



CYBERBULLYING: PROTECTING YOUR ONLINE IDENTITY AND REPUTATION

Anushka Bajpai

Bharati Vidyapeeth (Deemed to be University), New Law College, Pune, India

1. ABSTRACT

Everyone is acquainted with the term "internet," which has been around since 1983. For the Indian society, the internet has proven to be both a blessing and a curse. The widespread adoption of the internet has sparked a massive technological revolution in India that has fundamentally altered peoples' ways of thinking and conducting business. The internet has impacted every area of everyday life, making it easier to communicate with individuals around the world and offering information to a wide range of social classes with the touch of a button. As technology advanced, unforeseen dangers from cybercrimes arose. Cyberstalking, cyberbullying, spoofing, phishing, and credit card fraud are only a few examples of the numerous potential cybercrimes, many of which are yet unpredictable. Cyberbullying is a type of internet communication that has a lasting negative effect on a person's reputation or privacy, or that harasses, threatens, or bullies them. The purpose of the article is to explain the concept of cyberbullying, along with its kinds, causes, and available legal grounds under the Information Technology Act of 2000 and the Indian Penal Code of 1860.

Keywords: Cyberbullying, Harassment, Online bullying, Victims, Aggression, Abuser

2. INTRODUCTION

India is a developing country and it is growing rapidly in every other sector including cyber world. However along with the rise of the virtual world, India is also seeing a sharp surge in the number of cybercrimes along with the rise of the virtual world.

Bullying is a form of aggressive behaviour in which one person purposefully and persistently makes another feel awful or embarrassed.

So exactly what is cyberbullying?

Cyberbullying or electronic aggression is referred to as a form of online harassment or bullying that takes place over text, email, instant messaging, a website, blogs. The word "cyberbullying" was first used by a Canadian Bill Belsey in 2000 on a website he created to combat traditional or face-to-face bullying.[1] Cyberbullying is a widespread social practise that can have a detrimental impact on a victim's physical well-being, behaviour, and mental health. Cyberbullying victims might not be aware of their bully's identity or the reason why they are being targeted. the materials or the type of media used to harass the victim can be instantly disseminated with a large audience and remains available even after the initial incident. And this harassment can have significant ramifications on the victim. Although there are several major differences, cyberbullying often resembles traditional bullying. Traditional bullying and online bullying often coexist. However, cyberbullying leaves a digital trail—a record that may be helpful and give proof to bring an end to the abuse.

2.1 DEFINITIONS

- i. **National Crime Prevention Council defines** - “Cyberbullies can be classmates, online acquaintances, and even anonymous users, but most often they do know their victims.” [2]
- ii. **According to the Merriam-Webster Dictionary-** cyberbullying was first used in 1998 and is defined as “the electronic posting of mean-spirited messages about a person (such as a student) often done anonymously.” [3]
- iii. **StopBullying.gov defines** -Cyberbullying as “bullying that takes place over digital devices like cell phones, computers, and tablets. Cyberbullying can occur through SMS, Text, and apps, or online in social media, forums, or gaming where people can view, participate in, or share content. Cyberbullying includes sending, posting, or sharing negative, harmful, false, or mean content about someone else. It can include sharing personal or private information about someone else causing embarrassment or humiliation. Some cyberbullying crosses the line into unlawful or criminal behaviour.” [4]
- iv. **Cyberbullying Research Center defines-** Cyberbullying as the “wilful and repeated harm inflicted through the use of computers, cell phones, and other electronic devices.” [5]
- v. **UNICEF defines Cyberbullying as** “Bullying with the use of digital technologies. It can take place on social media, messaging platforms, gaming platforms and mobile phones. It is repeated behaviour, aimed at scaring, angering or shaming those who are targeted. Examples include:
 - spreading lies about or posting embarrassing photos or videos of someone on social media
 - sending hurtful, abusive or threatening messages, images or videos via messaging platforms

- impersonating someone and sending mean messages to others on their behalf or through fake accounts.”

[6]

3. TYPES OF CYBERBULLYING [7]

- i. **Cyberstalking** - Cyberstalking is a type of internet harassment where a victim is stalked using digital communications. Because there is usually a real threat to the victim's safety, this type of cyberbullying is regarded as being more hazardous than others. Cyber-stalkers may send repeated messages with the intention of threatening or harassing persons and. It is the persistent use of technology, such as social media, emails, and text messages, to contact and someone while making them fear for their safety. It is similar to traditional stalking because it invades the target's privacy and has the potential to be traumatising.
- ii. **Trolling** - Trolling or online trolls deliberately aim to aggravate or offend others in an effort to provoke a response. While some trolls participate in cyberbullying, others may be up to relatively harmless mischief. Trolls and cyberbullies may not always have the same objectives. Generally, these bullies don't have little personal connection to their victims and are more disengaged from them. Trolling can cause trouble because people might find it funny but it is inherently aggressive.
- iii. **Impersonation/Masquerading** - Impersonation, or acting in another person's online persona, is another usual form of cyberbullying. Teens can do this in a variety of techniques, but one of the most popular is to hack the account or steal the password in order to alter the target's profile. Once they obtain access, they might publish offensive content such as sexual, racist, or other things to damage the target's reputation and status in society. Or they could engage in conversation with others while acting like the victim. To upset and enrage the target's friends or acquaintances, they will say hurtful things. Another usual strategy is to create a screen name or social media account that is similar to the target's if they are unable to access the target's account. The account might appear real by using actual images of the victim.
- iv. **Harassment** - Harassment is a broad phrase that encompasses a variety of cyberbullying, but it typically refers to a persistent behaviour of sending offensive or threatening comments to others online. Teens may bully others by starting warning wars. This happens when people use a website's report feature to take down or put someone else offline—even when they are not breaking any rules. Children engage in text battles or text assaults as well. This kind of harassment happens when several children text the target repeatedly. Cyberbullies occasionally use a covert approach online, like sub tweeting and vague booking, which entails writing hurtful things about someone without specifically naming them. Other times, they will be very blatant in their harassment, intimidating the victim via email, instant messaging, and text messages.

- v. **Flaming** - The act of using inappropriate language or by using vulgarity to broadcast remarks on internet is known as flaming or roasting. This word shouldn't be used interchangeably with trolling, which describes someone's actions that incite controversy in real life or online. This concept evolved as users of Web forums can respond more violently because of their anonymity.
- vi. **Doxing** - The act of publicly disclosing private or sensitive information about someone without that person's consent with the intent to embarrass or humiliate them is generally referred to as doxing. This can also include sharing preserved personal communications in an online private group as well as disseminating private photos or data of celebs. The crucial factor is the victim's lack of permission.
- vii. **Frapping** - It is when an abuser uses your person's name to publish offensive content on social media. It might be innocuous but sometimes quite risky when people post wacky things to each other's pages. In order to damage someone's reputation, a bully might publish homosexual or racial insults on their profile.

4. CAUSES OF CYBERBULLYING

1. There are a number of additional characteristics that can lead someone to engage in cyberbullying, including personality qualities that can lead to antisocial or bullying behaviour.
2. The main reason for cyberbullying is when the perpetrator is fully anonymous, which makes it easier for the abuser to attack anyone online by disguising his or her true identity. [8]
3. Egotism can be a mindset in which people prioritise their relationships with others over their social standing and power. [9]
4. Aggression, which is defined as using force to overcome setbacks and failures, drives people to engage in cyberbullying as a kind of gratification. [10]
5. Online shyness or restricting, in which someone bullies another for the sake of hurt, dominance, retaliation, or just for pleasure, is another major factor.
6. The findings suggest that moral disengagement has an equivalent impact on bullying perpetration for those who are most engaged, independent of the victimisation status at the time, which points to one of the other explanations as moral disentanglement.

5. COVID-19 AND CYBERBULLYING

An upsurge in cyberbullying and more time invested online might have result from Covid -19. Due to the pandemic, many people experienced unfamiliar and unsettling emotions including worry, rage, fear, loneliness, or stress.[11] Children and teenagers are using internet platforms more frequently now that COVID-19 is widespread. They use digital platforms for more than just for online classes but also for chatting with their friends. Teens became accustomed to studying and connecting with friends electronically. And given the prevalence of social media and smartphones, abusers among students are more likely to engage in cyberbullying. Zoom has already faced criticism for the recent interruption of internet business meetings by strangers who posted offensive and offensive comments. If Zoom is so simple to hack into, teens and children are sure to try to do the same. The Zoom platform's security and privacy have been hacked, according to reports that have been sent to the New York City DOE (Department of Education). The DOE will no longer allow Zoom to be used as a result of their examination of this supporting documentation.[12]

6. STATISTICS OF BULLYING AND CYBER BULLYING

- i. According to the National Centre for Education Statistics and the Bureau of Justice's 2019 School Crime Supplement to the National Crime Victimization Survey, bullying affected roughly 22% of students nationwide between the ages of 12 and 18. [13]
 - ii. According to the 2019 Youth Risk Behaviour Surveillance System (Centres for Disease Control and Prevention), 19.5% of students in grades 9 through 12 nationwide report experiencing bullying on school grounds in the year before the survey.[14]
 - iii. According to recent studies, including a sizable surveillance study on bullying, 30% of young people engage in this behaviour. A harsh comment or insult has been directed at about 58% of students, either offline or online. [15]
 - iv. According to data from the American Justice Department, 1 in 4 kids will experience bullying during their teens. [16]
 - v. According to statistics on cyberbullying, India has the third-highest incidence after China and Singapore. The most frequently impacted age group is 8 to 17-year-old children.[16]
 - vi. McAfee Report – [17]
1. The market research firm MSI-ACI invited parents of children between the ages of 10 and 18 to participate in the study between June 15 and July 5, 2022, by sending them an email with a link to an online survey. In total, 11,687 parents and their kids from ten different countries—the US, UK, France, Germany, Australia, India, Canada, Japan, Brazil, and Mexico—completed the poll.

2. 85% of Indian children cyberbullied, highest globally.
 3. “Cyberbullying in India reaches alarming highs as more than 1 in 3 kids face cyber racism, sexual harassment, and threats of physical harm as early as the age of 10 - making India the #1 nation for reported cyberbullying in the world,” said Gagan Singh, Chief Product Officer, McAfee.
 4. The percentage of youngsters in India who have experienced racist cyberbullying is 42%, which is startlingly 14% more than the global average of 28%. Along with racism, the most extreme kinds of cyberbullying reported were trolling (36%) personal attacks (29%) sexual harassment (30%) threats of self-harm (28%), and doxing (23%), all of which were almost twice as common as the global average. Additionally, 39% of India's respondents reported spreading false rumours, 35% reported being excluded from groups and conversations, and 34% cited name-calling as prevalent forms of cyberbullying. On practically every social media and messaging platform, Indian youngsters see and endure the highest cyberbullying. 44 %
- vii. According to the Centres for Disease Control 2017, in high school, 15.5% of students experience cyberbullying and 20.2% experience bullying on school grounds. [18]
- viii. Victims of cyberbullying are 1.9 times more likely to commit suicide Bullying does more than merely erode victims' self-esteem. It could be worse. Cyber bullying statistics for 2022 show that its victims are twice as likely to experience suicide thoughts after being subjected to it. As a coping strategy, self-harming behaviour is also frequently used by victims. Furthermore, suicide is 1.7 times more likely to occur among offenders. Bullies do indeed come from unpleasant places, and the simplest way for them to cope with their problems is to harm both themselves and other people. Anti-bullying rules are therefore desperately needed in schools to help stop the issue. [19]
- ix. The likelihood of cyberbullying occurring among youth who identify as LGBTQ is much higher. According to the Cyberbullying Research Centre's survey, 56% of students who identified as LGBTQ had experienced cyberbullying, compared to only under a third of non-LGBTQ people. [20]

7. LEGISLATION

Laws prevailing in India

Cyberbullying is one such offence that causes mental agony in the mind of the victim for life, and they cannot easily get over it. In some cases, the effects of such cybercrimes are so extreme that the victim may also commit suicide. This act describes cyber offences and punishment for each offence. The Government of India passed the Information Technology Act, 2000 as a piece of law to address crimes committed in cyberspace or on the internet. The act also specifies penalties for such offences. It may seem preposterous,

yet there is no explicit law in India that addresses cyberbullying. Cyberstalking was deemed a criminal offence in the 2013 amendment to the act; however, cyberbullying has not yet been included.

Information Technology Act, 2000

The Indian Parliament passed the Information Technology Act, 2000 in the same year. For issues including e-commerce and cybercrime, it serves as the main legal framework in India. The act was passed to offer electronic trade and transactions legal legitimacy, to facilitate e-governance, and to combat cybercrime. This statute allows for the prosecution of foreign nationals for any offence involving an Indian computer system or network. Penalties are set forth by law for numerous forms of digital/electronic fraud and cybercrime. Digital signatures are also given legal legitimacy by this act. [21] Nevertheless, some of the provisions in Chapter XI of this act may offer some relief from the effects of cyberbullying:

Section 66(A): This section addresses the penalties for sending offensive, disparaging, abusive, or cruel remarks or materials over the internet via social media or any other digital chat room \or platform. Shall be punishable with imprisonment for a term which may extend to three years and with fine. [22]

Section 66 D: If someone deceives or cheats someone online using social media or any other online platform, they should be penalised with up to three years in prison and a fine of up to one lakh rupees. [23]

Section 66 (E): This section deals with the penalties for privacy infringement. If a person violates someone's privacy digitally, using their photos or sharing information, he is guilty of cyberbullying in some way and must be levied with a fine up to 3 lakh rupees or imprisonment for up to 3 years. [24]

Section 67: This section of the act deals with the penalties for posting, sending, or disseminating unpleasant, vulgar, or impolite information on the internet or in cyberspace. The maximum fine is 10 lakh rupees, and the maximum term of imprisonment is five years. [25]

Cyber Bullying Laws Under Indian Penal Code 1860

Cyberbullying is not specifically mentioned in the IPC as a form of harassment. But, a number of laws, including the following, may address the crimes of online bullying:

Section 507: if someone is subjected to criminal intimidation through an anonymous communication, the individual issuing the threats is subject to a maximum two-year sentence in prison. By virtue of the word "anonymous," cyberbullying and anti-bullying offences.[26]

Section 509: Anyone who makes an attempt to disparage the modesty of another woman may face legal action. This includes conduct that takes place online or on social media. Up to one year in prison is possible as a punishment, along with or without a fine. [27]

Section 354(C): When a woman is in her private area, it is illegal to capture her image without her consent or authority. If the accused continues to break the law, he may receive a term of three – seven years in prison instead of the possible range of one – three years.[28]

Section 354(D): If a person secretly follows another person online or keeps tabs on their everyday activities with the intent to hurt them or cause them harm, or if they do so for personal gain, they may face punishment. Up to three years in prison might be the punishment.[29]

Section 499: If someone creates or publishes any imputation about another person with the intent to injure that person's reputation or with knowledge that such imputation will do so, they are said to have defamed that person.[30]

Section 500: Anyone found guilty of defamation must either pay a fine, serve a sentence of simple imprisonment up to two years, or both.[31]

8. CASE LAWS

1. Manish Kathuria v. Ritu Kohli

This case was concerned with the stalking of Ritu Kohli, was the first known instance of cyber-stalking in India and the impetus behind the IT Act's revision in 2008. Kohli was stalked on a chat platform by Kathuria, who subsequently verbally assaulted her and gave her phone information to a number of others. Later, he started chatting on "www.mirc.com" using Kohli's guise. She then began getting nearly 40 vulgar phone calls over the course of three days at unusual hours. She was compelled by this circumstance to report the incident to the Delhi Police. After receiving the report, the Delhi Police tracked down the IP addresses and detained Kathuria in accordance with Section 509 of the Indian Penal Code. [32]

2. Jitender Singh Grewal v. The State of West Bengal

The defendant made a false victim Facebook account and posted her pornographic images there. The accused was charged with violating Sections 354A, 354D, 500, 509, and 67A of the IT Act. He applied for bail. The accused's motion for bail was denied by the trial court, and the Calcutta High Court supported this decision. [33]

3. Shubham Bansal v. The State (Govt of NCT Delhi)

The victim in this case experienced aggravation, insult, and harassment as a result of the accused's creation of a fraudulent Facebook account using Nidhi Taneja's name and the victim's phone number. As a result, a FIR was filed against the accused.

The victim then filed a second application pursuant to Section 173(8) of the CrPC asking the investigating officer to conduct an additional inquiry. As a result, the case was remanded to the Metropolitan Magistrate for further consideration. The accused then submitted a request to have the proceedings against him under Section 66A of the IT Act and Section 509 of the IPC dismissed. While rejecting the accused's appeal, the Delhi High Court directed that the investigating officer hold off on presenting his final report until the Magistrate gave instructions on the victim's ongoing application. The honourable court noted that the investigating officer's other option was to submit a report based on the work done up until that point, reserving the right to submit a follow-up challan or report in response to the victim's ongoing request for additional investigation under Section 173 (8) of the CrPC. [34]

4. Prakhar Sharma v. The State of Madhya Pradesh

The accused created a phoney Facebook account for the victim in addition to posting some depraved statements and pictures of the victim that were downloaded from her original Facebook account. Charges were brought against the defendant under Sections 66(C), 67, and 67(A) of the IT Act. The accused's bail application was denied by the Madhya Pradesh High Court.[35]

9. SUGGESTIONS

- i. Since the mode, repercussions, gravity, and potential targets differ, it is necessary to define specific laws for cybercrime offences.
- ii. Remind your child that you can always change their contact information if ignoring and blocking the cyberbullies does not work or only serves to amplify their attempts. Tell them you'd be pleased to assist them in changing their phone number and email address, and make sure they know it.
- iii. keep a log of all messages, remarks, and other internet bullying-related abuse. not to delete any communications and show them how to take screenshots. If you need to get in touch with any authorities, having evidence of the bullying will be useful.
- iv. Encourage your teen to refrain from responding to online bullies. It can be challenging to ignore deliberately hurtful remarks, but reassure your teen that doing so will only make the bully's tactics worse and that they are only trying to provoke a response. If your teen ignores the bullies, there is a better likelihood that the bullying will stop.
- v. Remind your child to delete any social media or phone numbers associated with bullies. This is particularly crucial if your adolescent finds it difficult to ignore the bullies or if they are persistent.

- Encourage your kid to block those accounts as well because bullies might create new ones or enlist the help of others to harass your teen in the future.
- vi. Even if the post is taken down, once something is posted online, it can never completely be erased. You should always consider who might eventually see the stuff you share online because you cannot predict or limit their access.
 - vii. When striving to address this issue, campaigns, laws, administrative changes in schools, and other actions aimed at identifying and eradicating cyberbullying are a good place to start. Promoting safe technology use can have favourable effects.
 - viii. Cyberbullying is one of the crimes that has to be tackled right away since it has the potential to escalate into something hideous. Considering how severely such an offence impacts a child's mental health, lawmakers should consult with psychiatrists while drafting laws against online bullying.
 - ix. To sensitize everyone—especially young people—on what defines cyberbullying and how to prevent being a victim. Seminars, webinars, articles, etc., can accomplish this.
 - x. Safeguard your privacy and establish personal boundaries.
 - xi. Paediatricians should receive special training to help support and care for children's social, mental, and developmental well-being.
 - xii. Both the offender and the victim should receive counselling. Since the intention is to inform the public and help them recognise their faults, the offender and victim may both benefit from counselling after such incidents, and in many cases, the abusers themselves have a history of bullying.
 - xiii. Since these offences have a higher influence on an individual's mental health than their physical health, mental health specialists should be consulted throughout the formulation of such regulations.

10. CONCLUSION

Cyberbullying lurks behind all of these different sorts of social media as the power of technology grows and more people are encouraged to do so. As stated earlier, electronic aggression or online bullying occurs when someone frequently and purposely harasses, mistreats, or mocks another person while utilising a computer, a smartphone, or any other electronic device. The use of social media, mobile devices, text messages, and online apps are methods and weapons of cyberbullying but these tools themselves are not the issue, people's decisions lead to cyberbullying. It has huge impact on persons physical and mental health. Cyberspace in India is constantly evolving, unlike physical space, it is impossible to predict in advance the crimes that may take place. Therefore, it must be tackled as soon as possible. Even the constitutionally protected right to freedom of expression is subject to certain reasonable limits, and the same must be true of freedom of expression on the Internet. However, using this freedom to emotionally harass or threaten someone should not be acceptable. The idea of justice would be lost if those who have been victimised by cybercrime were allowed to endure much more suffering. A robust mechanism for combating cyberbullying should be put in place, and the current laws against cybercrimes should be tightened.

11. REFERENCES

- [1] https://www.researchgate.net/publication/265937264_Cyberbullying_a_Virtual_Menace
- [2] <https://www.ncpc.org/resources/cyberbullying/>
- [3] <https://www.merriam-webster.com/dictionary/cyberbullying>
- [4] <https://www.stopbullying.gov/cyberbullying/what-is-it>
- [5] <https://cyberbullying.org/what-is-cyberbullying>
- [6] <https://www.unicef.org/end-violence/how-to-stop-cyberbullying>
- [7] <https://www.parentcircle.com/cyberbullying-laws-and-policies-in-india/article>
- [8] <https://www.legalserviceindia.com/legal/article-10150-cyber-bullying-a-brief-analysis.html>
- [9] <https://www.legalserviceindia.com/legal/article-10150-cyber-bullying-a-brief-analysis.html>
- [10] <https://www.legalserviceindia.com/legal/article-10150-cyber-bullying-a-brief-analysis.html>
- [11] <https://www.pacer.org/bullying/classroom/pdf/covid-infographic-parents.pdf>
- [12] <https://www.stompoutbullying.org/blog/Cyberbullying-During-COVID-19>
- [13] <https://www.stopbullying.gov/bullying/what-is-bullying#frequency>
- [14] <https://www.stopbullying.gov/bullying/what-is-bullying#frequency>
- [15] https://www.medindia.net/health_statistics/health_facts/top-15-facts-about-bullying.htm
- [16] https://www.medindia.net/health_statistics/health_facts/top-15-facts-about-bullying.htm
- [17] https://www.medindia.net/health_statistics/health_facts/top-15-facts-about-bullying.htm
- [18] https://www.business-standard.com/article/current-affairs/85-of-indian-children-cyberbullied-highest-globally-mcafee-report-122080800536_1.html
- [19] <https://www.stompoutbullying.org/blog/Cyberbullying-During-COVID-19>
- [20] <https://digitalcooperation.org/research/cyberbullying/>

- [21] <https://online.maryville.edu/blog/what-is-cyberbullying-an-overview-for-students-parents-and-teachers/>
- [22] <https://byjus.com/free-ias-prep/information-technology-act-2000/>
- [23] https://www.indiacode.nic.in/bitstream/123456789/13116/1/it_act_2000_updated.pdf
- [24] https://www.indiacode.nic.in/bitstream/123456789/13116/1/it_act_2000_updated.pdf
- [25] https://www.indiacode.nic.in/bitstream/123456789/13116/1/it_act_2000_updated.pdf
- [26] https://www.indiacode.nic.in/bitstream/123456789/13116/1/it_act_2000_updated.pdf
- [27] https://www.iitk.ac.in/wc/data/IPC_186045.pdf
- [28] https://www.iitk.ac.in/wc/data/IPC_186045.pdf
- [29] https://www.iitk.ac.in/wc/data/IPC_186045.pdf
- [30] https://www.iitk.ac.in/wc/data/IPC_186045.pdf
- [31] https://www.iitk.ac.in/wc/data/IPC_186045.pdf
- [32] https://www.iitk.ac.in/wc/data/IPC_186045.pdf
- [33] <https://www.mondaq.com/india/crime/989624/anti-cyber-bullying-laws-in-india---an-analysis>
- [34] <https://www.mondaq.com/india/crime/989624/anti-cyber-bullying-laws-in-india---an-analysis>
- [35] <https://www.mondaq.com/india/crime/989624/anti-cyber-bullying-laws-in-india---an-analysis>