
CYBERBULLYING AND ONLINE HARASSMENT: A GROWING LEGAL CHALLENGE FOR YOUTH

Samiksha, UIILS, Chandigarh University

ABSTRACT

The internet is no longer a separate space from everyday life - for most young people it is where a large part of that life happens. Social media, messaging apps, online games and other digital platforms are used daily to study, socialise and express opinions. But the same tools that bring people together can just as easily be turned against them. Over the last decade, cyberbullying and online harassment have grown from a niche concern into a serious social and legal issue.

Traditional bullying stops at the school gate or the office door. Cyberbullying does not. A hurtful comment, an embarrassing photograph or an edited video can reach hundreds, sometimes thousands, of people within minutes, and it can keep resurfacing long after the original incident. Fake accounts, impersonation and anonymous messaging only make matters worse for the person on the receiving end.

This article looks at what cyberbullying and online harassment actually mean, why they happen, and what effect they have - particularly on young people. It draws on recent international data, walks through the relevant parts of Indian law, and considers the harder questions around privacy, free speech, platform responsibility and the growing role of artificial intelligence. The central argument is a simple one: punishment alone will not solve this problem. Legal awareness, digital literacy, sensible platform design, workable reporting systems and genuine emotional support all have to work together.

Keywords: Cyberbullying, Online Harassment, Youth, Social Media, Information Technology Act, BNS, Privacy, Freedom of Speech, Digital Safety.

Introduction

Picture a student opening their phone in the morning to dozens of messages mocking them. A photo that was never meant to leave a private chat has been shared in a group. Somebody has set up a fake account in their name, and classmates are commenting, laughing, forwarding it further. For the person going through this, it isn't an abstract "thing happening on the internet" - it is happening to them, in real time, and that distinction matters.

The internet has reshaped how young people connect. It lets them stay in touch with friends, meet new people, share ideas, and build an identity beyond their immediate surroundings. Online classes, digital entertainment and constant connectivity have become simply normal. Yet this same shift has opened up new ways for people to be hurt. A person can be bullied without the bully ever being in the same room. Abusive messages can arrive while someone is sitting quietly at home. A private photograph can end up circulating without consent. A rumour can move through a group chat faster than anyone can stop it. India's National Cybercrime Training Centre, operating under the Indian Cybercrime Coordination Centre, treats cyberbullying, cyberstalking and related social-media offences as priority areas for both public awareness and investigation¹.

The stakes rise further when the person affected is young. Adolescence and early adulthood are years spent building confidence, identity and relationships - and online humiliation during this period rarely stays confined to a screen. The WHO/Europe Health Behaviour in School-aged Children study, published in 2024 and covering more than 279,000 young people across 44 countries and regions, found that roughly one in six adolescents - about 15% - reported experiencing cyberbullying, while around 12% admitted to bullying others online². These are not small numbers. They point to something that families, schools, governments, law enforcement and technology companies all need to take seriously, rather than dismiss as ordinary teenage friction.

What Cyberbullying Actually Means

At its core, cyberbullying is bullying carried out through digital technology. It can take many

¹National Cybercrime Training Centre, Indian Cybercrime Coordination Centre, Ministry of Home Affairs, Government of India, <https://www.cybercrime.gov.in> (last visited Sept. 17, 2026).

²World Health Organization Regional Office for Europe, One in Six School-Aged Children Experiences Cyberbullying, Finds New WHO/Europe Study (2024).

forms, including but not limited to:

- Social-media platforms
- Messaging applications
- Online gaming
- Email
- Discussion groups
- Comments and posts
- Fake accounts
- Digital photographs and videos
- Manipulated or edited content

It shows up as repeated insults, spreading rumours, threats, deliberate exclusion from online groups, sharing embarrassing material, or impersonating someone else entirely. UNICEF describes cyberbullying as something that can occur across social media, messaging platforms, gaming spaces and mobile phones generally, and it makes an important point: harmful online content leaves a digital footprint, which can later serve as evidence of what actually took place³.

Consider a fairly ordinary scenario. Two students have an argument. Rather than sorting it out privately, one of them sets up a fake social-media account and starts posting insulting content about the other. Friends pick it up, share it further, add their own comments - and within a short time, what began as a personal disagreement has become a public spectacle the original student never agreed to.

Cyberbullying vs. Online Harassment: Not Quite the Same Thing

These two terms tend to get used interchangeably, but they aren't identical. Cyberbullying is generally understood as bullying through digital means, and it's a term most often applied to children and young people specifically. Online harassment is the wider category - it can involve repeated unwanted contact, threats, stalking, abusive messages, impersonation, the publishing

³UNICEF, How to Stop Cyberbullying, UNICEF Online Safety Guidance.

of private information, or other harmful conduct online, regardless of the age of those involved.

It's worth being precise here, because not every unpleasant online exchange qualifies as cyberbullying. People disagree on the internet constantly. They criticise opinions, express unpopular views, argue back. None of that should automatically be labelled harassment. The genuinely difficult task - legally and socially - is telling ordinary disagreement apart from conduct that crosses into threatening, abusive, intimidating, humiliating or unlawful territory.

What the Data Actually Shows

The 2024 WHO/Europe HBSC study surveyed more than 279,000 young people across 44 countries and regions⁴. Its key findings:

- About 15% of adolescents reported experiencing cyberbullying.
- About 12% reported cyberbullying others.
- Reported cyberbullying rose between 2018 and 2022.
- Among boys, reported experience rose from 12% to 15%.
- Among girls, reported experience rose from 13% to 16%.

A caveat worth repeating: these figures describe the population the WHO/Europe study actually covered. They are not India-specific numbers, and should be read as international evidence rather than mistaken for Indian statistics. UNESCO has raised a related concern from a different angle - its material on school violence and bullying, drawing on the 2024 Global Education Monitoring Youth Report, notes that 58% of girls and young women report facing online harassment⁵. Within India, the National Cybercrime Training Centre has identified cyberbullying and cyberstalking as specific cyber-safety concerns and produces awareness material aimed at parents and young people⁶.

⁴World Health Organization Regional Office for Europe, One in Six School-Aged Children Experiences Cyberbullying, Finds New WHO/Europe Study (2024).

⁵UNESCO, School Violence and Bullying, citing GLOBAL EDUC. MONITORING YOUTH REPORT (2024).

⁶National Cybercrime Training Centre, Online Safety Tips and Cyber Awareness Material, Ministry of Home Affairs, Government of India.

Where Indian Law Stands

India has no single, dedicated "Cyberbullying Act." Instead, depending on exactly what happened, different statutes may come into play. The Information Technology Act, 2000 remains the country's primary statutory framework for offences and legal questions involving electronic communication and technology⁷. Depending on the facts, conduct online may also fall under the Bharatiya Nyaya Sanhita, 2023 (BNS), which replaced the Indian Penal Code from 1 July 2024⁸.

The legal issues that can arise include:

- Criminal intimidation
- Stalking
- Defamation
- Intentional insult
- Identity-related offences
- Privacy violations
- Unlawful publication or transmission of electronic material
- Offences involving children

Which provision actually applies depends entirely on the specific facts of a case. It would be inaccurate to suggest that every instance of cyberbullying automatically falls under one fixed section of the IT Act - that simply isn't how the law works here.

The Information Technology Act, 2000

The IT Act was originally enacted to give legal recognition to electronic transactions and communication, and more broadly to address technology-related legal issues as they arose⁹.

⁷Information Technology Act, No. 21 of 2000, INDIA CODE (2000).

⁸Bharatiya Nyaya Sanhita, No. 45 of 2023, INDIA CODE (2023).

⁹Information Technology Act, No. 21 of 2000, INDIA CODE (2000).

Some of its provisions become directly relevant when online harassment involves unlawful electronic content - Sections 67, 67A and 67B, for instance, deal with different categories of prohibited electronic content, including material involving children.

One point law students in particular should know: Section 66A of the IT Act is not a valid basis for prosecuting ordinary online harassment today. The Supreme Court struck it down in *Shreya Singhal v. Union of India* (2015)¹⁰. Yet a surprising number of older articles floating around online still cite Section 66A as though it remains good law - it does not, and relying on it is a genuine error.

Privacy and Cyberbullying

Privacy sits close to the centre of most online harassment cases. The Supreme Court's decision in *Justice K.S. Puttaswamy (Retd.) v. Union of India* (2017) recognised privacy as a constitutionally protected right¹¹, and this becomes directly relevant whenever someone's private information, photographs, conversations or personal data are shared without proper justification.

Take a simple example: a private conversation is screenshotted and posted publicly to embarrass someone. That single act can raise privacy questions alongside whatever other legal issues the underlying content might involve.

How Cyberbullying Affects Young People

Because digital platforms are so central to how young people live day to day, cyberbullying and online harassment can hit unusually hard. Unlike bullying confined to a physical location, online harassment doesn't end when the school day does - it follows a young person home, onto their phone, their laptop, their social media accounts. A single harmful comment, an embarrassing photo, a fake account, a threatening message, or a pattern of repeated humiliation can end up shaping much more than someone's online experience.

The consequences reach into education, relationships, confidence, behaviour and general wellbeing, and they're worth breaking down individually.

¹⁰*Shreya Singhal v. Union of India*, (2015) 5 S.C.C. 1 (India).

¹¹*Justice K.S. Puttaswamy (Retd.) v. Union of India*, (2017) 10 S.C.C. 1 (India).

1. Emotional and Psychological Impact

The emotional toll is often the most immediate. Young people facing repeated online harassment can feel embarrassed, angry, frightened, isolated or simply helpless. Many describe a constant low-level worry - what is being said about them right now, whether a particular photo or post is being reshared somewhere they can't see. Because content online can be viewed and passed along by so many people at once, victims often report feeling like there's nowhere private left to retreat to. Confidence takes a hit too: a student who was previously outgoing in class or social settings may withdraw, avoiding interaction out of fear of being judged or mocked further.

2. Impact on Education

Cyberbullying spills directly into academic life. A student under sustained online harassment may struggle to concentrate, or start avoiding school or university altogether. If someone is being repeatedly mocked in a class WhatsApp group or targeted on Instagram, for example, simply attending class can become uncomfortable - they know they'll be seeing the same people who are behind it, or watching it happen, in person.

3. Impact on Privacy and Reputation

There's also the matter of privacy itself being violated. Sharing someone's private photographs, messages or personal information without consent causes real, lasting harm - as does setting up a fake profile in their name. Both can seriously damage a person's standing among friends, classmates and teachers. For young people specifically, this kind of reputational damage is especially hard to shake, since digital content has a way of resurfacing or being reshared even long after the original post is taken down.

The Role of Schools, Universities and Parents

Educational institutions and parents are both central to preventing cyberbullying and responding to it properly when it happens. Schools and universities should have clear anti-cyberbullying policies in place, confidential channels for reporting, regular digital-safety awareness sessions, and access to counselling for students who need it. Teachers and staff need training to recognise the warning signs early and to handle complaints fairly and with sensitivity - not dismissively.

Parents matter just as much, arguably more, because young people frequently avoid bringing up online problems out of fear they'll be blamed or have their phone taken away as a punishment. A better response is to listen without judgment, offer support, teach responsible internet habits, and help preserve evidence - screenshots, saved messages - when it's needed later. When schools, universities and parents actually coordinate, young people are far better equipped to block and report harmful accounts, protect their own privacy, and avoid becoming part of the problem themselves. An environment where young people feel safe speaking up is, in the end, one of the strongest defences against cyberbullying escalating further.

Cyberbullying Compared to Traditional Bullying

Traditional bullying tends to happen in fixed physical spaces - schools, colleges, playgrounds, neighbourhoods - where both the victim and the bully are physically present. It can involve teasing, insults, threats, deliberate exclusion, or making someone feel persistently unwelcome. Cyberbullying plays out differently, through digital platforms: social media, messaging apps, online games and other internet spaces.

Even so, the underlying harm is similar. What sets the two apart is mostly geography and time. Traditional bullying can end, at least temporarily, once the victim leaves the location where it happened. Cyberbullying doesn't offer that same escape - it follows a person through their phone wherever they go, and a single hurtful post or photo can reach a large audience almost instantly. That combination can leave victims feeling like there's no safe space left at all. But in both cases, the real issue was never really the method - it's the human cost behind it: fear, embarrassment, loneliness, eroded confidence, difficulty trusting others afterward. That's precisely why cyberbullying deserves to be taken exactly as seriously as bullying that happens face to face, even though it unfolds behind a screen.

Conclusion

Cyberbullying and online harassment have stopped being purely "digital world" problems - they are now genuine social and legal concerns woven into the everyday lives of young people. A hurtful comment, an embarrassing photo, a fake account or a threatening message might look small to whoever is posting it, but for the person on the other end, it can be genuinely painful and hard to shake off. Unlike bullying confined to a physical place, online harassment can reach a young person even at home, making it that much harder to find anywhere that feels

completely safe.

The answer isn't to pull young people away from technology - it's to help them use it responsibly and safely. Schools and universities need to provide real awareness training, digital-safety education, functioning complaint mechanisms and emotional support. Parents need to build an environment where young people feel comfortable talking about what's happening to them online, without fear of being blamed for it. Laws and the platforms themselves also carry real responsibility for protection and accountability.

Perhaps the most important thing to remember is this: behind every profile, every photograph, every username, there is an actual person with real feelings. Before posting, sharing or commenting, it's worth pausing to consider what effect that action might have on someone else. Building a genuinely safer digital environment takes more than laws and technology alone - it takes empathy, awareness, responsibility and basic respect. If young people, families, schools, governments and technology platforms actually work together on this, the internet has every chance of becoming a space where young people feel connected and empowered, rather than threatened or humiliated.