
CYBERBULLYING AGAINST WOMEN AND CHILDREN IN INDIA: ASSESSING THE ADEQUACY OF THE EXISTING LEGAL FRAMEWORK

Dr. Dinesh Kumar SinghAssistant Professor, School of Law, Bennett University, India
dinesh.singh@bennett.edu.in**ABSTRACT**

The advent of social media, SMS messaging, online gaming and digitally mediated communication has changed lending structure of bullying from localised interactions to ubiquitous forms of violence. The methods of violence particularly affect women and children – victims of cyberstalking, sexual harassment, threats, impersonation, distribution of intimate photographs without consent, defamation, making inappropriate sexual images and public humiliations. Legal framework related to the cyberbullying is not well-defined in India. Acts of cyberbullying can be addressed through the Bhartiya Nyaya Sanhita, 2023, the Information Technology Act, 2000, the Protection of Children from Sexual Offences Act, 2012, and the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021 as amended.

Using doctrinal, analytical and evaluative methods, this paper assesses if the existing legal framework protects women and children. It investigates acts of sexual harassment, voyeurism, stalking, criminal intimidation, defamation, identity theft, invasion of privacy, dissemination of sexual material, and child sexual exploitation. It will also assess online mediator liability and constitutional aspects of Shreya Singhal v. Union of India. Child protection issues refer to Just Rights for Children Alliance v. S. Harish and Nipun Saxena v. Union of India is related to the dissemination of the information about sexual crime victims.

Results of the analysis are that law in India is relatively strong concerning acts of cyberbullying with sexual abuse, intimate images, stalking, threats or child sexual abuse materials. Besides, the protection is much weaker in the context of continual non-sexual abuse, trolling, doxxing, social exclusion, anonymous pile-on and bullying. The main issue is not the absence of regulations but fragmented, offence-specific, and elaborate nature of the law. Recommendations that arise from the paper are the narrowed down, harm-based definition of cyberbullying, different actions and penalties, inclusive regulation, the establishment of child-sensitive institutions, the preservation of electronic evidence and additional liability of platforms.

Keywords: cyberbullying, online violence, women, children, cyberstalking, image-based sexual abuse, intermediary liability, digital safety

1. INTRODUCTION

Digital communication affects the way and the consequences of interpersonal aggression. Traditional bullying occurs in a clear physical environment, such as a school or workplace. In contrast, cyberbullying follows the victim wherever there is an internet-enabled device. It can be shared quickly, duplicated with no loss in quality, stored for a long time and seen by an audience much larger than the initial circle of the victim and the aggressor. As a result, an insulting message may disappear from a social media site, but will remain in screenshots, archives or private group chats. Thus, the impact of the harmful message is influenced by the original message as well as by the communication technologies used to share and promote it.

In cyberbullying literature, researchers point out specific features such as intentionality of harm, repeated attacks, power imbalance and the usage of technology. Nevertheless, the repetition of a cyberbullying act is different from traditional repetition, since one upload creates the possibility for others to share it multiple times without intervention of the “first” person who uploaded it. Therefore, there are different levels of information exposure thanks to the characteristics of online bullying. The distinctiveness of online bullying from traditional bullying is determined by permanence, anonymity, public visibility etc.

The aftermath of such incidents is more serious than just a moment of shame. Studies show that the victim of cyberbullying suffers from various mental disorders such as anxiety and depression, withdrawal from society and problems with learning (Hamm et al., 2015; John et al., 2018). However, it must not be concluded that all online quarrels produce the above-mentioned negative consequences. Nevertheless, this is the reason why serious cyberbullying must not be left without attention.

Women and children undergo their own but partly overlapping types of suffering. Abuse addressed to women often includes sexual or degrading elements. It could be either a threat of sexual violence or stalking and harassment (Backe et al., 2018; Watson, 2024). While children may be bullied in chats or video games, girls are

subject to the effects of gender-based and age discrimination. At the same, boys experience the same perpetration of violence but may also be sexually exploited.

There is no separate definition of cyberbullying in the Indian legal system. Depending on the case, the law applicable can be one of the laws defining stalking, sexual harassment, voyeurism, intimidation, defamation or identity theft. The main advantage here is that not every malicious or unpleasant communication is treated as a crime; however, various actions committed at different times to harm an individual may fall into several categories that may prevent bringing the perpetrator to justice.

The present study raises the question of whether or not the historical development of criminal law, cyber law, laws for the protection of children, and law concerning intermediaries provide satisfactory protection against cyberbullying of girls and women. It concludes that while the framework can be considered to provide ample protection in practice, it still remains somewhat fragmented in terms of its structure. It is most efficient when it comes to abusive sexual and image-based behaviour; is somewhat effective when it comes to threats, stalking, and impersonation; but is the least effective when it comes to cumulative non-sexual harassment, doxxing, and coordinated pile-ons or peer-to-peer cyberbullying.

2. RESEARCH OBJECTIVES AND METHODOLOGY

To illustrate its objectives, the study sets itself the following tasks: defining cyberbullying in contrast with similar forms of online behaviour, identifying applicable legal rules relating to cyberbullying of women and minors, evaluating principles of constitutional law and judicial practices regulating freedom of speech and harm of a victim, analysing existing gaps of different kinds, and suggesting reasonable recommendations for improvement.

The study is based on doctrinal and analytical methods. It uses primary sources such as Indian Constitution, Bharatiya Nyaya Sanhita 2023, Information Technology Act 2000, Protection of Children from Sexual Offences Act 2012, Juvenile Justice (Care and Protection of Children) Act 2015 and intermediary rules as of February 2026. In judicial aspect, the study refers to three prominent Supreme Court judgments, namely, *Shreya Singhal v. Union of India*, *Nipun Saxena v. Union of India*, *Just Rights for Children Alliance v. S. Harish*. The use of secondary sources is restricted to journal publications which are confirmed by DOI.

This study does not contain any original surveys, interviews, and statistics on prosecutions. The results are based on legal framework analysis rather than on including any statistics on efficiency of the activity of police stations, platforms and courts.

3. CONCEPTUALISING CYBERBULLYING

For a term to be regarded as legal, the definition used has to be clear enough so that it includes harmful behavior but does not transform normal disagreements into crime. This study defines cyberbullying as:

Deliberate and knowingly harmful behavior conducted through digital means that constitutes repeating, continuing or seriously threatening, intimidating, embarrassing, sexually harassing and troubling other people, thus causing or leading to some risk of violence or harm in physical, psychological, reputation, sexual or moral aspects.

This definition consists of necessary precautions. First of all, it should target certain behaviors and not only refer to unpopular speech acts. On the other hand, it is essential that a behavior to be qualified as cyberbullying is repeated or continued on several occasions, and thus for example, the act of uploading someone's private photo can be recognized as an instance of cyberbullying even if it involves only a single act of uploading the photo because the technology allows in many cases continuous sharing of the information. The definition of the term presupposes considerable damage or harm that is to be somehow evident.

Cyberbullying is closely related to other terms but does not fully overlap with them. Cyberstalking is characterized by continuous monitoring of or following the victim or equal contact. Online defamation refers to actions in which defamatory statements are made against someone's reputation. The notion of trolling covers disturbing but not necessarily follows continuous harassment of the victim. Doxing implies revealing someone's personal information or location details, usually so that the person becomes stressed or threatened. Image-based sexual abuse is associated with making, disturbing or threatening to distribute sexual or personal images without the consent of a victim.

The mentioned distinction is important because cyberbullying legislation based on the term of offensiveness is unconstitutional. Political criticism, satire and investigative journalism can often lead to people's distress, yet remain within the range of legally accepted conduct.

4. CONSTITUTIONAL FOUNDATIONS

According to the constitution, the state has to perform the task of protecting dignity and safety while ensuring freedom of expression. Article 14 of the constitution establishes equality of all human beings in front of the law and provides equal legal protection to all the citizens. The content of the Article 15 (3) indicates that the disadvantaged groups, such as women and children, may be granted special safeguards, which implies that the need to establish safeguards for these vulnerable groups is acknowledged in the laws. Article 21 implies that the rights to life, liberty and privacy are guaranteed to the citizens. Various activities, such as cyberstalking, sexual threats, non-consensual photography and unauthorized disclosure of private information interfere with the rights of the individual even without any physical contact.

On the other hand, the Article 19 (1) (a) grants freedom of expression. The restrictions should be in line with the provisions of Article 19 (2). Thus, it has to be noted that a legal reaction cannot state that expression has become illegal because it creates discomfort to someone. The internet is a space of disagreement, confrontation, and emotions, and the provision of a too broad cyberbullying prohibition can easily become a way of oppression of dissenters, students, journalists, or other victims speaking about misconduct.

The objective of the constitutions is not to decide what is more important – safety or freedom of expression. The challenge lies in creating well-defined rules. The mentioned types of actions mentioned above are different from expressions and unpopular opinions. In the end, the optimal position is achieved when one party of the conflict violates legally protected interests or desires to frighten and humiliate someone.

5. CYBERBULLYING UNDER THE BHARATIYA NYAYA SANHITA, 2023

The Bharatiya Nyaya Sanhita, 2023 does not create a general cyberbullying offence. Its provisions are nevertheless technologically adaptable because many offences depend upon the nature and intention of the conduct rather than the physical medium used.

5.1 Sexual harassment, voyeurism and stalking

Section 75 makes certain types of sexual harassment crimes that a man commits against a woman, such as the display of pornography without her permission and making sexual comments. Thus this section can refer to unwanted pornography messages, sexual remarks and some other instances of online harassment. Its implementation depends on the proof of the written crime occurring and cannot be based on any communication that is offensive in nature.

Section 77 refers to voyeurism. It implies looking at a woman or taking a photo of her while she is performing something privately and disseminating this photo. Importantly, this section clarifies that giving consent to get the photo is not sufficient to obtain the right to disseminate it.

Section 78 specifically mentions the surveillance of a woman using the Internet, email, and other means of electronic communication. It also includes contacting the victim despite her clear unwillingness to communicate, which proves that the section recognizes technology-based forms of stalker behavior, such as sending many messages, monitoring of the online activities of the victim, and trying to contact the victim through the computer.

Section 79 implies that saying or doing something that can insult a woman is a crime. Although it can be used in cases involving electronic communication, searching for a word “modesty” is a big problem for the section.

While these laws can protect people, it should be noted that they are all written from the perspective of the man committing the crime against the woman. It means that men and people of other genders can use only general acts or the IT Act in these cases, and gender-inclusive laws should be created.

5.2 Criminal intimidation and defamation

Section 351 defines criminal intimidation as making an unapproved use of the digital context broadly enough to include threats made via the latter. To establish criminal intimidation, the criminal act must involve threats that cause injury to the victims themselves, their image, or property and that are done with the aim of creating fear or impelling the victim into action. The section takes into account the means of anonymous communication or concealment of identity. Thus, it fits well for the use of anonymous threats of violence or sexual violence.

Section 356 comes into play when a person publishes defamatory information knowing that it will damage someone's reputation. Purportedly fabricated accusations, social network rumors, and impacted postings may come within the statute. It should be noted, however, that defamation is not a substitute for cyberbullying since the focus of the latter is on the reputation of the victim and does not necessarily involve the acts of communicating the threat to them, ostracizing them, spying on them, or humiliating them without damaging their reputation in a legal way.

5.3 Limits of the BNS framework

The BNS is effective in cases where cyberbullying includes a well-known criminal offence. The problem is defining where harm from cyberbullying starts to become cumulative. One abusive post by itself may not amount to intimidation, stalking or defamation, while a series of posts by various accounts all belonging to the same campaign can create a hostile atmosphere forcing a woman to take some action such as taking down her profile or quitting a job. In criminal law, wrongdoing of an individual defendant is usually analysed separately from other defendants.

6. INFORMATION TECHNOLOGY ACT, 2000 AND INTERMEDIARY REGULATION**6.1 Identity theft, personation and privacy**

The Information Technology Act provides for several offences related to different technological advancements. Section 66C of the Act makes every act of fraudulent or unauthorised usage of electronic signature, password, or other unique identification attributes a criminal act. This section may apply to situations when a person gets access to the account of the victim and misuses his/her identification particulars. However, the creation of a fake or parody account is not considered identity fraud unless the criteria given under the definition of unique identification attributes are fulfilled.

Section 66D covers cheating by impersonation through a communication device or the computer resource. It is important to note that in this section the term cheating has been defined as one of the prerequisites that has to be fulfilled as per the definition of the crime. Creation of a fake account with the only agenda of mocking a woman or a child may not imply committing of the crime since cheating has not been established in such a situation.

Section 66E of the Information Technology Act states that it is a crime to intentionally or knowingly capture, publish or transmit the private area of a person without his/her consent when there is a violation of privacy. Unlike several BNS provisions, this section does not make a gender-based distinction. In spite of the fact that the section offers adequate protection against violations of privacy, its scope is limited in regards to the definition of the private area as established by the law. Even if the humiliating photograph does not depict the area defined by the law, it may cause noticeable harm to the victim. In addition, Sections 67 and 67A deal with the issues of obscene and sexually explicit electronic materials, while section 67B deals with all type of cyber crimes involving children and punishes perpetrators for creating and distributing taboo materials via the Internet.

These parts of the Act are significant in relation to techno-geek sexual abuse (Henry & Powell, 2018). It is very important that law enforcement agencies do not treat cases of intimate image abuse simply as problems between individuals. Studies about police behaviour in relation to this type of abuse show that law enforcement officials have to be educated in this field and do not perform the work without paying proper attention to the issue.

6.2 Extraterritoriality and enforcement

Section 75 allows for the application of the IT Act to certain activities performed outside the territory of India, provided that the offence involves the use of a computer, computer system or computer network located in India. This is important since the platforms, servers and offenders may all be located in different jurisdictions. However, the statutory extraterritoriality does not imply practical enforcement. Finding an anonymous internet account may necessitate the involvement of a foreign intermediary, data preservation and compliance with cross-border evidence rules.

6.3 Intermediary safe harbour

Intermediaries are offered conditional immunity from their responsibilities for any information posted by third parties under Section 79 of the law. The safe harbor protection applies as long as the intermediary acts within the limitations prescribed and exercises due diligence. This law represents a significant policy decision in the sense that it would be impractical to hold Internet Platforms liable as the original publishers of every message posted by users, but at the same time, the immunity cannot be absolute if the intermediary gets sufficient information about the illegal nature of the content or if it actively participates in the unlawful act.

The ruling of the Supreme Court in the case of Shreya Singhal and Union of India is essential for achieving this balance, as the Court held section 66A of the IT Act unconstitutional due to its ambiguous wording, such as annoyance or offensiveness, which result in a wide prohibition. The judgment stresses the need to differentiate between discussion or advocacy and incitement and narrows the definition of "actual knowledge" for purposes of avoiding liability of intermediaries to such notifications of illegality in terms of laws instead of giving platforms discretion to decide whether the information is legal or illegal in every specific case.

However, the ruling of the Court does not imply that cyberbullying must remain unregulated. It shows that regulation cannot be based on the vague definitions. Any further legal provisions need to clearly state what conduct is prohibited, what is the necessary mental element and what harm seriousness level presumption exists. The Act confirms that section 66A was struck down on the 24th of March 2015.

6.4 Grievance redressal and the 2026 amendments

The intermediary regulations lay down a different pathway for effective remedy. Under the latest intermediary regulations, a grievance officer of an intermediary is supposed to acknowledge the grievance within a period of 24 hours and resolve it usually within a period of one week. Removal complaints are supposed to be resolved within a period of 36 hours. When it comes to the complaints pertaining to materials which may show private parts, which may show nude or sexual actions, including the use of false identity and deep fake images, the intermediary has to take reasonable and practicable actions within a period of 2 hours.

The intermediary regulations also say that unlawful information that falls under the concept of actual knowledge should be removed by the intermediaries in a period of 3 hours after receiving a proper court decision or proper government communication. The intermediaries are supposed to keep the removed information and other records about it for a period of 180 days, which is crucial because taking quick actions of removal without keeping records may lead to losing the evidence, which may identify or punish the offender. The provisions from 2026 regarding synthetic content are related to child abuse and exploitation, non-consensual content, malicious content, false information and some other cases of misleading content.

These time frames show a great improvement in providing justice to victims. Intimate pictures may become impossible to control if the company delays for several days before taking actions. But taking the pictures down does not mean providing justice, since it does not necessarily lead to bringing the offender to justice, as well as does not prevent the pictures from reappearing again, does not help the victim out financially or psychologically. Besides, the victim may have to file several complaints with many platforms, since the materials may appear in many places.

7. CHILD-SPECIFIC PROTECTION UNDER THE POCSO ACT

The Protection of Children against Sexual Offences Act, 2012, secures all persons below eighteen years of age with the same level of protection regardless of their gender. Section 11 of the Act defines child sexual harassment and indicates that sexual harassment shall consist of making sexual advances by following, watching and contacting through different forms of traditional and digital communication. The new definitions also include the threat of using a real or false electronic image or hate scandalous material or seducing a minor. Sections 13 to 15 deal with the exploitation of children by using them for pornographic purposes.

19 of the Act obliges anyone who knows something about real or planned sexual abuse of children to inform the Special Juvenile Police Unit or the police and child abuse reports must be made in language accessible for children to understand.

The case of Just Rights for Children Alliance v. S. Harish, 2024 INSC 716 shows that the Supreme Court of India considered section 15 of the above Act and section 67B of the IT Act. The Court rejected the narrow interpretation of liability of possessing, viewing and storing abusing materials and proposed the term that will reflect the essence of what happened to children. The Court came to the conclusion that calling these materials child sexual abuse and exploitation materials is also more precise because it reveals that the recorded images of abuse for children are called ordinary pornography.

It means that POCSO is good in the case where cyberbullying can contain elements of sexual abuse, grooming and fake sexual images. Nevertheless, POCSO does not give full protection against cyberbullying of children. If children mock the appearance of other children, their disability, language, academic success or social background, there is no sexual way of causing any damage to minor.

If both the victim and the offender in a case are children, the approach to criminalization should be more careful and considerate. The Juvenile Justice system is based on rehabilitation and the child-oriented approach. In case serious sexual coercion and exploitation happened, there should be legal intervention; however, the cases of the abuse that do not involve delinquency can be better solved with the help of counseling and restorative approaches.

8. JUDICIAL PROTECTION OF IDENTITY AND INSTITUTIONAL CHALLENGES

The issue of cyberbullying is entirely relevant to this case, as it encompasses the publication of a victim's details including name, picture, school, workplace, and family details. In the case of Nipun Saxena v. Union of India, (2019) 2 SCC 703, the Supreme Court ruled laws that relate to safeguarding the identity or name of victims of

sexual offences and stressing on the disclosure limitations that apply to print, electronic and social media must be respected, subject to specific exceptions. The ruling is very relevant because digitization can create an environment for secondary victimization even when the first crime is either ongoing or finished. Often the absence of name may not be enough when other information points at victims' identity.

Apart from this it should also be well known that effective enforcement hinges on electronic evidence. Though screenshots are possible to create, they often don't contain metadata, account IDs, connections and context of conversation. Therefore victims should try to preserve URLs, usernames, timestamps, original files, email headers, and platform complaint acknowledgments. Police and platforms should recognize and perform the necessary actions ASAP.

Anonymity complicates attribution. Indeed, a display name doesn't prove authorship, and it is possible for accounts to be hacked, automated, or jointly operate. That's why legal processes must differentiate between who the named person on the account is and who actually produced or sent the content. Data requests from different countries, as well as encryptions, and temporary accounts make the investigation more complex and lengthy.

Institutional fragmentation is another issue. A victim can appeal to local police, a cybercrime division, a platform grievance officer, a school administration, a Special Juvenile Police Units, or a child protection body, however, each of them will resolve only part of a problem.

9. ASSESSING THE ADEQUACY OF THE EXISTING FRAMEWORK

The sufficiency of Indian legislation depends on a number of factors.

To begin with, the protection from sexual and image-based cyberbullying is significantly good. The BNS law includes provisions regarding sexual harassment, voyeurism, and stalking. The IT Act refers to violations of privacy and pornographic material. The POCSO Act prohibits electronic sexual abuse of minors. The intermediary guidelines allow for quick removal of sexually explicit, intimate, or altered content. The second step in terms of violence is that the protection from threats, stalking, and impersonation is very moderate depending on the situation. Criminal intimidation can help in the case of serious anonymous threats, and the BNS law states explicitly that it includes electronic surveillance of women. Identity fraud and impersonation provisions can target the abuser himself. However, there are some gaps that arise when fake profiles are created for humiliation. Third, the system does not have a strong approach to non-sexual humiliating violence such as trolling, doxxing, exclusion, and ridicule since none of the acts can qualify as an offense. The law system is targeted at specific offender possible acts while online violence could be generated by many contributors. It is important to point out that such a lack of the overall effects of violence presents a serious drawback of the system. Other weaknesses of the legal framework are the lack of the protection for different groups in case of the BNS crimes against the background of gender-based violence, while some crimes in the statute refer to men also. The IT Act is gender-neutral stating violation of the law regarding high-technology crimes but not mentioning harassment in general. At the same time, the POCSO law is strictly gender-neutral referring only to the sexual offences within the act. This shows that there is protection, but it varies. The legal mechanism is fundamentally oriented on criminal cases which is not enough for victims who may not want to institute the criminal case but just ask for the restraining order or removal of false information about them. Unfortunately, the criminal procedure may take much time. As it could be seen from the research conducted, the need for differentiated treatment of the law can be proved. The first step here is the meta-analysis of cyberbullying showing that it has some impact on people both mentally and socially but may manifest itself differently (Kowalski et al., 2014). Furthermore, gender differences cannot be reduced to the fact that only one gender could be the perpetrator of the crime. Age and social context also matter.

In summary, the legislative framework is partially effective as it possesses important offenses against a number of crimes but still does not provide victims with harm-focused practice of protection.

10. RECOMMENDATIONS

10.1 A narrow statutory definition

India should adopt a clear definition of cyberbullying, either through targeted legislation or a carefully framed amendment. The definition should require:

1. conduct directed at an identifiable person or limited group;
2. use of an electronic or digital communication system;
3. repetition, persistence, coordination or a serious single act capable of continuing dissemination;

4. intention, knowledge or recklessness concerning a substantial risk of harm; and
5. threatened or actual harm to safety, sexual autonomy, privacy, dignity, reputation or meaningful participation.

The law should expressly exclude good-faith journalism, academic work, lawful protest, reporting of misconduct, satire, artistic expression and criticism unless the conduct independently constitutes an offence. "Annoyance," "inconvenience" and undefined offensiveness must not become grounds of criminal liability.

10.2 Graded remedies

Not all cyberbullying should attract imprisonment. A graded framework could provide platform warnings, blocking and removal for lower-level conduct; civil protection or no-contact orders for persistent targeting; compensation and correction orders for demonstrated injury; and criminal liability for serious threats, coercion, sexual exploitation, doxxing creating a safety risk, repeated targeted harassment and unlawful intimate-image dissemination.

A narrowly framed protection order could restrain further digital contact and require removal without compelling the victim to establish every element of a criminal offence. Breach of the order could then attract proportionate consequences.

10.3 Child-sensitive institutional measures

Schools and educational institutions should maintain written cyberbullying policies applicable to institution-related digital groups and online learning systems. Policies should establish confidential reporting, evidence preservation, counselling, parental engagement and protection against retaliation. Where both parties are children and no serious sexual or violent offence is involved, restorative and rehabilitative measures should normally precede criminal intervention.

Children should be able to report abuse without navigating complex platform terms or legal categories. Interfaces should use age-appropriate language, and complaints involving a child should receive trained human review.

10.4 Gender-inclusive protection

The law should preserve specific recognition of gender-based cyberviolence while creating supplemental gender-neutral remedies. A residual offence or civil order should protect any person from persistent digital stalking, threats or harassment, without weakening the special protection available to women and children.

10.5 Platform accountability and evidence

Platforms should be required to preserve evidentiary copies and associated metadata before disabling reported content. Repeat-upload prevention should be used for adjudicated intimate imagery and child sexual exploitation material, subject to security and privacy safeguards. Transparency reports should identify complaint categories, response times, outcomes, appeals and repeat-offender measures without exposing victims.

Victims should receive a reasoned acknowledgement explaining whether content was removed, preserved or referred for further review. Where removal is refused, an accessible appeal should be available. Platform processes should also support Indian languages and recognise coordinated conduct across accounts.

10.6 Integrated victim assistance

A single-window digital complaint system should connect platform removal, evidence preservation, police referral, child-protection services, legal assistance and psychological support. The complainant should not be required to file substantially identical accounts with multiple authorities. Specialised cybercrime personnel should receive regular training in intimate-image abuse, child-sensitive interviewing, electronic attribution and preservation of cloud-based evidence.

11. CONCLUSION

It is inaccurate to claim that Indian law is powerless against cyberbullying. The BNS, IT Act, POCSO Act and intermediary rules have put in place an effective legal structure for dealing with issues of harassment, threats, sexual harassment, abuse of private images, identity scams and causing harm to children in digital space. There has been considerable progress in terms of ensuring fast resolution of platform complaints and acceptance of fake and artificial content.

However, the negative side of the present legal framework lies in the fact there is no proper system for the identification of cumulative digital damage. In situations involving continuous humiliation, group harassment, doxxing, mobbing of anonymous individuals, and non-sexual bullying of minors the existing legislation may

fail to address the situation where one or another act is considered to be non-criminal under law. The problem of fragmentation of procedures, destroyed evidences and the need to choose the right place for lodging a complaint prevent using the advantages of a well-developed legal framework.

The solution to the problem is not introduction of some unclear legislative body similar to the abolished section 66A. Regulation has to be based on the specifics of a behavior as well as the harm caused by it to the victims. The definition of cyberbullying has to be narrow; the variety of legal measures used in this process have to be adequate; the measures have to be created based on the principles of gender equality and child-friendliness; evidences and procedures have to be reliable and clear.

PRIMARY LEGAL AUTHORITIES

Just Rights for Children Alliance & Another v. S. Harish & Others, 2024 INSC 716.

Nipun Saxena & Another v. Union of India & Others, (2019) 2 SCC 703.

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

Bharatiya Nyaya Sanhita, 2023, Act No. 45 of 2023.

Constitution of India.

Information Technology Act, 2000, Act No. 21 of 2000.

Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021, as officially updated in February 2026.

Juvenile Justice (Care and Protection of Children) Act, 2015, Act No. 2 of 2016.

Protection of Children from Sexual Offences Act, 2012, Act No. 32 of 2012.

REFERENCES

Backe, E. L., Lilleston, P., & McCleary-Sills, J. (2018). Networked individuals, gendered violence: A literature review of cyberviolence. *Violence and Gender*, 5(3), 135–146. <https://doi.org/10.1089/vio.2017.0056>

Barlett, C. P., & Coyne, S. M. (2014). A meta-analysis of sex differences in cyber-bullying behavior: The moderating role of age. *Aggressive Behavior*, 40(5), 474–488. <https://doi.org/10.1002/ab.21555>

Hamm, M. P., Newton, A. S., Chisholm, A., Shulhan, J., Milne, A., Sundar, P., Ennis, H., Scott, S. D., & Hartling, L. (2015). Prevalence and effect of cyberbullying on children and young people: A scoping review of social media studies. *JAMA Pediatrics*, 169(8), 770–777. <https://doi.org/10.1001/jamapediatrics.2015.0944>

Henry, N., Flynn, A., & Powell, A. (2018). Policing image-based sexual abuse: Stakeholder perspectives. *Police Practice and Research*, 19(6), 565–581. <https://doi.org/10.1080/15614263.2018.1507892>

Henry, N., & Powell, A. (2018). Technology-facilitated sexual violence: A literature review of empirical research. *Trauma, Violence, & Abuse*, 19(2), 195–208. <https://doi.org/10.1177/1524838016650189>

John, A., Glendenning, A. C., Marchant, A., Montgomery, P., Stewart, A., Wood, S., Lloyd, K., & Hawton, K. (2018). Self-harm, suicidal behaviours, and cyberbullying in children and young people: Systematic review. *Journal of Medical Internet Research*, 20(4), e129. <https://doi.org/10.2196/jmir.9044>

Kowalski, R. M., Giumetti, G. W., Schroeder, A. N., & Lattanner, M. R. (2014). Bullying in the digital age: A critical review and meta-analysis of cyberbullying research among youth. *Psychological Bulletin*, 140(4), 1073–1137. <https://doi.org/10.1037/a0035618>

McGlynn, C., & Rackley, E. (2017). Image-based sexual abuse. *Oxford Journal of Legal Studies*, 37(3), 534–561. <https://doi.org/10.1093/ojls/gqw033>

Slonje, R., Smith, P. K., & Frisén, A. (2013). The nature of cyberbullying, and strategies for prevention. *Computers in Human Behavior*, 29(1), 26–32. <https://doi.org/10.1016/j.chb.2012.05.024>

Tokunaga, R. S. (2010). Following you home from school: A critical review and synthesis of research on cyberbullying victimization. *Computers in Human Behavior*, 26(3), 277–287. <https://doi.org/10.1016/j.chb.2009.11.014>

Watson, S. (2024). Online abuse of women: An interdisciplinary scoping review of the literature. *Feminist Media Studies*, 24(1), 51–69. <https://doi.org/10.1080/14680777.2023.2181136>