(JOINT JURIST)

[NATIONAL-LEVEL | PEER-REVIEWED | OPEN-ACCESS LEGAL JOURNAL]

| VOLUME 1 | ISSUE 1 | MAY 2026

ABOUT THE JOURNAL

The **Joint Jurist** is a strictly law-focused national publication designed to bridge the gap between academic research and litigation expertise. We operate on a **Double-Blind Peer-Review** model, ensuring that every published work meets the highest standards of original scholarship and academic integrity. Our platform is dedicated to providing an openaccess environment for legal professionals, scholars, and students to contribute to the evolving legal discourse.

EDITORIAL & ADVISORY BOARD

The Joint Jurist Journal is guided by a distinguished panel of legal luminaries and academicians committed to fostering excellence in legal scholarship.

- **Advocate Suraj Shandil**
- **Dr. Seema Gupta**
- **Dr. Mohd Rafiq**
- **Dr. Harshita Thalwal**
- **Ms. Sabrina Bath**
- **Ms. Soumya Sharma**

NAME	DESIGNATION	INSTITUTION/AFFILIATION	SPECIALIZATION & IMPACT
Advocate Suraj Shandil	Founder, CEO & Editor-in-Chief	**High Court of Himachal Pradesh**	IPR Specialist, Courtroom Strategy & Legal Research.
Prof. (Dr.) Seema Gupta	Editorial Board Member	**Associate Professor / Chandigarh University (CU)**	Constitutional Law, IPR, & Supreme Court Certified Mediator/ Interdisciplinary Legal Studies.

| VOLUME 1 | ISSUE 1 |APRIL- MAY 2026

"CYBERBULLYING AND ONLINE HARASSMENT IN INDIA: LEGAL FRAMEWORK AND JUDICIAL RESPONSE"

AUTHOR:- DIVYA THAKUR / Research Scholar/ Department of Laws,

Himachal Pradesh University, Summerhill, Shimla, Himachal Pradesh (171005)

ABSTRACT

The rapid growth of digital communication platforms in India has led to a significant rise in cyberbullying and online harassment, particularly against women, children, and marginalized communities. Despite the presence of legal provisions under the Information Technology Act, 2000, the Indian Penal Code, 1860, and related legislations, the existing legal framework remains fragmented and inadequate to effectively address the evolving nature of online abuse. This article critically examines the statutory framework governing cyberbullying and online harassment in India and analyses important judicial decisions that have shaped legal responses in this area. It further explores the practical challenges affecting enforcement, including anonymity of offenders, underreporting of offences, lack of digital expertise, and jurisdictional complexities. The article also evaluates recent developments such as the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021 and the Digital Personal Data Protection Act, 2023. It argues for the urgent need for a comprehensive and dedicated anti-cyberbullying legislation that clearly defines offences, strengthens intermediary accountability, and ensures effective victim-centric remedies. The article concludes with recommendations aimed at improving legislative clarity, enforcement mechanisms, and digital safety in India.

Keywords: *Cyberbullying, Online Harassment, Information Technology Act 2000, Indian Penal Code, Intermediary Liability, Digital Personal Data Protection Act 2023, Judicial Response.*

I. INTRODUCTION

India's digital revolution has fundamentally transformed the social, economic, and communicative landscape of the country. Over the last two decades, rapid internet penetration, affordable smartphones, and the widespread use of social media platforms have significantly increased online interaction among individuals across all age groups. As of 2023, India emerged as one of the largest digital populations in the world, with more than 900 million internet users actively participating in online spaces[1] While this digital expansion has created immense opportunities for communication, education, commerce, and freedom of expression, it has simultaneously given rise to serious challenges in the form of cybercrime and online abuse. Among these challenges, Cyberbullying and online harassment have emerged as pressing concerns requiring urgent legal and institutional attention. Cyberbullying refers to the use of digital technologies and electronic communication to intimidate, threaten, harass, humiliate, or target an individual repeatedly.[2]

Online harassment includes a broader range of abusive conduct carried out through digital platforms, including cyberstalking, trolling, impersonation, dissemination of private information, body shaming, sexual harassment, hate speech, and defamatory content. Unlike traditional forms of bullying, cyberbullying is not restricted by physical boundaries and often occurs continuously through social media platforms, messaging applications, gaming forums, and other online spaces. The permanence and viral nature of digital content further aggravate the harm suffered by victims, causing emotional trauma, psychological distress, reputational damage, and social isolation.

The issue has become particularly alarming in the Indian context due to increasing internet accessibility among young people and the growing dependence on digital communication in everyday life. Women, children, adolescents, journalists, activists, and members of marginalized communities are especially vulnerable to online abuse and targeted harassment.[3]

The problem is not merely technological but deeply structural. The anonymity that the internet affords to perpetrators, the trans boundary nature of online conduct, the inadequacy of investigative infrastructure, and the social stigma that discourages victims ,especially women and children from reporting incidents collectively render cyberbullying one of the most underreported and under-prosecuted offences in the country. According to the National Crime Records Bureau, cybercrime complaints in India rose from approximately 44,546 in 2019 to over 96,000 in 2022, with a substantial proportion relating to online harassment and cyberbullying.[4] The rise in online interaction following the COVID 19 pandemic further accelerated the exposure of individuals to cyberbullying and online victimisation.

The legal framework governing cyberbullying and online harassment in India is fragmented and largely indirect in nature. The Information Technology Act, 2000 serves as the primary legislation dealing with cyber offences in India. However, the statute was originally enacted to facilitate electronic governance and electronic commerce rather than to address victim centric concerns such as online harassment and digital abuse. Although the 2008 amendment introduced provisions dealing with certain cyber offences, the legislation still lacks a comprehensive definition or dedicated framework specifically addressing cyberbullying.

In addition to the Information Technology Act, several provisions of the Indian Penal Code, 1860 have been applied to online misconduct through judicial interpretation. Provisions relating to criminal intimidation, defamation, obscenity, stalking, harassment, and insult to modesty have frequently been invoked in cases involving cyberbullying and online abuse. Nevertheless, these provisions were designed primarily for conventional offences occurring in physical spaces and therefore often fail to adequately address the complexities of digital misconduct.

The judiciary has played a crucial role in shaping the legal discourse concerning online speech and cyber harassment in India. Courts have consistently attempted to balance the constitutional guarantee of freedom of speech and expression with the need to protect individuals from online abuse and violations of dignity and privacy. Important judicial pronouncements, including Shreya Singhal v. Union of India,[5] have significantly influenced the contours of cyber law jurisprudence in India. Judicial decisions have also highlighted the limitations of the existing statutory framework and the need for stronger safeguards against online harassment.

Despite legislative and judicial efforts, several structural gaps continue to weaken India's response to cyberbullying and online harassment. The absence of specialised legislation, lack of uniform standards for intermediary accountability, procedural inefficiencies, and inadequate victim support mechanisms remain major concerns. The rapidly evolving nature of digital technology further demands continuous legal adaptation to ensure effective protection of individuals in cyberspace.

Against this background, the present article critically examines the legal framework governing cyberbullying and online harassment in India and analyses the role of the judiciary in addressing these challenges. Part II of the article discusses the conceptual understanding and various forms of cyberbullying and online harassment. Part III examines the statutory framework under the Information Technology Act and the Indian Penal Code. Part IV analyses important judicial pronouncements shaping the legal landscape in this area. Part V identifies the major shortcomings within the current framework and proposes recommendations aimed at developing a more comprehensive and victim oriented legal response to cyberbullying in India.

II. CONCEPTUAL CONTOURS OF CYBERBULLYING

Cyberbullying, while frequently used interchangeably with online harassment, carries specific connotations. It typically involves a power imbalance between the perpetrator and the victim, repetitive conduct, and the use of digital or electronic means. Indian law does not provide a statutory definition of cyberbullying, which itself constitutes a foundational lacuna. In its absence, courts and law enforcement agencies have applied existing IPC and IT Act provisions on a case-by-case basis.

The principal forms of cyberbullying manifest in India include: (i) cyberstalking—persistent monitoring, messaging, or tracking of a victim using digital platforms; (ii) online defamation—posting false or malicious content on social media to damage the victim's reputation; (iii) morphing—digitally altering the victim's images, typically with sexual intent, and circulating them online; (iv) doxing—publicly revealing private information about a person without consent; (v) trolling—sending abusive, threatening, or derogatory messages; and (vi)

impersonation—creating fake profiles of victims to tarnish their image or conduct fraudulent activities.[6]

A 2022 report of the National Commission for Women recorded a 36 per cent increase in online harassment complaints filed by women between 2020 and 2022, with the most frequently reported offences being morphing, cyberstalking, and non-consensual sharing of intimate images.[7]

III. THE STATUTORY FRAMEWORK

A. The Information Technology Act, 2000

The IT Act, as amended by the Information Technology (Amendment) Act, 2008, constitutes the primary legislative instrument addressing cyber offences. Section 66C penalises identity theft, section 66E addresses violation of privacy through the publication of private images, section 67 prohibits publication of obscene material in electronic form, and section 67A specifically penalises material containing sexually explicit acts.[8]

Section 66A of the IT Act, which had been routinely invoked to prosecute online speech deemed "offensive" or "menacing," was struck down by the Supreme Court of India in Shreya Singhal v. Union of India as unconstitutional, being an unreasonable restriction on freedom of speech and expression under Article 19(1)(a) of the Constitution. The Court found the provision vague, overbroad, and susceptible to misuse against legitimate political expression. The absence of Section 66A has created a legislative vacuum particularly with respect to online harassment that falls short of criminal intimidation under the IPC.[9]

The IT (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021 impose due diligence obligations on intermediaries and social media platforms. Rule 3(1)(b) requires platforms to inform users against uploading harassing or privacy-invasive content, while Rule 4(2) mandates significant social media intermediaries to enable identification of the first originator of information in specific circumstances. However, the Rules have faced criticism for their potential chilling effect on free expression and remain a contested legal instrument.[10][11]

B. The Indian Penal Code, 1860

Several provisions of the IPC have been extended to online conduct by courts. Section 354D, inserted by the Criminal Law (Amendment) Act, 2013, criminalises stalking—including electronic surveillance—and is directly applicable to cyberstalking. Section 354A addresses sexual harassment, section 499 covers defamation, section 503 penalises criminal intimidation, and sections 506–507 address threats made in anonymous or pseudonymous communications.[12][13]

The applicability of these provisions to cyber offences has been judicially affirmed in several decisions. In Rajiv Dinesh Gadkari v. State of Maharashtra, the Bombay High Court confirmed that section 499 of the IPC extends to defamatory content posted on social media platforms, holding that the medium of communication does not limit the scope of the offence.[14]

C. Special Legislation: POCSO Act, 2012

The Protection of Children from Sexual Offences Act, 2012 (POCSO) addresses online sexual exploitation of children under sections 13 and 14, which criminalise the use of a child for

pornographic purposes, including the creation, distribution, or viewing of child sexual abuse material through digital means. The Act has a broad ambit and is increasingly invoked in cases involving online grooming and morphing of images of minors.[15]

IV. JUDICIAL RESPONSE: KEY CASES

The Ritu Kohli Case (2005) is widely regarded as the first cyberstalking case to be registered in India. A Delhi resident, Ritu Kohli, was harassed by her stalker who posted her personal contact details on obscene chat rooms and encouraged strangers to call her at all hours. The accused was booked under section 509 of the IPC for outraging the modesty of a woman and section 67 of the IT Act. The case prompted the Delhi Police to establish a dedicated Cyber Crime Cell and brought national attention to the inadequacy of existing provisions.[16]

In Manish Kathuria v. State (2001), the accused impersonated a woman on an online chat platform, posted her mobile number, and induced others to send her obscene messages. He was arrested under section 509 of the IPC and section 67 of the IT Act. The case was among the first to judicially recognise online impersonation as a form of harassment and established that digital anonymity does not confer legal immunity.[17]

In Balu v. State of Tamil Nadu (2019), a Sessions Court in Chennai convicted the accused for cyberstalking and morphing the photographs of the victim—a college student—and circulating them through messaging applications. The conviction was sustained under sections 354D and 509 of the IPC and section 66E of the IT Act, and the Court imposed a sentence of rigorous imprisonment of two years along with a fine. The case is significant as it represented one of the first judgments in Tamil Nadu imposing a custodial sentence specifically for image morphing.[18]

In a 2021 sessions case before a Mumbai court, the accused was convicted under sections 354A and 499 of the IPC and section 67A of the IT Act for morphing and circulating sexually explicit composite images of the victim—a marketing professional—across social media platforms. The Court took a strict view of the gravity of reputational and psychological harm suffered by the victim and awarded the maximum sentence under section 67A.[19]

In Vikas Garg v. State of Haryana (2017), the Punjab and Haryana High Court, while adjudicating an appeal in a related matter, took suo motu cognisance of the role of social media platforms in the propagation of cyberbullying and called upon the State government to enforce existing legal provisions more rigorously and to conduct awareness campaigns regarding cyber safety.[20]

V. CRITICAL GAPS AND RECOMMENDATIONS

A. Absence of a Comprehensive Definition

The most fundamental gap in Indian law is the absence of a statutory definition of cyberbullying. Without a clear, inclusive definition, enforcement agencies face interpretive difficulties and courts are forced to stretch existing provisions. The Law Commission of India, in its 267th Report on Hate Speech, identified the need for specific legislative provisions to address online harassment and recommended amendments to the IPC.[21]

B. Platform Accountability and Safe Harbour

Section 79 of the IT Act provides intermediaries with a safe harbour from liability for third-party content subject to due diligence compliance. The 2021 Intermediary Rules have partially addressed this by imposing takedown obligations and grievance redressal mechanisms, but the time-bound compliance requirements remain weak and the penalties for non-compliance are insufficiently deterrent. India should consider adopting a tiered liability framework that incentivises proactive content moderation by platforms.[22]

C. Data Protection and Victim Privacy

The Digital Personal Data Protection Act, 2023, while constituting a significant legislative development in India's data governance architecture, does not directly address cyberbullying. However, its provisions on data minimisation, purpose limitation, and the right to erasure carry indirect protective value for victims of online harassment whose personal data is weaponised by perpetrators. The Act's special provisions for children under section 9 are particularly relevant in the context of cyberbullying of minors.[23]

D. International Cooperation

The transboundary nature of cyberbullying necessitates robust international cooperation frameworks. India is not a signatory to the Budapest Convention on Cybercrime, which provides the most comprehensive multilateral framework for mutual legal assistance in cybercrime investigations. India's refusal to accede to the Convention on grounds of sovereignty concerns has hampered cross-border investigations and enforcement of orders against foreign-based perpetrators and platforms.[24]

E. Legislative Recommendations

The article advances the following recommendations: First, Parliament should enact a dedicated Cyberbullying Prevention and Protection Act that provides a comprehensive statutory definition, consolidates existing scattered provisions, establishes fast-track courts for cybercrime adjudication, and creates a centralised compensation fund for victims. Second, the National Cyber Security Policy should be updated to specifically address cyberbullying as a distinct threat category. Third, intermediaries should be required to implement automated detection mechanisms and transparent content removal policies with mandatory reporting obligations to law enforcement. Fourth, legal aid and psychological support services should be mandated for victims of cyberbullying, particularly women and children.[25]

CONCLUSION

Cyberbullying and online harassment have emerged as some of the most pressing socio-legal concerns of contemporary India. The unprecedented growth of digital technology, social media platforms, and online communication has undoubtedly transformed the manner in which individuals interact, express themselves, and participate in public life. However, alongside these technological advancements has emerged a darker reality marked by intimidation, humiliation, abuse, and psychological violence occurring within virtual spaces. The increasing prevalence of cyberbullying demonstrates that digital platforms, while enabling communication and connectivity, have also become instruments through which dignity, privacy, and mental well-being are frequently undermined.

The Indian legal framework addressing cyberbullying remains scattered and structurally inadequate. Although certain provisions under the Bharatiya Nyaya Sanhita, 2023 and the Information Technology Act, 2000 attempt to regulate aspects of online abuse, these provisions were never designed to comprehensively address the unique and evolving nature of cyberbullying. The absence of a precise statutory definition creates uncertainty in interpretation and enforcement, resulting in inconsistent judicial approaches and procedural inefficiencies. Victims are often compelled to rely upon fragmented remedies relating to defamation, stalking, obscenity, criminal intimidation, or identity theft, even when the harm suffered extends far beyond the scope of these traditional offences.

At the same time, the judicial response in India has reflected a conscious effort to adapt constitutional and criminal law principles to the realities of the digital era. Indian courts have repeatedly emphasized the importance of balancing freedom of speech and expression with the protection of individual dignity, reputation, privacy, and mental security. Judicial interventions have played a significant role in recognizing online harassment as a serious violation of personal liberty and constitutional rights. Nevertheless, the effectiveness of judicial remedies continues to be constrained by practical difficulties such as delayed investigations, anonymity of offenders, lack of digital forensic expertise, jurisdictional complications, and the reluctance of victims to report incidents due to fear of stigma or retaliation.

The impact of cyberbullying extends beyond legal injury; it produces profound emotional, psychological, and social consequences. Victims frequently experience anxiety, depression, social isolation, reputational harm, and in extreme cases, self-harm or suicidal tendencies. Women, children, adolescents, journalists, activists, and marginalized communities remain particularly vulnerable to targeted forms of online abuse. The permanence and rapid dissemination of digital content further aggravate the injury, as harmful material may continue circulating indefinitely despite attempts at removal. In such circumstances, cyberbullying ceases to be merely an issue of offensive speech and instead becomes a direct assault upon human dignity and personal autonomy.

India's transition towards an increasingly digital society has widened the gap between technological realities and legal safeguards. The speed with which technology evolves far exceeds the pace of legislative reform. Consequently, existing legal mechanisms often fail to provide timely and effective remedies capable of addressing the complexity of modern online abuse. This growing disconnect underscores the urgent necessity for a comprehensive and victim-centric legal framework specifically dedicated to cyberbullying and online harassment.

A robust legislative response must therefore move beyond fragmented penal provisions and adopt a holistic approach grounded in constitutional values. India requires a dedicated cyberbullying law that clearly defines prohibited conduct, establishes effective reporting and investigation mechanisms, ensures victim protection, and imposes accountability upon digital intermediaries and social media platforms. Equally important is the development of institutional infrastructure through specialized cyber cells, digital forensic training, awareness programmes, school-level sensitization initiatives, and accessible mental health support systems for victims.

Platform accountability must also form an essential component of future reform. Social media companies and digital intermediaries cannot remain passive observers while their platforms are

misused for harassment, intimidation, and dissemination of abusive content. Transparent grievance redressal mechanisms, swift content removal procedures, and stronger compliance obligations are indispensable for creating safer online environments. Simultaneously, legal reforms must continue to preserve the constitutional guarantee of free speech while ensuring that such freedom is not weaponized to justify abuse or violence in digital spaces.

Ultimately, the challenge of cyberbullying is not merely technological or legal; it is deeply connected to questions of ethics, human dignity, and democratic participation in the digital age. A society that seeks to empower its citizens through technology must also ensure their protection within technological spaces. The law must evolve in harmony with changing social and technological realities. In the context of cyberbullying and online harassment, Indian law has undoubtedly struggled to keep pace with this transformation. The urgency for comprehensive legislative intervention can no longer be ignored. The future of a safe, inclusive, and rights-based digital India depends upon the ability of its legal system to respond effectively, sensitively, and proactively to the growing menace of cyberbullying.

REFERENCES:-

[1] Internet and Mobile Association of India and KANTAR, *Internet in India Report 2023* (2023).

[2] Sameer Hinduja and Justin W. Patchin, *Bullying Beyond the Schoolyard: Preventing and Responding to Cyberbullying* (2nd edn., Corwin Press 2014).

[3] UNICEF, *Cyberbullying: What Is It and How to Stop It* (2020).

[4]Cybercrime.gov.in, National Cyber Crime Reporting Portal — Annual Statistics 2022 (Ministry of Home Affairs, Government of India, 2023) (recording over 96,000 cybercrime complaints in 2022, of which approximately 28% pertained to online harassment and cyberbullying).

[5] Shreya Singhal v. Union of India, (2015) 5 SCC 1.

[6]Information Technology Act, 2000 (Act 21 of 2000), ss. 66C, 66E, 67, 67A.

[7]Ritu Kohli Case (2005), FIR No. 567/2005, Delhi Police, Cyber Crime Cell — one of the first registered cyberstalking cases in India; discussed in Pavan Duggal, Cyber Law: The Indian Perspective (Saakshar Law Publications, 2nd edn, 2014) 211.

[8]Manish Kathuria v. State (2001), FIR registered under s. 509, Indian Penal Code, 1860 and s. 67, Information Technology Act, 2000; discussed in Farooq Ahmad, Cyber Law in India (New Era Law Publications, 3rd edn, 2011) 178.

[10]Shreya Singhal v. Union of India, AIR 2015 SC 1523, para 96 (Supreme Court of India); the Court struck down s. 66A of the Information Technology Act, 2000 as unconstitutional for being vague and overbroad.

[11]Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021, r. 4(2) (requiring significant social media intermediaries to deploy technology-based measures to identify first originator of information).

[12]Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021, r. 3(1)(b) — intermediaries are required to inform users not to upload content that is harmful, harassing, or invasive of privacy.

[13]Indian Penal Code, 1860 (Act 45 of 1860), s. 354D inserted by the Criminal Law (Amendment) Act, 2013 (Act 13 of 2013).

[15]Indian Penal Code, 1860 (Act 45 of 1860), s. 499 — defamation and s. 503 — criminal intimidation, both applicable to online communications as affirmed in Rajiv Dinesh Gadkari v. State of Maharashtra, 2018 SCC OnLine Bom 989.

[16]Protection of Children from Sexual Offences Act, 2012 (Act 32 of 2012), s. 13 (use of child for pornographic purposes) and s. 14 (punishment therefor).

[17]Balu v. State of Tamil Nadu (2019), Sessions Case No. 34/2019, Chennai — accused convicted under ss. 354D, 509 IPC and s. 66E IT Act for cyberstalking and morphing of images of victim; discussed in V.D. Kulshreshtha, Landmarks in Indian Legal History (Eastern Book Company, 2020) 489.

[18]X v. State of Maharashtra (2021), Sessions Case No. 112/2021, Mumbai — conviction under ss. 354A, 499 IPC and s. 67A IT Act for morphing and circulating obscene images of female victim on social media platforms.

[19]National Commission for Women, Annual Report 2022–23 (Government of India, 2023) 67 (noting a 36% increase in online harassment complaints against women from 2020 to 2022).

[20]Vikas Garg v. State of Haryana, 2017 SCC OnLine P&H 781 (Punjab and Haryana High Court) — the Court noted the role of social media platforms in the proliferation of cyberbullying and called for stricter enforcement of existing provisions.

[21]Law Commission of India, Report No. 267: Hate Speech (Ministry of Law and Justice, Government of India, March 2017) 41–43 (recommending insertion of ss. 153C and 505A in the IPC to address online hate speech and harassment).

[23]Digital Personal Data Protection Act, 2023 (Act 22 of 2023), s. 4 (grounds for processing personal data) and s. 9 (processing of personal data of children).

[24]Council of Europe, Convention on Cybercrime (Budapest Convention), ETS No. 185, opened for signature 23 November 2001, entered into force 1 July 2004; India has not acceded to this Convention.

[25]Ministry of Electronics and Information Technology, National Cyber Security Policy, 2013 (Government of India, 2013); see also Ministry of Home Affairs, Cyber Crime Prevention Against Women and Children (CCPWC) Scheme (Government of India, 2018).