevated risk of clinical depression, anxiety disorder and, in the most severe case, suicidal ideation and attempt, an association researchers attribute in part to cyberbullying's distinctive persistence: unlike a physical bullying episode confined to a specific time and place, cyberbullying content can remain accessible indefinitely, be repeatedly re-encountered by the victim, and continue circulating among peers long after the original act of posting. This persistence dimension distinguishes cyberbullying's psychological profile meaningfully from that of traditional bullying, and it supplies part of the doctrinal justification the Delhi High Court articulated in the 2025 decision this paper's Section 6.3 examines, recognising that the harm digital harassment inflicts does not diminish merely because it lacks physical contact.

4. COMPARATIVE INTERNATIONAL LEGAL STANDARDS

4.1 The United States

The United States occupies a leading position in cybercrime and child protection legislation specifically. The Children's Online Privacy Protection Act, 1998 safeguards the personal information of children under thirteen, mandating parental consent before any personal data collection from a child, an important structural protection for children navigating digital space.⁶ The Child Online Protection Act separately criminalised the dissemination of harmful content to children online, including content facilitating cyberbullying and online sexual exploitation, supplying American authorities with a further legal instrument for tracking offenders whose conduct specifically targets children's mental and social wellbeing.

International bodies, including the United Nations and the Council of Europe, have separately advocated harmonised regulation, capacity-building initiative and enhanced inter-state cooperation to address cyberbullying's inherently transnational character. Proposed solutions include model law adoption, intermediary liability for social media platform, and digital literacy programming, together intended to secure an online environment upholding the dignity and rights of vulnerable groups, children and adolescents foremost among them.

4.2 Canada and Australia

Canada addresses child protection in digital space substantially through the Personal Information Protection and Electronic Documents Act, which governs the collection, use and disclosure of personal information in commercial activity and requires parental consent before a company may collect personal data from a child, extending meaningful protection against violation arising from cyberbullying specifically.⁷ Australia has enacted comparable protection through legislation criminalising cyberbullying and online sexual exploitation of children, complemented by a Digital Safety Strategy for Children directed at raising awareness of online cybercrime and supplying practical remedy for affected children and their families.⁸ Australia's eSafety Commissioner, established under this framework, supplies a dedicated regulatory body with authority to order the removal of cyberbullying material targeting an Australian child, a model this paper's Section 8 recommendations draw upon directly in proposing comparable Indian institutional reform.

⁶ Children's Online Privacy Protection Act, 15 U.S.C. §§ 6501-6506 (1998).

⁷ Personal Information Protection and Electronic Documents Act, S.C. 2000, c. 5 (Can.).

⁸ Online Safety Act 2021 (Cth) (Austl.).

5. THE LEGISLATIVE FRAMEWORK GOVERNING CYBERBULLYING IN INDIA

The Information Technology Act, 2000, as amended in 2008, constitutes the principal legislative instrument addressing internet and cyberspace offence in India, together with the associated penalty for their commission. India's legislative framework for cyberbullying specifically continues to evolve alongside the rapid growth of social media and online interaction, though no standalone statute presently criminalises cyberbullying as a distinct offence, leaving victims to seek recourse through provisions drafted for related, if not identical, conduct.

Section 66E of the Information Technology Act penalises violation of privacy, and Section 67 penalises the transmission of obscene content online, both provisions of direct relevance to cyberbullying conduct involving image-based abuse or the non-consensual circulation of private material.⁹ The Bharatiya Nyaya Sanhita, 2023 supplies further relevant provision: Section 351 addresses criminal intimidation, Section 356 addresses defamation, and Section 352 addresses intentional insult calculated to provoke a breach of peace, provisions functionally continuing the protection the corresponding Indian Penal Code sections previously supplied.¹⁰ The Bharatiya Nyaya Sanhita additionally strengthens protection against conduct frequently accompanying cyberbullying specifically, Section 77 addressing voyeurism, the non-consensual watching, photographing or recording of a person in a private moment, Section 78 addressing stalking, encompassing repeated unwanted surveillance and communication, and Section 351(4) addressing criminal intimidation conveyed anonymously, each provision considerably relevant to the digital harassment context this paper examines.¹¹ The Digital Personal Data Protection Act, 2023 further strengthens this framework by protecting data privacy and imposing accountability obligation on social media platform, a data-protection dimension complementing the criminal law provisions this section has traced.

The Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021 supply a further, procedural layer of protection specifically relevant to cyberbullying: they require significant social media intermediaries to establish a grievance redressal mechanism and to remove flagged unlawful content within a prescribed timeline upon receiving a valid complaint, including complaint concerning content that exposes the private area

⁹ Information Technology Act, 2000, §§ 66E, 67, No. 21, Acts of Parliament, 2000 (India).

¹⁰ Bharatiya Nyaya Sanhita, 2023, §§ 351, 352, 356, No. 45, Acts of Parliament, 2023 (India).

¹¹ Bharatiya Nyaya Sanhita, 2023, §§ 77-78, 351(4), No. 45, Acts of Parliament, 2023 (India).

of an individual or depicts them in a sexually explicit context.¹² This intermediary-facing obligation operates alongside the criminal provisions this section has already traced, supplying victims a comparatively faster, platform-level avenue for content removal that does not depend upon the outcome of a criminal prosecution, though the Rules themselves stop short of defining cyberbullying as a distinct category of prohibited content, leaving platforms to map complaint against the same patchwork of adjacent statutory category this paper's Section 7 identifies as a continuing source of definitional ambiguity.

6. JUDICIAL RESPONSES: FROM SHREYA SINGHAL TO CONTEMPORARY JURISPRUDENCE

Indian courts have engaged with online harassment and cyberbullying across a developing body of case law, from the constitutional invalidation of an overbroad criminal provision to more recent recognition of the genuine psychological harm cyberbullying inflicts.

6.1 Shreya Singhal v. Union of India (2015)

*Shreya Singhal v. Union of India*¹³ addressed the constitutionality of Section 66A of the Information Technology Act, which had penalised sending offensive message through electronic communication. The Supreme Court held the provision unconstitutional for infringing Article 19(1)(a)'s guarantee of free speech and expression, finding that terms such as offensive and annoying were impermissibly vague and consequently susceptible to misuse. The decision underscored the need for clarity and precision in cybercrime legislation, a principle this paper's Section 5 discussion of the current statutory landscape must itself satisfy if future cyberbullying-specific legislation is to withstand comparable constitutional scrutiny.

6.2 Ritu Kohli (2001) and S. Pradeep Kumar v. Union of India (2012)

The Ritu Kohli case, one of India's earliest documented instances of cyberstalking, involved an unknown individual impersonating the complainant online and disclosing her home address to strangers, resulting in unsolicited contact at all hours. Police registered the case under Section 509 of the then Indian Penal Code, addressing insult to the modesty of a woman, together with Sections 67 and 72 of the Information Technology Act, and the episode marked an early moment of public and institutional awareness regarding cyberstalking

¹² Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021, Rule 3, No. 139 (India).

¹³ *Shreya Singhal v. Union of India*, (2015) 5 S.C.C. 1 (India).

specifically, highlighting the need for a legal provision addressing the conduct more directly.¹⁴

In *S. Pradeep Kumar v. Union of India*¹⁵, the complainant alleged that a colleague had circulated defamatory email about him to his employer and professional peers, and the accused was charged under Section 66A. The defence argued that defamatory content could not properly be classified as grossly offensive within the meaning of that section, a contention that exposed the same interpretive overreach the Supreme Court would later confirm in *Shreya Singhal*, and the case is accordingly frequently cited as contributing to the eventual constitutional challenge that provision faced.

6.3 Contemporary Judicial Recognition: The 2025 Delhi High Court Ruling

Judicial recognition of cyberbullying's genuine psychological severity has deepened considerably in recent case law. In a 2025 decision upholding a conviction under the Protection of Children from Sexual Offences Act and related provision, arising from the morphing of a minor girl's face onto explicit imagery accompanied by threatening message, the Delhi High Court held that cyberbullying, though faceless and silent, can prove as mentally traumatic and scarring as physical violence, particularly where directed at a child.¹⁶ The Court characterised the case as a textbook example of cyberbullying, observing that a morphed image, once created and circulated, can inflict lasting damage to a child's mental health, dignity and reputation, and that the fear of circulation alone, even absent actual publication, suffices to terrorise a young mind. The Court further held that the creation of safe environment for children cannot remain confined to physical space alone, extending that protective obligation explicitly to digital space, a holding of considerable doctrinal significance for the broader cyberbullying framework this paper examines, since it locates the harm cyberbullying inflicts squarely within the constitutional and statutory protection Indian child protection law already recognises rather than treating it as a lesser, merely virtual harm.

A related line of authority addresses the non-consensual circulation of intimate imagery specifically, a form of image-based cyberbullying and harassment with particularly severe consequence for victims. In *X v. Union of India*¹⁷, the Delhi High Court, confronting the re-publication of a victim's private photograph on a pornographic website after an earlier removal order had proven ineffective, appointed a cyber law expert as *amicus curiae* and directed

¹⁴ Ritu Kohli Case, Delhi Police, F.I.R. No. 208 (2001).

¹⁵ *S. Pradeep Kumar v. Union of India*, W.P. (C) (Madras High Court, 2012).

¹⁶ *X v. State (NCT of Delhi)*, CrI. A. (Delhi High Court, 2025) (Sharma, J.).

¹⁷ *X v. Union of India*, W.P. (C) (Delhi High Court).

both the removal of unlawfully published content and its de-indexing from search engine results, emphasising the need for immediate and efficacious remedy in cases of this kind while balancing intermediary obligation against user right. The decision illustrates the practical remedial architecture courts have begun to develop for image-based online harassment specifically, extending beyond the criminal law provisions this paper's Section 5 has traced into civil and injunctive relief capable of addressing the ongoing, self-replicating harm such content can inflict once released online.

7. PERSISTING CHALLENGES IN COMBATING CYBERBULLYING

Notwithstanding the legislative and judicial development this paper has traced, several persistent obstacles continue to complicate effective enforcement against cyberbullying.

- Anonymity and platform reach: cyberbullies frequently operate behind fabricated profile, evading identification and accountability, and readily create replacement accounts should an existing one face suspension, a pattern that emboldens offenders and frustrates enforcement effort considerably.
- Cross-border jurisdiction: cyberbullying frequently involves an offender and victim located in different countries, and the resulting variation in national legal framework, enforcement protocol and inter-state cooperation considerably complicates investigation, identification and prosecution across jurisdictional boundary.
- Under-reporting driven by limited awareness: many victims remain unaware they are being victimised in a manner the law recognises, or unaware of the reporting mechanism available to them, leaving cases unresolved and permitting harm, including serious mental health consequence, to continue unaddressed.
- Inconsistent enforcement: existing legal framework, notwithstanding formal availability, is applied unevenly, with some jurisdictions pursuing meaningful legal reform and awareness campaign while others lag considerably behind in developing robust institutional response.
- Definitional ambiguity: the absence of a universally accepted definition of cyberbullying, frequently referred to instead as online or electronic harassment, produces genuine interpretive difficulty; Indian law specifically contains no dedicated statutory definition of cyberbullying, a gap this paper's Section 5 discussion has already identified and this paper's recommendations directly address.

8. CONCLUSION AND RECOMMENDATIONS

Cyberbullying constitutes a genuine global threat to individual mental wellbeing and to broader societal cohesion. Notwithstanding existing legislative measure, regulation and awareness campaign, a considerably more harmonised approach remains necessary to address it effectively, and the jurisdictional, enforcement and definitional variation across countries this paper's Section 7 has documented continues to complicate prosecution considerably. Several jurisdictions, the United States, Canada, the United Kingdom and Australia among them, have taken meaningful institutional step toward addressing this problem, including dedicated regulatory body such as Australia's eSafety Commissioner and the United Kingdom's Online Safety Act framework, yet cross-border jurisdictional limitation remains the single greatest obstacle these institutions continue to confront.

The following reforms would strengthen India's legal and institutional response to cyberbullying specifically.

- Adopt a statutory definition of cyberbullying, drafted with the precision Shreya Singhal requires to withstand constitutional scrutiny, to close the definitional gap Section 5 and Section 7 have identified and to supply enforcement agencies with clear, actionable statutory language.
- Establish extradition-compatible cross-border cooperation mechanism, enabling participating countries to exercise jurisdiction over offenders whose conduct victimises a person within the victim's own country, addressing the jurisdictional obstacle this paper's Section 7 identifies as the most persistent challenge international bodies presently confront.
- Require social media platforms to deploy artificial intelligence-based detection tools capable of identifying and removing cyberbullying content proactively, before it reaches or is widely viewed by an intended victim, extending the removal and de-indexing remedy the Delhi High Court has already developed in the image-based harassment context to broader, earlier-stage content moderation.
- Establish a dedicated Indian regulatory body, modelled on Australia's eSafety Commissioner, empowered to order expedited content removal in verified cyberbullying case, particularly those involving minor victim, supplying a specialised institutional alternative to the ordinary criminal process this paper's Section 5 and Section 6 examine.

- Expand school-based digital literacy and awareness programming, recognising, consistent with the Delhi High Court's 2025 ruling examined in Section 6.3, that children and adolescents remain cyberbullying's most vulnerable victims and that schools accordingly bear a meaningful role in fostering safer online environment and responsible digital conduct among their students.

Addressing cyberbullying demands a genuinely multifaceted response: strengthened legal framework, expanded public awareness, and international cooperation capable of overcoming the jurisdictional challenge this paper has traced throughout. Defining cyberbullying with precision in both national and international law remains essential to equipping enforcement agency with the tools necessary to identify, track and prosecute offenders effectively; absent these measures, the psychological, mental and emotional harm cyberbullying inflicts upon its victims will continue largely unabated, a cost this paper's recommendations are directed at reducing without compromising the constitutional protection for free expression Indian courts have rightly insisted any cybercrime framework must respect.