INTERNATIONAL JOURNAL FOR LEGAL RESEARCH AND ANALYSIS

Open Access, Refereed Journal Multi Disciplinary
Peer Reviewed

www.ijlra.com

ISSN: 2582-6433

DISCLAIMER

ISSN: 2582-6433

EDITORIALTEAM

EDITORS

Dr. Samrat Datta

Dr. Samrat Datta Seedling School of Law and Governance, Jaipur National University, Jaipur. Dr. Samrat Datta is currently associated with Seedling School of Law and Governance, Jaipur National University, Jaipur. Dr. Datta has completed his graduation i.e., B.A.LL.B. from Law College Dehradun, Hemvati Nandan Bahuguna Garhwal University, Srinagar, Uttarakhand. He is an alumnus of KIIT University, Bhubaneswar where he pursued his post-graduation (LL.M.) in Criminal Law and subsequently completed his Ph.D. in Police Law and Information Technology from the Pacific Academy of Higher Education and Research University, Udaipur in 2020. His area of interest and research is Criminal and Police Law. Dr. Datta has a teaching experience of 7 years in various law schools across North India and has held administrative positions like Academic Coordinator, Centre Superintendent for Examinations, Deputy Controller of Examinations, Member of the Proctorial Board

Dr. Namita Jain

Head & Associate Professor
School of Law, JECRC University, Jaipur Ph.D. (Commercial Law) LL.M., UGC-NET Post Graduation Diploma in Taxation law and Practice, Bachelor of Commerce.

Teaching Experience: 12 years, AWARDS AND RECOGNITION of Dr. Namita Jain are - ICF Global Excellence Award 2020 in the category of educationalist by I Can Foundation, India. India Women Empowerment Award in the category of "Emerging Excellence in Academics by Prime Time & Utkrisht Bharat Foundation, New Delhi. (2020). Conferred in FL Book of Top 21 Record Holders in the category of education by Fashion Lifestyle Magazine, New Delhi. (2020).Certificate of Appreciation for organizing and managing the Professional Development Training Program on IPR in Collaboration with Trade Innovations Services, Jaipur on March 14th, 2019

ISSN: 2582-6433

Mrs.S.Kalpana

Assistant professor of Law

Mrs.S.Kalpana, presently Assistant professor of Law, VelTech Rangarajan Dr.Sagunthala R & D Institute of Science and Technology, Avadi. Formerly Assistant professor of Law,Vels University in the year 2019 to 2020, Worked as Guest Faculty, Chennai Dr.Ambedkar Law College, Pudupakkam. Published one book. Published 8Articles in various reputed Law Journals. Conducted 1Moot court competition and participated in nearly 80 National and International seminars and webinars conducted on various subjects of Law. Did ML in Criminal Law and Criminal Justice Administration.10 paper presentations in various National and International seminars. Attended more than 10 FDP programs. Ph.D. in Law pursuing.

Avinash Kumar

Avinash Kumar has completed his Ph.D. in International Investment Law from the Dept. of Law & Governance, Central University of South Bihar. His research work is on "International Investment Agreement and State's right to regulate Foreign Investment." He qualified UGC-NET and has been selected for the prestigious ICSSR Doctoral Fellowship. He is an alumnus of the Faculty of Law, University of Delhi. Formerly he has been elected as Students Union President of Law Centre-1, University of Delhi. Moreover, he completed his LL.M. from the University of Delhi (2014-16), dissertation on "Cross-border Merger & Acquisition"; LL.B. from the University of Delhi (2011-14), and B.A. (Hons.) from Maharaja Agrasen College, University of Delhi. He has also obtained P.G. Diploma in IPR from the Indian Society of International Law, New Delhi. He has qualified UGC – NET examination and has been awarded ICSSR – Doctoral Fellowship. He has published six-plus articles and presented 9 plus papers in national and international seminars/conferences. He participated in several workshops on research methodology and teaching and learning.

ISSN: 2582-6433

ABOUT US

INTERNATIONAL JOURNAL FOR LEGAL RESEARCH & ANLAYSIS ISSN- 2582-6433 is an Online Journal is Monthly, Peer Review, Academic Journal, Published online, that seeks to provide an interactive platform for the publication of Short Articles, Long Articles, Book Review, Case Comments, Research Papers, Essay in the field of Law & Multidisciplinary issue. Our aim is to upgrade the level of interaction and discourse about contemporary issues of law. We are eager to become a highly cited academic publication, through quality contributions from students, academics, professionals from the industry, the bar and the bench. INTERNATIONAL JOURNAL FOR LEGAL RESEARCH & ANALYSIS ISSN 2582-6433 welcomes contributions from all legal branches, as long as the work is original, unpublished and is in consonance with the submission guidelines.

ISSN: 2582-6433

CYBERBULLYING AND CHILD RIGHTS: A LEGAL ANALYSIS OF PROTECTION MECHANISM

"Children are the world's most valuable resource and its best hope for the future."

~ John F. Kennedy

AUTHORED BY - DR. SALONI SRIVASTAVA[1] DR. BUSHRA KHAN[2]

Abstract

In the digital age, cyberbullying has emerged as a pervasive threat to the safety and dignity of children worldwide. With the increasing access to internet-enabled devices and social media platforms, children are becoming more vulnerable to various forms of online harassment, including threats, defamation, impersonation, and the dissemination of harmful content. This research paper undertakes a comprehensive legal analysis of the protection mechanisms in place to safeguard child rights against cyberbullying.

The study examines international human rights instruments such as the United Nations Convention on the Rights of the Child (UNCRC) and how they frame the rights of children in the digital context. It further investigates regional frameworks and national legislations, with a particular focus on jurisdictions like India, the United States, and the European Union, highlighting both strengths and gaps in existing legal systems. The research also analyses the role of technology intermediaries, the responsibility of social media platforms, and law enforcement agencies in curbing cyberbullying.

Special attention is paid to the procedural challenges faced by victims in reporting and accessing justice, especially in cases involving cross-border cybercrimes. The paper also explores restorative justice approaches and non-legal interventions such as awareness campaigns and digital literacy programs aimed at prevention.

By critically analysing judicial precedents, policy initiatives, and institutional responses, this

[1] Ph.D. in Law, Legal Researcher.
[2] Ph.D. in Law, Legal Researcher.

ISSN: 2582-6433

study seeks to evaluate the efficacy of current legal mechanisms and propose reforms to enhance child protection in cyberspace. The research emphasizes a child-centric, rights-based approach and underscores the urgent need for harmonized international cooperation, robust legal frameworks, and holistic support systems to address the complex and evolving nature of cyberbullying.

Key Words; Restorative Justice, Digital Literacy, Child-Centric Approach, Rights-Based Approach, Law Enforcement, Policy Initiatives

1. Introduction

In recent years, the digital revolution has significantly altered the social, educational, and personal lives of children. While the internet offers numerous opportunities for learning, self-expression, and communication, it has also exposed children to new risks—most notably, cyberbullying. Cyberbullying refers to the use of electronic communication to harass, threaten, or humiliate a person, often anonymously and persistently. Unlike traditional forms of bullying, cyberbullying invades the private spaces of children, making them vulnerable 24/7 and often causing profound emotional and psychological harm.

Cyberbullying among children and adolescents has emerged as a pressing concern across jurisdictions. In a global survey conducted by UNICEF, one in three young people in 30 countries reported being a victim of online bullying, with nearly one in five having skipped school due to cyberbullying or violence perpetrated online.[3] The increase in smartphone usage, social media engagement, and online learning—especially in the wake of the COVID-19 pandemic—has amplified the prevalence and impact of this issue. Yet, the legal responses to this growing crisis remain fragmented and inconsistent, raising concerns about the adequacy of existing protection mechanisms for children.

This paper investigates the intersection of cyberbullying and child rights through a legal lens. It explores how international and national legal frameworks respond to cyberbullying and assesses whether they offer sufficient protection to children in the digital age. Key questions

[3] *One in Three Young People in 30 Countries Report Being a Victim of Online Bullying – UNICEF and the UN Special Representative of the Secretary-General on Violence Against Children*, UNICEF (Sept. 3, 2019), https://www.unicef.org/press-releases/one-three-young-people-30-countries-report-being-victim-online-bullying-unicef-and.

ISSN: 2582-6433

addressed in this study include: What are the current legal provisions aimed at preventing and punishing cyberbullying involving minors? How effective are these laws in practice? What role do digital platforms, parents, and law enforcement play in safeguarding child rights online?
The study relies on doctrinal legal research, drawing from international treaties, statutes, case law, and policy documents. The methodology includes comparative analysis between jurisdictions such as India, the United States, and the European Union. The paper also incorporates a review of landmark cases and judicial interpretations to assess how courts have addressed cyberbullying and upheld child rights in cyberspace.

This research is significant because it recognizes the urgency of developing a rights-based and child-centric approach to online safety. By identifying legal gaps and offering recommendations for reform, the paper aims to contribute to the ongoing global discourse on protecting children in the digital world.

2. Understanding Cyberbullying and Its Impact on Children

Cyberbullying, a digital extension of traditional bullying, represents a serious and increasingly prevalent threat to children's well-being in the online environment. It involves the intentional and repeated use of electronic communication to inflict harm, distress, or humiliation on others, particularly minors. Common platforms for cyberbullying include social networking sites, instant messaging apps, online gaming communities, and even educational platforms. The anonymity and immediacy of the internet enable perpetrators to inflict psychological harm with little fear of retribution, making cyberbullying more pervasive and invasive than conventional bullying.[4]

Cyberbullying manifests in various forms, including—but not limited to—harassment, defamation, impersonation, cyberstalking, exclusion, and the non-consensual distribution of intimate images.[5] These actions can be executed through text messages, images, videos, or social media posts. One of the most concerning aspects of cyberbullying is its persistence: the content shared online is often permanent and can be viewed, shared, or manipulated repeatedly, extending the trauma experienced by the victim.[6]

[4] Nancy E. Willard, *Cyberbullying and Cyberthreats: Responding to the Challenge of Online Social Aggression, Threats, and Distress* 6 (2007).
[5] Sameer Hinduja & Justin W. Patchin, *Bullying Beyond the Schoolyard: Preventing and Responding to Cyberbullying* 15–17 (2d ed. 2014).
[6] Sonia Livingstone & Julian Sefton-Green, *The Class: Living and Learning in the Digital Age* 119–121 (2016).

ISSN: 2582-6433

Children and adolescents are particularly susceptible to the psychological consequences of cyberbullying due to their developmental stage. Research has linked cyberbullying to a range of negative outcomes, including depression, anxiety, low self-esteem, academic decline, and in extreme cases, self-harm or suicide.[7] Unlike traditional bullying, which may be confined to school premises, cyberbullying follows the child home, often leaving them without a safe space for emotional retreat. The 24/7 nature of the internet creates a persistent threat that significantly affects children's mental health and sense of security.[8]

The effects of cyberbullying are compounded in vulnerable populations, including children with disabilities, those belonging to minority communities, and LGBTQ+ youth.[9] These groups often experience intersectional discrimination, which exacerbates the emotional toll of cyberbullying and complicates their access to justice and support. The digital divide also plays a role: children from economically disadvantaged backgrounds may lack the digital literacy or parental guidance necessary to recognize and report harmful online behaviour.[10]

Data from around the world illustrate the global scope of the problem. According to a 2021 report by the Cyberbullying Research Centre, approximately 37% of young people between the ages of 12 and 17 in the United States reported being victims of cyberbullying at some point in their lives.[11] Similar statistics are echoed in countries like India and the United Kingdom, where increased smartphone penetration and online engagement among youth correlate with rising instances of online harassment.[12]

The legal systems across jurisdictions have historically struggled to keep pace with the rapid evolution of online platforms and the unique harms posed by cyberbullying. Many legal frameworks were designed for offline crimes and do not adequately account for the

[7] Ann John et al., Self-Harm, Suicidal Behaviours, and Cyberbullying in Children and Young People: Systematic Review, *The Lancet* (June 2018), https://www.thelancet.com/journals/lanchi/article/PIIS2352-4642(18)30162-9/fulltext.
[8] Sameer Hinduja & Justin W. Patchin, *Cyberbullying Identification, Prevention, and Response* 3 (Cyberbullying Research Center, 2021), https://cyberbullying.org/Cyberbullying-Identification-Prevention-Response.pdf.
[9] *Ending Violence Against Children: Six Strategies for Action*, World Health Organization (2020), https://www.who.int/publications/i/item/9789240004192.
[10] Sonia Livingstone & Brian O'Neill, *Children's Rights and Digital Technologies*, 24 New Media & Society 29, 34–36 (2022).
[11] Sameer Hinduja & Justin W. Patchin, *Cyberbullying Fact Sheet: Identification, Prevention, and Response* (2021), https://cyberbullying.org/facts.
[12] *Cyberbullying Cases in India Rising Sharply, NCRB Data Shows*, The Times of India (Oct. 7, 2022), https://timesofindia.indiatimes.com/india/cyberbullying-cases-in-india-rising-sharply-ncrb-data-shows/articleshow/94693270.cms.

ISSN: 2582-6433

complexities of digital interactions among minors.[13] Furthermore, defining and distinguishing cyberbullying from other online offenses remains a challenge due to the subjective nature of harm and the difficulty in establishing intent, repetition, and age-specific contexts.

Thus, a nuanced understanding of cyberbullying is essential for developing effective legal and policy responses. It is not merely an issue of online misconduct but a violation of multiple fundamental rights guaranteed to children—including the right to dignity, privacy, protection from violence, and access to remedies.[14] Addressing cyberbullying requires an interdisciplinary approach that combines legal intervention, technological safeguards, educational programs, and psychological support systems tailored to children's developmental needs.

3. International Legal Framework on Child Rights and Cyberbullying

The international legal community has increasingly recognized the urgent need to protect children's rights in the digital space, particularly in response to cyberbullying. While there is no single binding international treaty specifically addressing cyberbullying, various human rights instruments and soft law documents establish legal obligations and guidance that collectively form a framework for safeguarding children from digital harm.

The cornerstone of international child rights protection is the **United Nations Convention on the Rights of the Child (UNCRC)**, adopted in 1989.[15] As the most widely ratified human rights treaty in history, the UNCRC recognizes a broad range of rights for children, including the right to protection from all forms of violence (Article 19), the right to privacy (Article 16), and the right to freedom of expression (Article 13). Although the Convention predates the digital era, its principles apply fully to online environments, including the need to protect children from harmful content and conduct such as cyberbullying.

In 2021, the Committee on the Rights of the Child issued **General Comment No. 25 on children's rights in relation to the digital environment**, which marked a significant development in the interpretation of the UNCRC. It explicitly states that cyberbullying constitutes a form of violence and calls on States to adopt measures to prevent and respond to

[13] Emma Nottingham & Sonia Livingstone, *Children's Rights in the Digital Age: An Emerging Agenda*, 5 Hum. Rts. L. Rev. 35, 41 (2019).
[14] United Nations Committee on the Rights of the Child, *General Comment No. 25 on Children's Rights in Relation to the Digital Environment*, U.N. Doc. CRC/C/GC/25 (2021).
[15] Convention on the Rights of the Child, Nov. 20, 1989, 1577 U.N.T.S. 3.

ISSN: 2582-6433

digital abuse through legal, policy, and educational initiatives. The General Comment emphasizes that children's rights to be heard, to access information, and to participate must be balanced with the need for protection from online harm.

Another relevant instrument is the **Optional Protocol to the Convention on the Rights of the Child on the Sale of Children, Child Prostitution and Child Pornography (OPSC)**.[16] Though not directly aimed at cyberbullying, this Protocol addresses the online exploitation of children and mandates State Parties to criminalize certain harmful online conduct. Increasingly, cyberbullying intersects with these forms of exploitation, particularly in cases involving the dissemination of sexually explicit material without consent—a phenomenon known as "revenge porn" or image-based abuse.

At the regional level, several instruments further reinforce international standards. The **Council of Europe's Convention on Cybercrime (Budapest Convention)** is a key international treaty that, while primarily aimed at cybercrime, provides tools that may be used to investigate and prosecute severe forms of cyberbullying. The Convention encourages international cooperation and mutual legal assistance, which are essential in addressing cross-border cyberbullying cases. The **European Convention on Human Rights (ECHR)**, though not specific to children, has been used by the European Court of Human Rights (ECtHR) to uphold children's rights in digital and educational contexts. In cases involving online harassment, the ECtHR has affirmed the State's positive obligation to protect individuals—including children—from foreseeable threats to their physical or mental well-being.

International organizations have also developed non-binding frameworks to support national responses. **UNICEF** and the **International Telecommunication Union (ITU)** have issued guidelines for industry and governments on creating a safer digital environment for children.[17] These guidelines emphasize corporate social responsibility and encourage digital service providers to implement child-friendly safety settings, content moderation, and reporting mechanisms.

Despite these developments, several challenges persist. First, international instruments often

[16] Optional Protocol to the Convention on the Rights of the Child on the Sale of Children, Child Prostitution and Child Pornography, May 25, 2000, 2171 U.N.T.S. 227.
[17] UNICEF & ITU, *Guidelines on Child Online Protection*, https://www.unicef.org/globalinsight/reports/guidelines-child-online-protection.

ISSN: 2582-6433

lack enforceability, especially where soft law documents like General Comments and guidelines are concerned. Second, there is a notable absence of a unified international legal definition of cyberbullying, which hampers the ability to prosecute offenders and collect consistent data. The varying national standards and definitions contribute to legal uncertainty and underreporting.

Moreover, enforcement is complicated by the borderless nature of the internet. Cyberbullying acts often originate in one country and affect victims in another, raising jurisdictional issues and complicating the process of holding perpetrators accountable.[18] While instruments like the Budapest Convention encourage cross-border cooperation, not all countries are signatories, limiting the global applicability of these mechanisms. To address these challenges, scholars and policymakers have advocated for a binding international treaty or protocol specifically focused on online child protection, including cyberbullying.[19] Such an instrument would clarify States' obligations, establish minimum standards for national legislation, and provide monitoring and enforcement mechanisms.

International law provides a broad framework for protecting children from cyberbullying, it remains fragmented and largely dependent on domestic implementation. The evolving digital environment demands a more cohesive, enforceable, and child-focused international legal approach that reflects the lived realities of children online.

4. Comparative Analysis of National Legal Frameworks

National legal frameworks play a pivotal role in implementing international child protection standards within domestic jurisdictions. While international instruments like the UNCRC set out broad principles, it is through national laws that practical mechanisms for protection against cyberbullying are enforced. This section analyzes the legal responses to cyberbullying affecting children in three major jurisdictions—India, the United States, and the European Union (EU)—to assess the effectiveness, strengths, and limitations of their respective legal approaches.

4.1 India

India's legal response to cyberbullying is largely shaped by two statutes: the **Information**

[18] Emma Nottingham, *Cross-Border Challenges in Child Cyberbullying Cases*, 24 Int'l J. L. & Info. Tech. 205, 211–13 (2022).
[19] John Carr, *Towards a Global Treaty on Digital Child Protection*, 40 Child. Legal Rts. J. 15, 20–22 (2021).

ISSN: 2582-6433

Technology Act, 2000 (IT Act) and the **Protection of Children from Sexual Offences Act, 2012 (POCSO Act)**. While the IT Act does not explicitly define or criminalize cyberbullying, several of its provisions can be applied to address cyberbullying-related behavior. Section 66A—now struck down by the Supreme Court in *Shreya Singhal v. Union of India*[20]—was once used to penalize offensive online messages. Presently, sections such as 66E (violation of privacy), 67 (publishing obscene material), and 72 (breach of confidentiality and privacy) may be invoked in cyberbullying cases.[21]

For children specifically, the POCSO Act criminalizes online grooming and the transmission of sexually explicit material involving minors.[3] In addition, the **Juvenile Justice (Care and Protection of Children) Act, 2015** provides for the rehabilitation of child offenders and victims, including those involved in cyberbullying incidents.[4] However, India lacks a unified legal definition of cyberbullying and a child-specific cyber safety law, leading to fragmented enforcement and underreporting.[22]

In 2021, the Ministry of Electronics and Information Technology (MeitY) issued the **Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules**, mandating social media platforms to act promptly against harmful content, including content targeting minors. While this represents progress, critics argue that enforcement remains weak due to over-reliance on self-regulation by tech companies.[23]

4.2 United States

In the United States, cyberbullying is primarily governed at the **state level**, with significant variation in the scope and language of anti-bullying laws. As of 2025, all 50 states have laws addressing bullying, and most include provisions for cyberbullying.[24] However, these laws differ in how they define the offense, prescribe school duties, and mandate reporting mechanisms.

[20] AIR 2015 SC
[21] https://pib.gov.in/PressReleasePage.aspx?PRID=1579351
[22] https://jotwani.com/cyberbullying-and-legal-remedies-in-the-indian-context-a-comprehensive-case-study-by-aditi-sharma/
[23] https://prsindia.org/billtrack/the-information-technology-intermediary-guidelines-and-digital-media-ethics- code-rules-2021
[24] National Conference of State Legislatures, *Cyberbullying and the Law* (2024), https://www.ncsl.org/research/education/cyberbullying.aspx.

ISSN: 2582-6433

At the **federal level**, there is no specific law criminalizing cyberbullying. However, several statutes are indirectly relevant. The **Children's Online Privacy Protection Act (COPPA)** protects children under 13 by regulating the collection and use of their personal data by online services.[25] The **Computer Fraud and Abuse Act (CFAA)** may also apply where cyberbullying involves hacking or unauthorized access to digital accounts. Additionally, federal civil rights laws, such as Title IX and the Civil Rights Act of 1964, have been interpreted to address discriminatory harassment, including online conduct in educational institutions.

The **Stop Bullying.gov** initiative, supported by the Department of Health and Human Services, promotes education and resources but lacks legal enforcement authority.[26] The absence of a unified federal law has led to calls for a national framework to address cyberbullying in a consistent and enforceable manner. While the U.S. emphasizes freedom of expression under the First Amendment, courts have generally upheld restrictions on online speech that crosses the line into harassment, especially when minors are involved.

4.3 European Union

The EU adopts a comprehensive and harmonized approach to digital child protection through regulations, directives, and coordinated policy efforts among member states. One of the cornerstone instruments is the **General Data Protection Regulation (GDPR)**, which offers robust privacy protections for children. Article 8 of the GDPR requires parental consent for processing personal data of children under 16, ensuring a level of control over children's digital footprints.[27]

The **Audiovisual Media Services Directive (AVMSD)** and the **Digital Services Act (DSA)** also contribute significantly to online safety. The DSA, adopted in 2022, places clear obligations on digital platforms to remove harmful and illegal content, conduct risk assessments, and prioritize child safety.[28] It also mandates transparency in content moderation algorithms and provides children with accessible mechanisms to report harmful content.

[25] Children's Online Privacy Protection Act, 15 U.S.C. 6501–6506 (1998).
[26] StopBullying.gov, *What Is Cyberbullying?*, https://www.stopbullying.gov/cyberbullying/what-is-it (last visited Apr. 17, 2025).
[27] Regulation 2016/679, of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data (General Data Protection Regulation), 2016 O.J. (L 119) 1.
[28] Regulation 2022/2065, of the European Parliament and of the Council of 19 October 2022 on a Single Market for Digital Services (Digital Services Act), 2022 O.J. (L 277) 1.

ISSN: 2582-6433

In addition, the **EU Strategy for a More Effective Fight Against Child Sexual Abuse (2020–2025)** addresses both prevention and law enforcement strategies in the digital realm.[29] The **Safer Internet Programme** and **Better Internet for Kids** initiative further support education, reporting mechanisms, and public awareness campaigns.[30]

Unlike India and the U.S., the EU's approach to cyberbullying is deeply rooted in children's rights frameworks and data protection principles. However, despite strong institutional support, member states vary in the implementation of cyberbullying-specific laws. For example, while countries like Germany and France have passed national legislation explicitly addressing cyberbullying, others have yet to incorporate similar provisions.

4.4 Comparative Evaluation

Each jurisdiction offers unique strengths and faces distinct challenges. India has made strides in integrating digital safety within broader child protection laws, but lacks a targeted cyberbullying statute and enforcement remains inconsistent. The United States benefits from state-level flexibility but suffers from fragmentation and the absence of a cohesive federal law. The European Union, through centralized policymaking and regulatory enforcement, presents a model of harmonization but still grapples with uneven application among member states.

A key takeaway from this comparative analysis is the need for a **rights-based and child-centric approach** that not only criminalizes harmful behavior but also ensures preventive, educational, and restorative strategies. Jurisdictions must also improve cooperation with digital service providers, enhance cross-border legal assistance, and strengthen child-friendly reporting and support mechanisms.

5. Challenges in Legal Enforcement

Despite the proliferation of laws aimed at combating cyberbullying, especially those concerning children, their enforcement remains a formidable challenge in India. The gap between legislative intent and on-ground implementation underscores several systemic, procedural, and infrastructural hurdles. This section critically explores the key challenges that hamper effective legal enforcement in protecting children from cyberbullying.

[29] European Commission, *EU Strategy for a More Effective Fight Against Child Sexual Abuse* (2020), https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/12475.
[30] European Commission, *Better Internet for Kids Programme*, https://digital-strategy.ec.europa.eu/en/policies/better-internet-kids.

ISSN: 2582-6433

5.1 Ambiguity and Fragmentation in Legal Provisions

One of the most significant issues is the **lack of a clear, unified legal definition** of cyberbullying in Indian law. The term "cyberbullying" does not appear explicitly in the Information Technology Act, 2000, or in the Indian Penal Code, 1860. Instead, various provisions are applied piecemeal to incidents involving online abuse, such as Sections 66C, 66E, and 67 of the IT Act and Sections 354A, 354D, and 507 of the IPC.[31] This fragmented approach leads to **confusion among law enforcement** officers and inconsistent application in courts. Moreover, laws such as the **Protection of Children from Sexual Offences Act, 2012 (POCSO)** are more focused on sexual offences rather than broader forms of online harassment, leaving out many non-sexual yet harmful behaviours like social exclusion, body shaming, or trolling.[32]

5.2 Underreporting and Fear of Stigma

Another major barrier is **underreporting of cyberbullying incidents**, particularly among children. Victims often refrain from reporting due to fear of social stigma, victim-blaming, or punitive repercussions from parents and teachers.[33] According to a study by the National Crime Records Bureau (NCRB), cybercrime complaints by minors remain disproportionately low despite growing access to digital devices.[34]

The lack of confidential, child-sensitive reporting mechanisms also discourages children from seeking help. Most reporting systems—such as filing an FIR at a police station—are not designed to be child-friendly, which further **marginalizes victims** and allows perpetrators to go unpunished.

5.3 Inadequate Training of Law Enforcement

Many police personnel and judicial officers lack **specialized training** in dealing with cyber offences, particularly those involving minors. While cybercrime cells exist in major cities, rural areas and smaller towns often do not have adequately trained officers or technical infrastructure to investigate digital offences.

[31] Information Technology Act, 2000, Section 66C, 66E, 67, No. 21, Acts of Parliament, 2000 ; Indian Penal Code, 1860, Section 354A, 354D, 507.
[32] Protection of Children from Sexual Offences Act, 2012, No. 32, Acts of Parliament, 2012 (India).
[33] UNICEF India, *Online Safety of Children and Young People in India: A Guide for Educators and Caregivers* (2021), https://www.unicef.org/india/reports/online-safety-guide.
[34] National Crime Records Bureau, *Crime in India – 2022*, https://ncrb.gov.in.

ISSN: 2582-6433

Even where training modules exist—for instance, those developed by the National Cyber Crime Reporting Portal (cybercrime.gov.in) or the Bureau of Police Research and Development—they remain **underutilized or outdated**. Furthermore, officers frequently struggle to collect and preserve digital evidence in a forensically sound manner, weakening the prosecutorial process.[35]

5.4 Jurisdictional and Procedural Complexities

Cyberbullying often transcends geographical boundaries, posing challenges of **jurisdiction and cooperation**. A child in India may be bullied by someone outside the country, or through a platform hosted abroad. This makes evidence collection difficult and delays legal processes, especially in the absence of effective **mutual legal assistance treaties (MLATs)** or cooperation with foreign service providers.

Moreover, procedural bottlenecks in invoking relevant sections of the IT Act or IPC often delay investigations. Cases registered under inappropriate sections, or those lacking adequate evidence, frequently result in acquittals or dismissal.[36]

5.5 Limited Accountability of Intermediaries

Digital platforms—especially social media sites—are frequently used as mediums for cyberbullying. While the **IT (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021** impose obligations on intermediaries to remove harmful content within 24 hours of receiving complaints, enforcement remains patchy.[37]

A 2022 study by SFLC.in (Software Freedom Law Centre, India) revealed that most intermediaries failed to meet basic transparency and grievance redressal requirements outlined in the IT Rules. Moreover, **victims often find it difficult to navigate content takedown procedures**, especially when platforms fail to respond promptly or offer opaque complaint systems.

The rules also give intermediaries considerable discretion in determining whether content

[35] Indian Police Foundation, *Cybercrime in India: Capabilities and Challenges* (2022), https://www.policefoundationindia.org.
[36] SFLC.in, *Online Harassment: A Study on Platform Accountability* (2022), https://sflc.in/report-online-harassment.
[37] Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021, G.S.R. 139(E), Mar. 2021.

ISSN: 2582-6433

violates their terms, which may not always align with Indian laws or child rights norms.

5.6 Data Protection and Children's Privacy

India still lacks a **comprehensive data protection law**, although the **Digital Personal Data Protection Act, 2023 (DPDP Act)** marks progress. While the Act recognizes children as a vulnerable group and mandates verifiable parental consent for processing data of minors, its implementation is in early stages.[38]

Concerns remain about the **enforcement capacity of the Data Protection Board** and the technical preparedness of platforms to comply with child-centric data privacy requirements. Additionally, ambiguities about the age of digital consent (set at 18 under the DPDP Act) could hinder access to beneficial services and platforms for adolescents, without necessarily improving their safety.[39]

5.7 Absence of Child-Centric Infrastructure

Indian law enforcement and judicial systems are still evolving towards **child-sensitive procedures** in digital abuse cases. Although the **Juvenile Justice (Care and Protection of Children) Act, 2015** mandates child-friendly courts and processes, these are rarely applied in cyberbullying cases.[40] Most interactions with the justice system remain intimidating for children and may result in secondary trauma.

Moreover, rehabilitation mechanisms for victims and reformative programs for child offenders are either non-existent or grossly underfunded. NGOs such as **Aarambh India** and **Childline India Foundation** have stepped in to fill this gap but cannot substitute for state-backed, systemic measures.[41]

5.8 Cultural and Societal Barriers

Cyberbullying is often normalized or dismissed as "harmless fun" by both adults and peers, which leads to **minimization of the harm** it causes. Cultural stigmas around mental health,

[38] Digital Personal Data Protection Act, 2023, No. 22, Acts of Parliament, 2023.
[39] Internet Freedom Foundation, *Preliminary Analysis of the DPDP Act*, https://internetfreedom.in/dpdp-analysis (Aug. 2023).
[40] Juvenile Justice (Care and Protection of Children) Act, 2015, No. 2, Acts of Parliament, 2016 (India).
[41] Aarambh India, *Cyber Safety & Children*, https://aarambhindia.org; Childline India Foundation, https://www.childlineindia.org.

ISSN: 2582-6433

sexuality, and gender further silence victims—particularly girls, LGBTQ+ youth, and children from marginalized communities.

There is also a generational gap in how digital threats are perceived. Many parents and teachers are unaware of the platforms children use or the nuanced ways in which bullying manifests online. This **lack of awareness results in inadequate responses** to children's complaints, perpetuating a culture of silence.

India's legal framework has laid an important foundation for addressing cyberbullying against children, but enforcement gaps remain stark. Bridging these gaps requires institutional capacity-building, inter-agency cooperation, digital literacy, and a fundamental shift towards child-centric justice. Strengthening the accountability of intermediaries and fostering inclusive, safe digital environments must be prioritized. Above all, listening to and empowering children as rights-holders remains central to any meaningful enforcement strategy.

6. Recommendations and Way Forward

Tackling cyberbullying against children in India requires more than a legal response; it necessitates a robust, multi-dimensional strategy that involves legal reform, institutional strengthening, public awareness, digital literacy, and cross-sector collaboration. The recommendations below are structured to address the gaps identified in previous sections, and are grounded in a rights-based and child-centric approach.

6.1 Enactment of a Comprehensive Anti-Cyberbullying Law

One of the most urgent reforms needed is the **enactment of a dedicated anti-cyberbullying law**, which clearly defines cyberbullying and incorporates provisions specific to children. This would help reduce ambiguity in enforcement and ensure consistent judicial interpretation.

The law should cover a wide spectrum of online harms including doxing, impersonation, non-consensual sharing of private information, and psychological harassment. It should also mandate **child-friendly reporting mechanisms**, fast-track adjudication, and offer clear guidelines for platform accountability.[42] The **National Commission for Protection of Child Rights (NCPCR)** has previously recommended tailored laws to combat digital abuse of

[42] National Commission for Protection of Child Rights (NCPCR), *Report on Effects of Online Gaming and Cyberbullying on Children* (2022), https://ncpcr.gov.in.

ISSN: 2582-6433

children, indicating institutional support for such reform.[43]

6.2 Strengthening Enforcement Infrastructure and Capacity Building

Even where laws exist, enforcement suffers due to the lack of trained personnel and technical infrastructure. There is an urgent need to:

- Expand and equip **cybercrime cells** in every district with child protection officers;
- Include **mandatory modules on child cyber safety** in police and judicial academies;
- Provide regular training and workshops for prosecutors, school administrators, and child protection units.

The Bureau of Police Research and Development and the Ministry of Home Affairs should collaborate with experts to design **updated training modules** focused on digital evidence collection, child interviewing techniques, and restorative justice approaches.[44]

6.3 Enhancing Child-Friendly Reporting Mechanisms

Most children find the current system of reporting cybercrimes inaccessible or intimidating. Child-specific helplines, digital platforms, and in-school counselling systems should be promoted as **first lines of reporting**. The **Childline 1098 service** should be integrated with online portals like **cybercrime.gov.in**, allowing children to file reports anonymously or with minimal adult intervention.[45]

Further, **ombudspersons or nodal officers for child cyber safety** should be appointed at state and district levels to oversee complaints and ensure time-bound redressal.

6.4 School-Based Interventions and Digital Literacy

Schools should be placed at the **heart of cyberbullying prevention efforts**. The Ministry of Education, in collaboration with NCPCR and NGOs, should mandate the inclusion of digital citizenship and cyber safety education in the **National Curriculum Framework (NCF)**.

Key recommendations include:

- Introduction of **age-appropriate cyber safety modules** from primary to secondary levels;
- Designation of a **"Cyber Safety Mentor"** in every school;

[43] National Commission for Protection of Child Rights (NCPCR), *Report on Effects of Online Gaming and Cyberbullying on Children* (2022), https://ncpcr.gov.in.
[44] Bureau of Police Research and Development, *Cyber Crime Investigation Manual* (2021), https://bprd.nic.in.
[45] CHILDLINE India Foundation, *Childline 1098*, https://www.childlineindia.org.

ISSN: 2582-6433

- Hosting annual workshops for students, teachers, and parents;
- Incorporating cyber-ethics into teacher training curricula.

Research by the **UNESCO Mahatma Gandhi Institute of Education for Peace and Sustainable Development (MGIEP)** indicates that social-emotional learning combined with digital literacy is effective in reducing online aggression among adolescents.[46]

6.5 Regulation and Accountability of Digital Platforms

Under the **IT Rules, 2021**, intermediaries are required to remove harmful content within 24 hours upon receiving complaints. However, enforcement remains weak, especially regarding children's online safety. The government should:

- Mandate **periodic transparency reports** from intermediaries, especially regarding child-targeted abuse;
- Impose **graded penalties** for non-compliance with takedown and moderation standards;
- Promote **age-appropriate design standards** (such as limiting algorithmic targeting and enabling easy reporting features for minors).

Intermediaries must be required to **design their platforms with child safety by default and design**, as suggested by both the **UNICEF Guidelines on Child Online Protection** and India's **MeitY consultations on child safety online**.[47]

6.6 Public Awareness and Community Engagement

Public perception of cyberbullying as a minor issue or "normal teenage behaviour" must be countered through **mass awareness campaigns**. Government agencies, civil society, and media must collaborate to raise awareness among parents, educators, and children about the seriousness of cyberbullying.

Suggested initiatives include:

- Launching **nationwide campaigns** akin to "Beti Bachao Beti Padhao," specifically focused on digital safety;
- Local-language awareness materials to ensure regional accessibility;

[46] UNESCO MGIEP, *Building Resilience through SEL and Digital Literacy*, https://mgiep.unesco.org.
[47] Ministry of Electronics and Information Technology (MeitY), *Guidelines for Children's Online Safety* (2021), https://www.meity.gov.in.

ISSN: 2582-6433

- Community-based events involving children in co-creating anti-bullying pledges, online safety charters, and peer-to-peer awareness.

Civil society organizations like **Aarambh India**, **Cyber Peace Foundation**, and **Save the Children India** have successfully piloted such initiatives and could be scaled in partnership with state agencies.[48]

6.7 Strengthening Data Protection and Privacy Safeguards

The **Digital Personal Data Protection Act, 2023** must be enforced effectively, with **additional safeguards for children's data**. This includes:

- Establishing **parental controls** that are transparent and easy to use;
- Enforcing **data minimization and purpose limitation** for platforms targeting children;
- Conducting **periodic audits of digital service providers** handling children's data.

Further, **children above 13 years** should have **graduated digital consent rights**, as recommended by the **Internet Freedom Foundation**, which balances autonomy and protection.[49]

6.8 Multistakeholder Governance and Child Participation

Finally, the way forward must be anchored in **collaborative governance models**, involving all stakeholders—government, tech companies, civil society, educators, and, most importantly, **children themselves**.

- Children should be included in **advisory councils** on cyber safety policies;
- Platforms must establish **youth advisory boards** to understand the evolving nature of online interaction;
- Civil society must be empowered to monitor, report, and audit child digital rights violations.

Empowering children as **digital citizens**, not just passive users, ensures that they are both protected and heard. Cyberbullying is a deeply entrenched, multifaceted challenge, but it is not insurmountable. A child-rights-based, participatory, and coordinated response—backed by strong laws, effective enforcement, public engagement, and platform accountability—can make Indian cyberspace safer for its youngest users.

[48] Aarambh India, https://aarambhindia.org; Cyber Peace Foundation, https://www.cyberpeace.org; Save the Children India, https://www.savethechildren.in.
[49] Internet Freedom Foundation, *Analysis of DPDP Act 2023 and Its Impact on Children's Rights* (Aug. 2023), https://internetfreedom.in.

ISSN: 2582-6433

7. Conclusion

Cyberbullying has emerged as one of the most insidious threats to child rights in the digital era. The unprecedented penetration of the internet and mobile devices among children in India has offered them immense opportunities—but it has also exposed them to new forms of abuse, humiliation, and trauma, often in spaces where guardianship is weak or absent. Despite having a framework of laws and policies that touch upon digital safety, India is yet to develop a **cohesive, child-centric legal approach** to cyberbullying.

This research paper has demonstrated that while various provisions under the **Information Technology Act, 2000**, the **Indian Penal Code, 1860**, the **POCSO Act, 2012**, and other statutes provide some degree of protection, their application to cyberbullying remains **fragmented and inadequate**. The absence of an explicit legal definition of cyberbullying, the procedural complexity of enforcement, jurisdictional hurdles, and the lack of accountability of digital intermediaries severely undermine the child's right to protection from harm under **Article 21** of the Indian Constitution.

Moreover, enforcement challenges are exacerbated by systemic barriers such as **lack of training among law enforcement**, underreporting due to social stigma, and the failure to design **child-friendly complaint and redressal systems**. The findings also underscore the crucial role of **schools, families, and communities** in prevention, as much of the psychological harm caused by cyberbullying is compounded by inadequate support systems.

Equally important is the need to **empower children as digital citizens**, capable of not just using technology but shaping it ethically and safely. Children's voices must be included in policy-making, curriculum design, and platform governance to ensure the solutions are grounded in their lived experiences. **Digital safety should not be reactive but preventive, restorative, and holistic**.

In conclusion, cyberbullying is not just a legal issue—it is a **developmental, psychological, and social crisis**. Addressing it effectively will require **not only laws and policies but also empathy, education, and empowerment**. India must seize this moment to evolve its child protection mechanisms to be fit for the digital age—ensuring that every child grows up free, safe, and respected, both offline and online.