



CYBERBULLYING IN THE DIGITAL AGE: LEGAL CHALLENGES AND SOLUTIONS

DR. SURENDER SINGH DAHIYA

Professor, Faculty of Law, M.D.U., Rohtak (Har.)

KIRTI VERMA

Research Scholar, Faculty of Law, M.D.U., Rohtak (Har.)

ABSTRACT

The digital age has seen a rise in cyberbullying, a form of online harassment that has serious negative effects on the mental health of victims. Its characteristics, such as anonymity and wide scope, make it difficult to combat. The same faces enforcement challenges due to a lack of specific definitions, and jurisdictional conflicts persist. Comprehensive legislation, harmonised international standards, increased law enforcement cooperation, and legal assistance to victims play an imperative role in addressing it. This paper highlights the crucial role of digital literacy in curbing this global issue and further outlines the laws adopted by different jurisdictions to guide efforts to eliminate it. Furthermore, it discusses the active steps taken by the Indian judiciary and the legislature's concern about eliminating this issue.

KEYWORD: Cyberbullying, Digital Literacy, Mental Health, Australian Law

INTRODUCTION

Rapid globalisation accelerates digitalisation worldwide, introducing a new aspect of citizenship: cyber citizenship. Today, people across jurisdictions can connect and interact in the cyber world without barriers. This brings advantages that help individuals to express their thoughts and opinions, but it also brings a new set of responsibilities and challenges. Cybercrimes are also evolving as digitisation advances. They introduce new forms of cybercrime that many people are unfamiliar with, making them easy targets. People are expected to comprehend, navigate, and use technology efficiently in many aspects of their lives. It is a cinch to disseminate misinformation on social media and cyberbully someone. Technology can spread unverified information, whether intentionally or unintentionally. Consequently, it has broad societal repercussions. The American Psychological Association defined bullying as *"A form of aggressive behaviour in which someone intentionally and repeatedly causes another person injury or discomfort. It can take the form of physical contact, words, or more subtle actions"*.¹

DIGITAL LITERACY AND CYBERBULLYING

UNESCO: literacy pertains to the foundational ability to understand, identify, create, interpret, compute, communicate, and to use the printed and written materials that are associated with

¹ American Psychological Association, "Bullying," APA, available at: <https://www.apa.org/topics/bullying> (last visited on January 17, 2026).



International Journal of Engineering, Science and Humanities

An international peer reviewed, refereed, open access journal

Impact Factor: 8.3 www.ijesh.com **ISSN: 2250 3552**

varying contexts. Literacy is the set of skills and abilities a person possesses to express ideas and thoughts, encompassing effective communication. Digital literacy is the set of skills, abilities, and knowledge needed to use various digital media platforms, such as computers, the internet, and cellular phones. It requires a critical approach to understanding digital media content and its various applications. It also includes the capacity and knowledge to create media content using digital technologies. Digital literacy instils the capabilities needed to address the challenges of the technological era. Digital literacy includes:

1. Media literacy,
2. Media and communication, and technological literacy. The impact of digital literacy includes quick, smooth transactions that help content reach people worldwide and become more popular and well-known.
3. It can be accessed unlimitedly through hyperlinks.
4. To halt the contentious content, one can take appropriate steps to stop its dissemination.
5. Empowering people to detect the signs of cyberbullying, whether in the position of the victim or bystanders.

When an individual bullies others on digital platforms, it is termed cyberbullying. This act is likely to harm the targeted individual. Presently, there is no widely accepted definition of cyberbullying, but various researchers have attempted to define it. Cyberbullying, as defined by Bill Belsey, President of Bullying.org, states, ² *"Cyberbullying involves the use of information and communication technologies such as e-mail, cell phone, and pager text messages, instant messaging, defamatory personal websites, and defamatory online personal polling websites to support deliberate, repeated, and hostile behaviour by an individual or group that is intended to harm others"*.

Various forms of cyberbullying can be stated as:

Harassment: When a bully sends threatening or abusive messages.

Impersonation fraud: Creating a fake profile in someone else's name or hacking into someone else's account.

Flaming: Involves the repeated exchange of obscene, vulgar, or angry electronic messages.

Denigration: Spreading rumours about a person to defame them

Outing: Sharing a person's secrets or personal information without their permission

Cyberstalking: Sending malicious messages or engaging in other online activities that raise security concerns. ³

Deepfake videos - Created by artificial intelligence that combines images to create new events that never happened. These components of cyberbullying have the identical essence to bullying;

² Bill Belsey, "Cyberbullying," Bill Belsey, available at: <https://billbelsey.com/?cat=12> (last visited on September 17, 2026).

³ Rakesh Chandra, "Cyberbullying and Indian Legal Regime: An Overview," Creative Connect International Publisher Group (2018).



the only extra aspect of cyberbullying is using technology to perpetrate cyberbullying. Other comparable developments in cyberbullying and bullying are the aggressive conduct of the cyberbully and the aim. The aim suggests malice and pre-organised plans to purposefully damage the person-centred approach to cyberbullying, though this isn't identical in each cyberbullying case; in a few instances, the perpetrators say or act in a certain way with an understanding of the likely damage to the sufferer. Cyberbullying is much riskier than conventional bullying because it "intensifies the sufferer's feelings", as the sufferer of cyberbullying has a sense that his/her records are published on the web platform and he/she no longer has any means to get the details of the publisher or control the circulation of data. According to Rusdy and Fauzi, a lack of proper understanding of digital literacy can negatively affect children and adults⁴. This is due to inadequate education on responding to online behaviours and ethical obligations. Individuals may be likely to develop harmful behaviours. Lack of digital literacy also results in exclusion from meaningful participation in society, as these individuals can only engage partially in areas such as finance, work, and informed decision-making. Further, poor digital literacy makes individuals susceptible to harmful content. This can lead to the spread of hurtful or false information without fully understanding the consequences of their actions.

CYBERBULLYING DURING THE COVID-19 ERA

During the COVID-19 pandemic, quarantine and social distancing disrupted daily life, making online activities the main way people communicated and interacted. Many turned to the Internet and social media to stay connected, while others used online gaming and streaming for entertainment. As a result, platforms like dating sites, gaming services, and online medical services saw more users. As people spent more time online, cases of cyber victimisation also increased. This includes people facing violence, harassment, trolling, stalking, intimidation, and other forms of cybercrime.

Research shows that cyber attackers often target individuals with physical or intellectual disabilities and chronic illnesses, leading to depression, anxiety, worry, physical health problems, and self-harm.⁵ Cyberbullying has become more common during the pandemic. Before the pandemic, its prevalence ranged from 6% to 35%, but those numbers have increased⁶. Students who use Instagram, play online games, spend more time gaming, or share their opinions online are at higher risk of being cyberbullied⁷. In some cases, cyber victimisation has led to death through live streaming, a phenomenon known as cyber suicide.

⁴ Marhamah Rusdy and Fauzi, "Digital Literacy and Cyberbullying Behavior of Youths in Instagram" 12 *KOMUNIKE: Jurnal Komunikasi Penyiaran Islam* 122-145 (2020).

⁵ Z.A. Alhaboby, J. Barnes, H. Evans and E. Short, "Cyber-Victimization of People with Chronic Conditions and Disabilities: A Systematic Review of Scope and Impact" 20 *Trauma, Violence, & Abuse* 398-415 (2019).

⁶ S. Shoib, S. Philip, S. Bista, F. Saeed, S. Javed, D. Ori, A. Bashir and M. Chandradasa, "Cyber Victimization during the COVID-19 Pandemic: A Syndemic Looming Large" 5 *Health Science Reports* e528 (2022).

⁷ S.M. Bottino, C.M. Bottino, C.G. Regina, A.V. Correia and W.S. Ribeiro, "Cyberbullying and Adolescent Mental Health: Systematic Review" 31 *Cad. Saude Publica* 463-475 (2015).



PREVALENCE OF CYBERBULLYING

Comprehensive national data on cyberbullying prevalence in India remain limited; however, existing studies indicate significant variation among adolescents. One study involving 228 adolescents aged 11 to 15 years reported a 17.2% prevalence of cyberbullying victimisation⁸. A separate survey in Delhi among 174 secondary school students found that 8% had engaged in cyberbullying, while 17% reported being victims⁹. Additionally, a study of 1,721 students from higher education institutions in India found that 30% had experienced cyberbullying. These findings indicate that cyberbullying is a substantial concern among Indian adolescents, though prevalence rates differ by location and sample characteristics. According to the National Crime Records Bureau (NCRB), India reported 50,035 cybercrime cases in 2020¹⁰. This trend underscores the urgent need for effective interventions to address online harassment, identity theft, and abuse. With approximately 760 million internet users, India is experiencing a rise in cyberbullying incidents. A 2020 study by the India Child Protection Foundation (ICPF) reported that 1 out of 4 children in India is a victim, with girls and LGBTQ+ youth disproportionately affected. Approximately 71 million children aged 5 to 11 access the internet on family members' devices, representing about 14% of the country's active internet users, which exceeds 760 million¹¹. In India, nearly two out of every three internet users are between 12 and 29 years old, according to the Internet & Mobile Association of India. With the surge in online activity after the lockdown, children and young people now face a greater threat of cyberbullying and online discrimination.

JUDICIAL APPROACH TO CYBERBULLYING IN INDIA

This century marks the beginning of the digital era and revolution. The Indian government has taken significant steps to digitise services, making the online world an integral part of daily life. As a result, new legislation has emerged to address cybercrimes such as cyber-harassment, stalking, defamation, and bullying. The primary law governing cybercrimes in India is the Information Technology Act, 2000 (IT Act). In 2009, Section 66A was introduced to criminalise sending offensive messages through communication devices. However, the Apex Court struck down this provision in *Shreya case*¹² due to its vague language and potential for misuse.

⁸ P.J. Ranjith, M.N. Vranda and M.T. Kishore, "Predictors, Prevalence, and Patterns of Cyberbullying among School-Going Children and Adolescents" 65 *Indian Journal of Psychiatry* 720-728 (2023).

⁹ D. Sharma, J. Kishore, N. Sharma and M. Duggal, "Aggression in Schools: Cyberbullying and Gender Issues" 29 *Asian Journal of Psychiatry* 142-145 (2017).

¹⁰ V.M., G. Balamurugan, S. Sevak, K. Gurung, B.G., S.X., T.P. and T.S., "Silent Screams: A Narrative Review of Cyberbullying Among Indian Adolescents" 16 *Cureus* e66292 (2024).

¹¹ Akshat Khetan, "Cyber-Bullying: How Should India Legally Equip Itself?" *LiveLaw*, Nov. 15, 2024, available at: <https://www.livelaw.in/law-firms/law-firm-articles/-cyber-bullying-digital-harassment-indian-child-protection-fund-national-crime-records-bureau-cybercrime-cyber-attacks-social-stigma-abuse-pocso-it-act-275322> (last visited on May 17, 2026).

¹² *Shreya Singhal v. Union of India*, (2015) 5 SCC 1.



International Journal of Engineering, Science and Humanities

An international peer reviewed, refereed, open access journal

Impact Factor: 8.3 www.ijesh.com ISSN: 2250 3552

In the Supreme Court case *K.A. Abbas v. Union of India & Another*¹³ the court noted that when a law seems unclear, judges should interpret it as much as possible within the limits of its language. This interpretation should follow the intention of the lawmakers, choosing the meaning that best supports the law's purpose. In 2012, P. Pajeeve, a member of parliament representing a constituency in Kerala, introduced a resolution to amend the same section. He argued that the boundaries of the provision should prioritise the safety of women and be clearly defined, rather than eliminating the provision entirely. He further suggested replacing the terms 'grossly' and 'demeaning' with 'menacing' and including 'sexually' in the language of the provision.

R v Juggernaut Books Pvt Ltd holds considerable significance for cyberbullying and defamation in India's legal framework. It illustrates the complexities involved in regulating online content and the resulting implications for freedom of expression and individual rights. The court acknowledged the potential harm to Ramdev's reputation and stressed the need to verify facts before publication. This ruling highlighted the need to balance free speech with safeguarding individual reputations in a digital era characterised by rapid information dissemination. Subsequent hearings further examined the legal intricacies of defamation, freedom of expression, and the responsibilities of publishers concerning the content they distribute. The court reaffirmed that, although freedom of speech is a fundamental right, it does not encompass false statements that may damage an individual's reputation.

*Rini Johar v. State of MP*¹⁴ In this case, the Madhya Pradesh High Court ordered the cyberbully to pay compensation to the victim of online harassment and character assassination. The court highlighted the importance of protecting people from online abuse and defamation.

In *Nikita Singh v. State of MP*, the Madhya Pradesh High Court upheld the conviction of an individual who created a false Facebook profile in the victim's name and uploaded defamatory content. The court recognised the gravity of internet abuse and defamation.

In *Rajat Prasad v. CBI*, the Apex Court of India addressed the legality of sting operations. The court found the journalist guilty of abetment to bribery, emphasising that conducting a sting without public interest can constitute a crime. This case highlighted the legal complexities surrounding media practices and cyberbullying, as it set a precedent for accountability in journalistic conduct while navigating issues of online harassment and defamation.

In a recent landmark case¹⁵ the Apex Court held that any act of viewing, distributing, or displaying child pornography on the Internet, even without physical possession or storage of the material, may constitute "possession" under Section 15 of the POCSO Act if the individual exercises an unaltered degree of control over the material, as defined by the doctrine of constructive possession. The judgment clarifies that constructive possession extends beyond physical control to situations

¹³ *K.A. Abbas v. Union of India & Anr.*, (1970) 2 SCC 780.

¹⁴ *Dr. Rini Johar & Anr. v. State of M.P. & Ors.*, (2016) 11 SCC 703.

¹⁵ *Just Rights for Children Alliance & Anr. v. S. Harish & Ors.*, 2024 INSC 716.



where an individual has both the right and intention to control the contraband, even without direct physical possession.

PREVENTIVE MEASURES TAKEN BY DIFFERENT JURISDICTIONS

An Australian Parliament recently enacted a landmark law¹⁶ aimed at protecting the mental health and well-being of young people from the risks associated with excessive online activity. Prime Minister Anthony Albanese stated that the law addresses parental concerns regarding online harms to children. He emphasised that “Platforms now have a social responsibility to ensure that the safety of our children is their top priority.”

Key Provisions of the Australian Social Media Law:

Age Verification: Social media platforms are required to prevent users under the age of 16 from accessing their services.

Tough Penalties: Businesses that fail to comply with age verification requirements may face substantial fines of up to \$49.5 million¹⁷.

Exceptions: Messaging applications, online gaming platforms, and educational services are exempt from these restrictions.

In the United States, the Children’s Online Privacy Protection Act (COPPA), enacted in 1998, mandates parental consent for websites collecting personal information from children under 13. In response, many companies have blocked access for this age group, resulting in widespread age misrepresentation. The Children’s Internet Protection Act (CIPA) of 2000 restricts access to inappropriate content in schools and libraries. However, critics argue that CIPA is a limited solution, as children can still access unrestricted online content outside these environments, and the law may inadvertently block access to valuable information.¹⁸

In the European Union (EU), To handle the personal data of anyone under 16, parental consent is a must. Still, some member states can choose to set this age as low as 13.¹⁹ In Germany, minors aged 13 to 16 may use social media only with parental consent. There are currently no plans to introduce additional restrictions. Child protection advocates contend that existing controls are inadequate and advocate for stronger enforcement of current regulations. Belgium sets the bar at 13, letting kids create social media accounts on their own once they reach that age. In Italy, the threshold is a bit higher: parental consent is needed until 14, after which teens can sign up freely.

¹⁶ Prime Minister of Australia, “Social Media Reforms to Protect Our Kids Online Pass Parliament,” Nov. 29, 2024, available at: <https://www.pm.gov.au/media/social-media-reforms-protect-our-kids-online-pass-parliament> (last visited on September 17, 2026)

¹⁷ Parliament of Australia, Parliamentary Library, “Online Safety Amendment (Social Media Minimum Age) Bill 2024,” available at: https://www.aph.gov.au/Parliamentary_Business/Bills_Legislation/bd/bd2425/25bd39 (last visited on September 17, 2026).

¹⁸ Wikipedia, “Children’s Online Privacy Protection Act,” Wikipedia, available at: https://en.m.wikipedia.org/wiki/Children%27s_Online_Privacy_Protection_Act (last visited on September 17, 2026).

¹⁹ Tech.co, “Countries with Age Restrictions on Social Media,” Tech.co, available at: <https://tech.co/news/countries-age-restrictions-social-media> (last visited on September 17, 2026).



International Journal of Engineering, Science and Humanities

An international peer reviewed, refereed, open access journal

Impact Factor: 8.3 www.ijesh.com **ISSN: 2250 3552**

In China, the cyberspace regulator ruled in the previous year that children under 18 should not use smartphones for more than two hours per day. The Cyberspace Administration of China (CAC) has called for smart device vendors to implement a minors program that would block users under 18 from going online on their mobile devices during the late-night hours, from 10 p.m. to 6 a.m.

LEGAL FRAMEWORK IN INDIA

Currently, there are no explicit legal restrictions dedicated to protecting children from online harm in India. The Information Technology (Intermediary Guidelines and Digital Media Ethics Rules, 2021)²⁰ prohibits streaming platforms from broadcasting illegal content and mandates the categorisation of content by age group, as well as the implementation of age-control mechanisms to restrict children's access to inappropriate material. However, further measures are necessary to strengthen social media and over-the-top (OTT) platforms to effectively curb the dissemination of vulgar content. Ashwini Vaishnaw, Union Minister of Railways, Information and Broadcasting, recently emphasised the need for the parliamentary standing committee to examine these issues.²¹ The proliferation of social media and OTT platforms has significantly transformed the media landscape. Democratic institutions and traditional journalism, which previously relied on editorial controls to maintain accountability and content accuracy, have experienced a decline in these regulatory mechanisms. In the absence of such controls, social media serves both as a platform for press freedom and as a space for unregulated expression, which can include vulgar content. The Minister has therefore requested that the parliamentary standing committee on communications and information technology investigate this category of online content.

Fact-Checking Websites

Alt News is widely recognised as one of the leading fact-checking platforms in India. Its primary objective is to counter various forms of propaganda, misinformation, and disinformation disseminated on social media. The platform addresses topics such as politics, social issues, health, and community conflicts. Alt News produces comprehensive articles that examine the accuracy of diverse claims, evaluate visual content, and provide evidence-based refutations of false assertions. Additionally, Alt News engages with its audience across multiple social media channels, encouraging users to report inaccurate content for verification and fostering interactive communication. Fact Checker is an independent initiative in India that verifies information and disseminates it to the public. Its primary function is to investigate and authenticate claims made by public figures, including politicians and media personnel. The platform employs experienced journalists who conduct thorough research, gather evidence, and assess the validity of various statements. Fact Checker publishes detailed articles that present comprehensive fact checks and

²⁰ The Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021, G.S.R. 139(E), Gazette of India, Feb. 25, 2021.

²¹ Lalmani Verma, "Minister Ashwini Vaishnaw Calls for Stricter Laws to Regulate Social Media, OTT Platforms," The Indian Express, Nov. 28, 2024, available at: <https://indianexpress.com/article/india/minister-ashwini-vaishnaw-stricter-laws-regulate-social-media-ott-platforms-9693484/> (last visited on September 17, 2026).



International Journal of Engineering, Science and Humanities

An international peer reviewed, refereed, open access journal

Impact Factor: 8.3 www.ijesh.com **ISSN: 2250 3552**

provide access to the sources and evidence used in their analyses. The platform emphasises transparency and reliability, ensuring that its conclusions are based on rigorous research and comprehensive analysis. Quintuplet.com features a specialised fact-checking section, Web Qoof, operated by The Quint, a digital news platform. Web Qoof aims to dispel myths and false information prevalent in India by verifying claims and conducting thorough research, including interviews with subject-matter experts and reviews of official sources. The platform covers a broad spectrum of topics, including politics, health, and trending issues on social media. To engage a wider audience, Web Qoof presents its findings in diverse formats such as articles, videos, and infographics.

GOVERNMENT INITIATIVES AND INSTITUTIONAL MECHANISMS

The Indian Government has implemented several preventive measures to address this issue. Victims are now able to file online complaints regarding their grievances, which streamlines the process compared to traditional offline proceedings. The National Crime Reporting Portal²² The National Commission for Women and the Ministry of Women and Child Development have established platforms that allow complaints to be lodged online, via helpline numbers, or through email²³.

CONCLUSION

This research highlights the essential role of digital literacy in addressing cyberbullying. As technology advances, it is increasingly important for individuals to develop the skills necessary to navigate digital environments safely and responsibly. Digital literacy enables users to recognise, prevent, and respond to online harassment, thereby fostering a more supportive and respectful online environment. Recent legal judgments and actions by governments and organisations demonstrate a growing commitment to combating cyberbullying; however, the implementation of educational programs focused on digital literacy remains critical. Equipping individuals with the knowledge to understand digital dynamics can contribute to safer online communities and a reduction in cyberbullying incidents. Looking ahead, a comprehensive strategy that integrates education, policy, and technology will be essential for effectively reducing cyberbullying and maintaining digital spaces that support healthy and productive interactions. Imposing Australian-style social media restrictions in India would present significant challenges due to the country's large population and technological diversity. There are notable parallels with the increase in cybercrime affecting adults and businesses across various sectors. Banning specific websites represents a short-term measure that overlooks broader concerns related to digital literacy, cybersecurity, and effective online monitoring. Comprehensive solutions that address the underlying causes of cybercrime are required, rather than merely restricting internet access.

²² Government of India, "National Cyber Crime Reporting Portal," available at: <https://cybercrime.gov.in> (last visited on September 17, 2026).

²³ National Commission for Women, "Helplines," available at: <http://www.ncw.nic.in/helplines> (last visited on September 17, 2026).



International Journal of Engineering, Science and Humanities

An international peer reviewed, refereed, open access journal

Impact Factor: 8.3 www.ijesh.com **ISSN: 2250 3552**

SUGGESTION

1. Implementing a ban on social media for individuals under 18 in India presents significant challenges due to the country's large population and technological diversity, which complicate enforcement. Adolescents may circumvent such restrictions by using VPNs, false credentials, proxy websites, or alternative platforms. A more effective approach would promote safe online practices, enhance digital literacy, and provide tools that encourage responsible internet use. This strategy would enable children to access essential features while safeguarding them from harmful content, offering a more targeted and feasible solution.
2. The central issue concerns whether social media should be banned for children or subjected to stricter regulation. Rather than banning platforms, robust age-verification systems for content moderation could be an effective alternative. Such measures could include barriers that limit access to harmful content. Completely restricting children's internet access may seem protective, but it is impractical in today's digital era. Therefore, emphasis should be placed on promoting safe online practices and digital literacy.
3. Addressing this issue necessitates the establishment of a specific law that regulates and prescribes penalties for the offence, rather than relying on existing legal provisions.
The Indian Government is rapidly advancing digitalisation initiatives. To make them more effective, the government should promote digital literacy, especially at the school level, to increase children's awareness and responsibility when using online platforms and foster a safer cyber environment.