



The Indian Journal for Research in Law and Management

Open Access Law Journal – Copyright © 2026

Editor-in-Chief – Dr. Muktai Deb Chavan; Publisher – Alden Vas; ISSN: 2583-9896

This is an Open Access article distributed under the terms of the Creative Commons Attribution-Non-Commercial-Share Alike 4.0 International (CC-BY-NC-SA 4.0) License, which permits unrestricted non-commercial use, distribution, and reproduction in any medium provided the original work is properly cited.

CYBERBULLYING LAWS IN INDIA

~*Kriti Jaiswal*

Abstract

Rapid proliferation of internet usage and social media usage has resulted in the problem of cyber bullying that poses severe threats to the dignity, privacy and mental health of individuals. In India, the problem of cyber bullying is regulated by a number of provisions from the Information Technology Act, 2000, Bharatiya Nyaya Sanhita, 2023 and other laws, but there is no particular statute that covers this crime. The current research paper is aimed at analyzing the regulatory framework of the law that regulates the issue of cyber bullying and at identifying problems with its implementation. The paper will evaluate the potential of court decisions and digital intermediaries to address online harassment as well.

Keywords: Cyber Bullying, Information Technology Act, Bharatiya Nyaya Sanhita, Cybercrime, Online Harassment, India.

INTRODUCTION

With the advent of the Internet, people have become more connected in all walks of life. From communication to education, trade, governance to recreation, all aspects of everyday life now hinge on the Internet. India has been experiencing a lot of digital growth in the last decade owing to the use of smartphones cheaper internet access and efforts of the government like Digital India. Despite having contributed positively to our lives these advancements have also made us vulnerable to different kinds of cybercrimes. Cyberbullying is one of the many cybercrimes that has become a serious concern in the recent years.

Unlike the conventional form of bullying, cyberbullying does not have any geographical boundaries nor does it happen in the physical world. Messages filled with offense, distorted

pictures, fake social media accounts, defamatory posts and public humiliation are some of the common features of cyberbullying which are spread instantaneously on the online platforms causing immense harm to the victim.

The issue of cyberbullying has raised concerns in particular amongst school/college students, professionals, women, journalists, public personalities and members of vulnerable groups. Victims of cyberbullying suffer from depression, anxiety, loneliness, low self-esteem and in some cases suicidal thoughts. Such facts demonstrate the importance of addressing the problem of cyberbullying as it is not only an issue related to the use of new technologies but a matter of human rights which include such aspects as respect, dignity, privacy, equality and freedom. Despite the existence of laws against cybercrime in India, there is no specific legislative act which addresses the problem of cyberbullying and criminalizes it.

Therefore, the victim of cyberbullying uses different laws which regulate matters like intimidation, harassment, obscenity, defamation, stalking, identity theft and the violation of privacy. New developments in technologies such as the use of artificial intelligence, deep fake technologies and encryption of communication create additional difficulties in law enforcement.

MEANING AND CONCEPT OF CYBERBULLYING

Cyberbullying is defined as the systematic and repeated use of technology to torment, scare, threaten, embarrass or belittle someone. The act includes the use of electronic communication gadgets such as mobile phones, personal computers, laptops and other technological gadgets to emotionally or psychologically torture another individual. As opposed to disputes that arise from the internet cyberbullying is characterized by the constant and deliberate acts intended to torment the victim.

The most unique aspect about cyberbullying is its ability to be experienced by a large number of people simultaneously. Unwanted content on the internet can be duplicated and posted indefinitely, thus making it impossible for the victim to stop the torment. Moreover the identity of the bully can never be known because they hide behind fictitious or fake account names. The acts of cyberbullying take place on social networking sites, instant messaging software, discussion forums, games online, video sharing sites, blogs and emails. With the continuous advancement in technology new cases of cyberbullying keep emerging each day.

According to United Nations International Children's Emergency Fund (UNICEF), cyberbullying is defined as "bullying carried out through digital technologies such as social networking sites, instant messaging, gaming systems and cell phones where there is repeated aggressive behavior with the intention of frightening, embarrassing or targeting another person."¹

FORMS OF CYBERBULLYING

Cyberbullying takes many forms and each one of them has certain legal and psychological implications. The first form is called **online harassment**. It consists of sending repeated threatening rude or harassing messages via email instant message or social network sites. This form usually causes emotional distress and fear.

Another very common type of cyberbullying is called **cyber stalking**. Here, offenders continually harass watch or communicate with the victims using electronic means. Cyber stalking is highly dangerous since it can escalate to physical intimidation. Women are at great risk of becoming victims of cyber stalking.

The next one is known as **impersonation**. In cases of this type of cyberbullying, offenders either create fake online profiles or gain unauthorized access to someone's account to post false information. **Outing or doxing** involves sharing private or confidential information such as personal addresses, phone numbers, bank statements or sexually explicit pictures without the individual's permission.

There is another growing trend of non-consensual sharing of intimate images known as **revenge pornography**. The unauthorized dissemination of such images can lead to serious psychological impact on the individual causing both emotional trauma and damage to their reputation.

Another type of harassment that can be observed on social media is **trolling**. It must be noted that although the criticism and disagreements are part of the freedom of expression, persistent insulting remarks about an individual based on his/her appearance, religion, sex, race or personal characteristics can be considered cyberbullying when the intent to intimidate or humiliate is present. Modern technologies have led to deep fake cyberbullying where AI is

¹ UNICEF, *What Is Cyberbullying?* (last visited July 27, 2026),

employed to alter photos, videos and voice recordings of individuals involved in certain actions they had never undertaken.

Cyberbullying Trend in India

India's digital revolution has ensured that access to the internet has become easier in both urban and rural areas of the country. The proliferation of affordable smart phones along with cheap mobile data services has made sure that millions of people are involved in using social media and other digital communications. While this revolution has been helpful in ensuring the economic growth of the country, it has also paved way for cyberbullying.

The most vulnerable segments of the society remain children and teenagers. Social networking sites have resulted in harassment, peer pressure, alienation and even embarrassment of young internet users. Educational institutions in India have found themselves reporting incidents of abusive chat groups, circulation of manipulated photos, creation of fake social media profiles and spreading of rumors among students.

Women in India have also become victims of such practices. Women lawyers, female journalists, women politicians and female students have faced explicit sexual messages, threats of violence, character assassination and unconsented circulation of their personal pictures on the internet.

Both professionals and public figures are equally subjected to organized attacks on the internet. The use of anonymous profiles can result in defamation, manipulated media content and harassment in an attempt to tarnish their reputation or prevent them from engaging publicly.

The fast-paced development of artificial intelligence has only added to the problem. As a result, it is now possible for offenders to create realistic yet falsified digital content using AI images, voice cloning and deep fake technology, making it hard to identify the offenders. Therefore, traditional measures of legal recourse prove to be ineffective when tackling such high-tech crimes. The growing frequency of cyberbullying clearly shows that technological progress needs to be paired with legal security and law enforcement methods.

Effects of Cyberbullying

Cyberbullying causes effects which go beyond mere emotional pain. According to psychological researches, victims of cyberbullying regularly suffer from stress, depression,

anxiety, sleeplessness, isolation and low self-esteem. Minor victims commonly face decreased academic performance, refusal to go to school and socialization problems.

As opposed to the traditional form of bullying, cyberbullying is an unceasing phenomenon. Damaging messages and slander can be accessed 24/7 at any time without the possibility of victims resting from attacks. Due to viral nature of Internet communications, victims are exposed to the humiliation of an unlimited audience.

The professional effect of cyberbullying can also be quite severe. Defamatory messages, altered photographs and other slanders posted on the Internet may harm the professional life of the victim negatively impacting his/her employment, education and professional reputation. Even after the removal of the initial information, digital traces can still be available through screenshots, archives or reposting of the information.

Constitutionally, cyberbullying poses a danger for the constitutional rights of individuals as guaranteed by the Constitution of India. The right to privacy, dignity, reputation, equality and personal liberty as provided for by articles 14, 19 and 21 is constantly being violated by cyberbullying.

Legal Framework against Cyber Bullying in India

There is no statutory law against cyber bullying in India at present. Individuals suffering from cyber bullying are protected by a number of constitutional laws, the Information Technology Act of 2000, the Bharatiya Nyaya Sanhita, 2023 (BNS) along with some other allied laws. Though all these laws take care of various kinds of offences that can be considered as parts of cyber bullying, they are disjointed and fail to fully address the aspects of cybercrimes.

Lack of a statutory definition of cyber bullying makes it difficult for the victim, the investigating agency, and the court of law to determine whether it is a crime. Online harassment, online impersonation, publishing private intimate pictures of the individual on the Internet, cyber stalking and criminal intimidation are few of the offences that come under cyber bullying but are prosecuted differently on the basis of their individual nature.

Constitutional Protection against Cyberbullying

Despite the lack of specific mention of cyberbullying in the Constitution of India, there are some Fundamental Rights which indirectly provide constitutional protection against the same.

According to Article 14, citizens have a right to equality before law and equal protection of laws. Any form of cyberbullying targeting women, children or members of marginalized communities goes against the constitutional guarantee of equality, since these groups become unable to exercise their fundamental right to participate freely on the Internet.²

According to Article 19(1) (a), there is a right to freedom of speech and expression. But this right is subject to reasonable restrictions mentioned in Article 19(2) which are based on considerations of public order, decency, morality, defamation and sovereignty and integrity of India.³ Thus, abusive language on the Internet in the form of criminal intimidation, obscenity or defamation is not protected by the Constitution.

According to Article 21, there is a right to life and personal liberty. The Supreme Court through its decisions has interpreted the Article 21 to mean right to privacy, reputation, dignity and mental well-being. Therefore, any form of cyberbullying which interferes with these rights of individuals is unconstitutional.⁴ Thus, constitutional law provides the basis for legislative measures protecting individuals against cyberbullying.

Information Technology Act, 2000

The Information Technology Act, 2000 was the first legislation in India that comprehensively addresses e-governance and cyber-crimes. While the Information Technology Act, 2000 does not explicitly cover cyberbullying, many provisions under the Act are often cited when there is a case of online abuse that amounts to a criminal offense.

Identity Theft and Impersonation

Section 66C makes it a crime to commit identity theft using the electronic signature, password, or any other unique identification feature of another person.⁵ Cyberbullies generally make false identities or hack into victims' electronic signatures or passwords to send out defamatory information or tarnish reputations.

² INDIA CONST. art. 14.

³ INDIA CONST. art.14

⁴ INDIA CONST. art. 19(1) (a), art. 19(2).

⁵ Information Technology Act, No. 21 of 2000, § 66C, India Code (2000).

Section 66D makes it a crime to cheat or deceive through personation using computer resources or communication devices.⁶ Any offenders who deceive others using their identity through the internet can be charged under this section.

Violation of Privacy

Section 66E provides punishment for intentionally taking, publishing, or transmitting any electronic picture of private parts of an individual.⁷ This section will apply to any instance of cyberbullying where the victim is being harassed through circulation of intimate photographs or videos.

Publication of Obscene Material

Sections 67, 67A and 67B make it a crime to publish, transmit, or distribute obscene, sexually explicit and child sexual abuse material in electronic form.⁸ These sections will apply to any instance of cyberbullying where obscene material is involved.

Liability of Intermediaries

Section 79 gives conditional protection from any liability to intermediaries, including social media platforms, if they take due diligence and fulfill the statutory requirements.⁹ Moreover, the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021 require intermediaries to provide mechanisms to address grievances and take down illegal content based on legal orders from competent authorities.¹⁰

Shreya Singhal v. Union of India

Another important landmark case in the Indian cyber laws is *Shreya Singhal v. Union of India*, wherein the Supreme Court ruled that Section 66A of the IT Act was unconstitutional.¹¹

Section 66A penalized the sending of offensive electronic messages through communication services. The Supreme Court however found that the provision in question was too vague,

⁶ *Id.* § 66D.

⁷ *Id.* § 66E.

⁸ *Id.* §§ 67–67B.

⁹ *Id.* § 79.

¹⁰ Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021, G.S.R. 139(E), RR. 3–4 (India).

¹¹ *Shreya Singhal v. Union of India*, (2015) 5 S.C.C. 1.

broad and arbitrarily applied to be compliant with the fundamental right of freedom of speech as guaranteed by Article 19(1) (a) of the Constitution of India.

Despite making the exercise of free speech online easier the case raised questions about the lack of legislation to deal with cyberbullying since the said section was also used in some cases of online harassment. It should be noted that according to the Supreme Court, there were enough existing statutes to prosecute criminal intimidation defamation obscenity and incitement cases.

Bharatiya Nyaya Sanhita, 2023

Following the repeal of the Indian Penal Code, 1860, many offences relevant to cyberbullying are now governed by the Bharatiya Nyaya Sanhita, 2023.

While cyberbullying is not criminalized under the BNS, various provisions will apply based on the nature of such an act. An online threat can be an instance of criminal intimidation. Publication of any defamatory statement that may affect one's reputation constitutes defamation. Distribution of obscene content via electronic media is punishable under the BNS and the Information Technology Act.

Likewise, acts like sexual harassment, insult to the modesty of women, criminal intimidation, extortion and the dissemination of false information via electronic media can be charged under the relevant provisions of the BNS as well as specialized cyber laws.

Hence, the BNS works in tandem with the Information Technology Act in covering the substantive criminal offenses conducted using digital technology.

Approach of Courts with Respect to Dignity and Privacy Online

There is an established understanding by Indian courts that privacy and dignity form part of the constitutional liberty.

In *Justice K.S. Puttaswamy (Retd.) v. Union of India*, a nine-judge Bench of the Supreme Court has affirmed in unison the right to privacy as a fundamental right under Article 21 of the Constitution.¹² The decision has recognised informational privacy and has highlighted the fact

¹² Justice K.S. Puttaswamy (Retd.) v. Union of India, (2017) 10 S.C.C. 1.

that people have genuine interests in the control and dissemination of their personal information.

The precedents laid down in the case of Puttaswamy have great significance in relation to cyberbullying since the publishing of the private communication, pictures, and personal data and intimate material without consent violates informational privacy. Equally, Indian courts have time and again noted that reputation is one of the important facets of human dignity under Article 21 of the Constitution.

Challenges in Dealing with Cyberbullying

Although there are numerous legal provisions available some practical challenges still persist that prevent effective implementation.

The first one is that there is no clear statutory definition of cyberbullying. Due to the lack of legislative definition law enforcement organizations cannot identify appropriate provisions for diverse types of cyberbullying.

Furthermore, criminals often use anonymity, virtual private networks, encrypted messaging apps and foreign websites, which makes their identification complicated. International cooperation is needed for cross-border investigations and it takes time and a lot of procedure.

Additionally technologies develop faster than the laws do. Currently artificial intelligence allows the creation of extremely realistic deep fake images, videos and voice recordings which can cause serious damage to the person's reputation. Current legislation was passed before the emergence of such technologies and does not cover all the aspects of these new problems.

Under-reporting is another issue. Victims often do not report cyberbullying because they are afraid of the social stigma, embarrassment, long-term litigation process, or even unawareness about existing legal mechanisms.

Finally, many investigating authorities are still lacking qualified personnel and technological equipment to investigate cybercrimes.

Recommendations

India needs to pass a specific anti-cyberbullying legislation that will define cyberbullying, specify types of cyberbullying, and provide proportional punishments and special procedures for conducting investigations and victim support.

There is a need for educational institutions to develop digital literacy programmes that will teach students about proper online behavior, privacy, ethics and possible legal consequences of engaging in such misconduct online.

Social media companies must improve their content moderation tools by integrating artificial intelligence into their systems to enable fast removal of all the abusive posts while ensuring free speech online.

Training and education of law enforcement officials is critical in terms of improving the cyber-forensics, collecting digital evidence, analyzing block chains, using artificial intelligence in investigations and conducting international cybercrime investigations.

Lastly, the Government should engage more in awareness campaigns that will encourage victims to report cyberbullying without facing any stigma from their community. Reporting mechanisms, counselling and victim support programs must be in place along with criminal enforcement.

Conclusion

Cyberbullying has become a significant challenge in India's rapidly expanding digital landscape, affecting individuals' privacy, dignity and mental well-being. Although the Constitution, the Information Technology Act, 2000 and the Bharatiya Nyaya Sanhita, 2023 provide legal remedies against various forms of online harassment India still lacks a dedicated law specifically addressing cyberbullying. Strengthening the legal framework, improving digital literacy, enhancing law enforcement capabilities and ensuring responsible conduct by social media platforms are essential to effectively combat cyberbullying. A balanced approach that protects both individual rights and freedom of expression is necessary to create a safer and more secure digital environment.