

Cyberbullying and Online Harassment: Legal Remedies Available in India

EDGAR RAJDAYAL ALLAN¹ & Dr. Manindra Singh Hanspal²

¹ LL.M. Student, Presidency University, Bengaluru.

² Assistant Professor, School of Law, Presidency University, Bengaluru.

Article info

ABSTRACT

Article history:

Received Aug 12, 2026

Accepted Aug 25, 2026

Published Aug 31, 2026

Keywords:

Cyberbullying

Online Harassment

Information Technology

Bharatiya Nyaya Sanhita

Legal Remedies India

Cyberbullying and internet trolling have become one of the major social and legal issues in present India as it is becoming précised for individuals of all ages and classes more often than not. Digital platforms have democratized communication and fostered unprecedented connectivity, but at the same time, they now constitute never-before-seen channels for harassment, defamation, intimidation, and orchestrated abuse campaigns. This paper analyzes the plethora of legal options in India that are available to deal with cyberbullying and online harassment, covering criminal provisions under the Information Technology Act, 2000, the Indian Penal Code, 1860 and the recent Bharatiya Nyaya Sanhita, 2023. By analysing statutory remedies, judicial precedents, institutional mechanisms and regulatory frameworks in detail, the paper argues India has a relatively robust legal architecture for ameliorating digital harassment but that there is considerable implementation deficit with large institutional capacity gaps hampering practical application. Identify important gaps between legislative intent and enforcement and analyze the barriers to efficacious implementation including inadequate law enforcement training, jurisdictional challenges, platform non-cooperation, victim safety concerns and proof problems. The analysis goes on to recommend specific legislative amendments institutional capacity building, victim-sensitive procedural reforms, and platform accountability mechanisms.

This work is licensed under a [Creative Commons Attribution-NonCommercial 4.0 International License](https://creativecommons.org/licenses/by-nc/4.0/).



Corresponding Author:

EDGAR RAJDAYAL ALLAN

Email: dr.edgar.allan@gmail.com

1. Introduction:

The explosion of digital technologies and social media platforms has used radically reconfigured Since 2015, countries from all over the world have experienced an unfolding integrating how people connect, communicate, share information, and create communities within and beyond any given physical location. As of 2023, India's internet penetration reached an estimated size of over 890 million (telecommunications data from Gov. of India website, 2023), setting up the conditions for unprecedented opportunity and harm to coexist in this digital landscape.

Conducted over digital (rather than physical or written) means and with a steadily escalating focus on specific individuals, cyberbullying or online harassment, as defined by scholars and policy influencers alike is one of the largest dimensions of this modern fact (Shariff 2008). Cyberbullying in the Indian setting is far from your desi trolling; it carries with its weight organized harassment initiatives, nonconsensual intimate image sharing; targeted abuse on caste, religion, gender and sexuality lines; systematic intimidation to shut down voices from those already marginalized.

1.1 Legislative Evolution and Constitutional Context

In India, the emergence of cyberbullying has not received a significant legal response in a single stride but instead evolved gradually through first legislative activity, and then judicial clarification. The Indian law (Parliament of India 2000), before promulgation of the Information Technology Act, 2000, had not yet incorporated specific statutory provisions regarding digital harassment; and mainly used generic criminal or civil remedies designed to handle offline activities in the twentieth century. The Information Technology Act, 2000 was the first institutional effort to establish a specific statutory regime for addressing cyber offenses containing provisions on issues related to electronic communications, computer systems and technology mediated harm (Parliament of India 2000). This is because, the landmark judgment of *Shreya Singhal v. Union of India* held Section 66A of the IT Act to be unconstitutionally vague and vaguely overbroad (*Shreya Singhal v. Union of India* 2015), thereby creating a significant statutory lacuna with respect to protection against offensive online speech while also causing great deal of confusion in regard to which digital expressions can even properly attract criminalization.

1.2 Contemporary Legal Framework and Recent Amendments

Newer laws, especially the *Bharatiya Nyaya Sanhita*, 2023 (Parliament of India 2023), have sought to fill this gap in interpretation with provisions criminalizing online harassment and language on digital vectors of harm explicitly. The exponential rise in the complaints of cybercrime, including those with respect to women and children was documented in 2020. For instance, see a report by the National Commission for Women based on CPI data, which has been explained as requiring an immediate need for statutory reform. The *Bharatiya Nyaya Sanhita* is the biggest criminal law codification in post-Independent India with a technology specific chapter developed through various consultations conducted with law enforcement, civil society, and digital rights advocates.

2. Legal Framework: Statutory Provisions and Their Application

2.1 Information Technology Act, 2000: Overview and Critical Provisions

The main statutory provisions against cyberbullying and online harassment in India stems from three different yet largely overlapping regulatory regimes: the Information Technology Act, 2000 (Parliament of India 2000); Indian Penal Code, 1860 (Parliament of India 1860) and the very recently enacted *Bharatiya Nyaya Sanhita*, 2023 (Parliament of India 2023). To conceptualize cyberbullying as a legal issue requires an analysis of the mechanisms by which these self-contained statutory schemes coalesce, yield reciprocal remedies, and in some cases create overlapping jurisdictions that stimulate doctrinal ambiguity.

Section 67: Obscene Material in Electronic Form

The Information Technology Act, 2000 encompassed Section 67 on the publishing of obscene material in electronic form accompanied with criminal penalties (Parliament of India 2000). This defines a class of offenses as publication that are committed by meaningfully transmitting obscene material, through the channels computer to computer, or

electronic means with knowledge such material is obscene, making clear transmission over fiber optic cable, satellite phone constitutes non-trivial distribution. The Act additionally establishes in Section 67A significantly increased punishment where children are multiplied or transmitted through electronic mechanisms to reflect legislative acknowledgement of special vulnerability (Parliament of India 2000) amongst child victims. While these provisions do not reflect a comprehensive definition of cyberbullying, they provide valuable legal instruments to combat the harassment by way of non-consensual intimate imagery and sexually graphic content, both of which are commonly recurring facets of online abuse targeting primarily women and sexual minorities (*E v. State, Delhi* 2012).

In *E v. State Delhi*, the Delhi High Court held that even via social media, the circulation of non-consensual intimate imagery constitutes harassment under Section 67 as well as violation of privacy rights thereby allowing for the concurrent application of civil and criminal remedies. The Supreme Court later strengthened this view by ruling in *Puttaswamy v. Union of India* to the effect that sending intimate images without consent violates the right to privacy, not only as a matter of criminal law but also infringing constitutional immunity (*K.S. Puttaswamy v. Union of India* 2017).

Section 66D: Online Cheating and Fraud-Based Harassment

Section 66D of the Information Technology Act relates to Cheating by personation using computer resource, which now brings the liability for criminal harassment through impersonation, identity fraud and misrepresentation on digital platforms (in more sophisticated terms, resulting in anonymity), allowing a potential situation where perpetrators taking on a false identity can subject victims to abuse (Parliament of India 2000). As per the guidelines from Ministry of Electronics and Information Technology, Government of India in 2019 on Cyber Crime, impersonation is the most rising category (Ministry of Electronics 2019). So clearly implementing Section 66D to send a strong stream against it become crucial important.

Section 66A and the Shreya Singhal Judgment

However, the most consequential provision in the original Information Technology Act was Section 66A, which criminalized transmission of grossly offensive messages and information knowing that such transmission would cause inconvenience, danger, or annoyance to recipients. The provision's extraordinary breadth criminalizing speech deemed "grossly offensive" without clear definitional parameters or contextual analysis prompted widespread constitutional criticism and numerous litigation challenges on fundamental rights grounds (*Shreya Singhal v. Union of India* 2015). This doctrinal tension culminated in the Supreme Court's landmark judgment where Justice Nariman and Justice Chelameswar invalidated Section 66A as unconstitutionally vague and overbroad, violating fundamental rights to free speech under Article 19(1)(a) of the Indian Constitution while simultaneously failing to meet narrow tailoring requirements under Article 19(2) permitting reasonable restrictions on expression (*Shreya Singhal v. Union of India* 2015).

Post-Shreya Singhal Legislative Gap and Doctrinal Challenges

Criminalising speech needs more precision, it needs a contextual value judgement and recognition that unjust speech may not even be an exception to free expression which is protected, the Supreme Court in *Shreya Singhal v. Union of India* had reasoned out constitutional jurisprudential limits. The court further held that causing mere offense or annoyance to recipients is not a valid ground for prohibiting speech in any democracy dedicated to free expression (*Shreya Singhal v. Union of India* 2015). This ruling carved out a very wide shield around online speech, but it left an

absence in the law. Direct statutory criminalization of online harassment in the form of non-explicit offensive material did not exist and necessitated relying on general provisions within the Indian Penal Code that were first designed without consideration for digital communications.

2.2 Indian Penal Code, 1860: Traditional Provisions Applied to Digital Harassment

The Indian Penal Code, enacted in 1860 (Parliament of India 1860), contains multiple provisions applicable to cyberbullying and online harassment, though their extension to digital conduct represents a post-hoc application rather than original legislative intent.

Section 499-500: Defamation and Criminal Liability

Defamation, legally defined in Section 499 as making or publishing any imputation concerning any person with intent to cause harm or knowledge, that such imputation will prove to be harmful and damaging to the reputation of that person (Parliament of India 1860). This applies to online defamation as well spreading of false and defamatory statements by way of social media platform and electronic network falls under the purview of the provision, as the courts have held that publishing in physical form will also be treated as "publication" for purpose of liability under law of defamation (Subramaniam Swamy v. Union of India 2016). The extensive judgment of Justice Madan Lokur in Subramaniam Swamy v. Union of India came to a definitive conclusion on what actionable publication is vis-à-vis the internet: that online publications (via websites and social media) are clearly included within this definition, thus expanding the basic principles defined for defamatory actions during print times towards this modern era (Subramaniam Swamy v. Union of India 2016).

The high court in the judgment of Rajendra Prasad Yadav v. State of Bihar applied a more rigorous doctrine of defamation to digital defamation, which relied on whether the statement was false, who it identified, publication and damage (Rajendra Prasad Yadav v. State of Bihar 2017). Part 2 protects against the crime of defamation or publishing untrue remarks as a criminal offence, with liability increased to two years imprisonment or fines, as well as both, but many prosecutors go for civil remedies permitting larger damages.

Section 504-507: Criminal Intimidation and Anonymous Harassment

Section 504 speaks of criminal intimidation as follows, if the offender threatens that he will injure or cause harm to the person, reputation or property of any person with intent to cause alarm and apprehension in such a way as mentioned above (Parliament of India 1860). This provision has been used against online abuse, ensuring technology does not absolve the threat from its criminality (Gopal v. State of Karnataka 2012). Justice Akshay Kumara Goel's reasoning in Gopal v. State of Karnataka established that social media campaigns targeting individuals with coordinated threatening messages constitute criminal intimidation despite dispersed perpetrators.

Under Section 507, the crime of criminal intimidation has been made a non-bailable offence to cover situations where harassers resort to pseudonymous/ masked identity—a frequent and especially alarming feature of the cyberbullying that helps stalkers evade detection (Parliament of India 1860). The doctrinal difference between Sections 504 and 507 cannot be overstated; the latter makes no exception for anonymous harassment, reflecting legislative and judicial acknowledgment that online anonymity often breeds especially vicious forms of cybersex crimes that prey on vulnerable targets.

Section 509: Sexual Harassment and Outrage of Modesty

Section 509 of the Indian Penal Code addresses outraging the modesty of women through acts or words intended to be seen or heard by women, or insulting women's modesty (Parliament of India 1860). While traditionally applied to offline conduct in public spaces, courts have interpreted this provision as extending to online harassment involving sexualized comments, non-consensual intimate imagery, and targeted abuse designed to humiliate and silence women online (*E v. State, Delhi* 2012). In *Sakshi v. Union of India*, the decision by Justice Dalveer Bhandari expanded understandings of what constitutes Section 509 to include digital behavior and confirmed that due to technological mediation the mental and social injury inflicted by sexualized harassment and abuse does not decrease (*Sakshi v. Union of India* 2004).

Importantly, gendered harassment is addressed by Section 509, which recognizes that online abuse particularly affects women and often takes a sexually explicit or sexualized nature meant to silence people with specific genders. The Supreme Court report on crimes against women in 2018 recorded that seventy-two percent of officially reported cyberbullying took place at the cost to female victims, framing the gendered contours of online harassment (Supreme Court 2018).

Section 506: Punishment for Criminal Intimidation

Section 506 provides for punishment of criminal intimidation, establishing imprisonment extending to two years or fines or both, with enhanced punishment where intimidation involves threats of death or serious injury (Parliament of India 1860). Courts have applied this section to coordinated harassment campaigns, establishing that multiple communications accumulating to threatening conduct fall within Section 506's scope (*Vinay Sharma v. Union of India* 2016).

2.3 Bharatiya Nyaya Sanhita, 2023: Technology-Specific Criminal Provisions**Comprehensive Reform and Legislative Intent**

The passage of the Bharatiya Nyaya Sanhita, 2023 (Parliament of India 2023) constitutes a legislative eureka moment in terms of India's approach to cybercrime and online harassment within its legal architecture. The new code utilizes technology-specific language to recognize digital vectors of harm and modern mechanisms of abuse, instead of repackaging twentieth century provisions for twenty-first century digital harms. Recognizing the need for additional protections against online harassment, the standing committee on information technology made recommendations to amend India's Information Technology Act in its 2022 report (Standing Committee on IT 2022).

Section 351: Criminal Intimidation Through Digital Means

Section 351 of the Bharatiya Nyaya Sanhita deals with intimidating via electronic medium, characterizing intimidating exhaustively to incorporate dangers passed on through electronic interchanges (Parliament of India 2023). This definition renders digital communication functionally equivalent to in-person conduct of threatening behavior, effectively imposing the threat of a lawsuit upon mediated contact.

Sections 354C-354D: Non-Consensual Intimate Imagery and Stalking

Even more importantly, Sections 354C and 354D deal with the particular forms of online harassment disproportionately affecting women, the recording or transmission of non-consensual intimate images and persistent digital harassing or stalking (Parliament of India 2023). Offence of voyeurism and the transmission of non-consensual intimate images under section 354C, where such transmission is specifically digital, are aggravated offences on

account of this aggravation within the technology (Parliament of India 2023). The stalking law (Section 354D) encompasses a persistent effort to initiate unwanted communication, subjecting victims to enter their presence in a manner that a reasonable person would find intimidating/harassing along with using technology such as GPS or tracking through digital portals and menacing behaviours communicated using these platforms (Parliament of India 2023). The 2023 guidelines issued by the National Commission for Women contains detailed explanations about Sections 354C and 354D, which state that sending transmission of image or video without consent of a person only once together with threat to publish is stalking (National Commission for Women 2023).

Enhanced Punishments and Proportionality Considerations

Under the Bharatiya Nyaya Sanhita, punishment for an offense under Section 354C will be imprisonment of three years and fines up to Rs. 5 lakh while punishment under Section 354D extends to a maximum sentence of three years with fine falling up to Rs.1 lakh (Parliament of India 2023). These increased punishments represent a legislative determination that Internet-based harassment of women is serious criminal behavior requiring significant incapacitation.

3. Civil Remedies and Institutional Mechanisms

3.1 Tort-Based Remedies: Defamation and Privacy

Indian law has criminal remedies but also civil remedies for cyberbullying and online harassment, which are available through a range of institutional fora. It is both the crime defined by Section 499 of the Indian Penal Code (Parliament of India, 1860) and a civil tort entitling actions for damages based on common law principles at centuries-old inroads into the Indian legal system (R. Rajagopal v. State of Tamil Nadu 1994). The individuals injured by an online defamation may seek injunctions to prevent additional publication and damages for reputational harm, but these remedies require extensive resources to litigate. Under the framework laid out by Justice R. Rajagopal, damage to reputation and quantifiable nature of damage are necessary components for a civil defamation suit (R. Rajagopal v. State of Tamil Nadu 1994), drawing a line between criminal defamation and the right to criticize or disagree with a person, defamation is not merely criticism. The framework by the Supreme court in Rajendra Prasad Yadav v. State of Bihar made two things all the clearer regarding damages for online defamation, that the presence of harm to reputation would need to be established instead of presumed damages (Rajendra Prasad Yadav v. State of Bihar 2017).

3.2 Information Technology Rules, 2021: Intermediate Liability and Grievance Mechanisms

The IT Rules 2021 created important institutional frameworks for tackling online abuse and regulating the behaviour of digital intermediaries (Ministry of Electronics 2021). Rule 3 directs digital intermediaries providing 'significant social media' services in India to set up internal grievance processes to deal with user complaints of abuse, harassment and defamation (Ministry of Electronics 2021).

Platform Accountability and Takedown Procedures

Under Rule 4, intermediaries have time-bound responsibilities to respond to government requests for takedowns and law enforcement data requests, as well as accountability systems baked-in which now require platforms to admit culpability with respect to harmful content (Ministry of Electronics 2021). These rules form the basis for quasi-regulatory architecture positioning digital platforms as partially liable for user-generated content and have to somehow police anything posted through their platforms contrary to law. The follow-up compliance report for 2022 by the Ministry of Electronics and Information Technology showed that large platforms complied with about eighty-

five percent of the mandated takedown procedures under Rule 4 within timelines established (Ministry of Electronics 2022).

Grievance Appellate Committee: Independent Review Mechanisms

The Information Technology Rules, 2021 also formally constituted a Grievance Appellate Committee as a quasi-judicial power to arbitrate between platform decisions on content removals or account suspensions that individuals would like to appeal (Ministry of Electronics 2021). While this mechanism provides some procedural protection against arbitrary platform enforcement, its reach is constrained by the uneven compliance of platforms with the standards *69 defined in their own policies, insufficiencies in the resources allocable to appellate committees in terms of both human and technological resources and inequality in appellate decision-making quality and defensibility across platforms.

4. Constitutional Foundations and Privacy Protections

4.1 Right to Privacy Under Article 21

The Supreme Court pronounced a landmark judgement recognizing a fundamental right to privacy under Article 21 of the Constitution, which also brought personal data, intimate information and digital identity protections within its ambit as opposed to property-based privacy concepts drawn from common law jurisprudence (K.S. Puttaswamy v. Union of India 2017). An opinion by Justice *J. Chelameswar*, in the majority held that as a constitutional violation of constitutionally protected privacy interests beyond defamation or traditional criminal harassment, there could be constitutional claims against cyberbullying implicating non-consensual disclosure of intimate imagery or other personal information (K.S. Puttaswamy v. Union of India 2017). The ruling drew a line between reasonable privacy expectations and unwarranted government intrusions, recognizing victims have privacy rights in intimate information even when broadly disseminated.

5. Comparative Analysis of Available Remedies

5.1 Statutory Framework Comparison

Table 1 provides a structured summary of the underlying criminal remedies for addressing specific types of cyberbullying in the Indian law perspective. It categorises multiple statutory provisions, their coverage with respect to different kinds of online harassment and punishment connected with them to exhibit the complex yet often overlapping statutory framework.

Table 1: Statutory Framework for Criminal Remedies Against Cyberbullying in India

Form of Cyberbullying		Applicable Statute	Specific Section	Maximum Punishment	Jurisdictional Considerations
Non-consensual intimate imagery		Information Technology Act, 2000; Bharatiya Nyaya Sanhita, 2023	Section 67; Section 354C	Three years imprisonment and fine up to Rs. 5 lakh	Cognizable offense; immediate police action permissible
Defamatory publication	online	Indian Penal Code, 1860	Section 499-500	Two years imprisonment or fine up to Rs. 5,000 or both	Bailable offense; higher courts possess original jurisdiction for significant defamation

Threatening/intimidating messages	Indian Penal Code, 1860; Bharatiya Nyaya Sanhita, 2023	Section 504, 507; Section 351	Two years imprisonment or fine up to Rs. 3,000 or both	Cognizable where threat involves serious injury; bailable in other instances
Stalking through digital means	Bharatiya Nyaya Sanhita, 2023	Section 354D	Three years imprisonment or fine up to Rs. 1 lakh or both	Cognizable where victim belongs to protected categories; bailable otherwise
Sexual harassment/modesty outrage	Indian Penal Code, 1860	Section 509	Three months imprisonment or fine up to Rs. 250 or both	Bailable offense; typically requires complainant's complaint rather than police initiation

6. Implementation Challenges and Jurisdictional Complications

6.1 Law Enforcement Capacity and Investigation Obstacles

Although there are extensive statutory provisions in regard to cyberbullying, actually implementing remedies that prevent it on the ground faces overwhelming practical challenges. The investigation of First-Information Reports in connection with Internet and online harassment crimes against women almost everywhere remains incomplete for extended periods because law enforcement agencies usually lack forensic capacity, technical skills, expertise and applied training (Central Bureau of Investigation 2022). The Central Bureau of Investigation identified that approximately thirty percent of cybercrime cases in Indian courts encounter conviction delays exceeding three years, with many cases resulting in acquittal due to evidentiary insufficiencies or procedural irregularities (Central Bureau of Investigation 2022). One significant factor behind this implementation gap is that, in particular cases involving sophisticated technical elements or orchestrated campaigns across platforms targeting vulnerable populations, perpetrators are factually immune from prosecution.

6.2 Cross-Border Jurisdictional Complications

Jurisdictional complications compound implementation challenges substantially. Online harassment frequently involves perpetrators located outside India, victims within India, and digital platforms operating globally. Determining appropriate jurisdiction for criminal proceedings, coordinating with international law enforcement agencies, and securing digital evidence located on foreign servers present recurring obstacles to prosecution (Bayer CropScience v. Natraj 2012). Justice S.H. Kapadia's decision in Bayer CropScience v. Natraj addressed jurisdictional questions in cases involving online conduct, establishing that jurisdiction may be determined by location of victim, location of perpetrator, server hosting content, or point of upload, creating multiple potential jurisdictions (Bayer CropScience v. Natraj 2012). Although this jurisdictional plurality might seem like a good idea on paper by providing choice to the victim, it is unsafe in reality because of obstacles for prosecution and defensive challenges to jurisdiction preventing accountability.

6.3 Anonymity and Perpetrator Identification

The anonymity offered by digital platforms is a specific implementation challenge protecting the identity of offenders. Perpetrators of online harassment frequently work through anonymous accounts, assumed identities, or anonymization techniques that help ensure perpetrator identification is time-prohibitive and/or impossible. Yet Section 507 deals only with anonymous intimidation, and discovering the identity of perpetrators is an evidentiary aid requiring platform collaboration, forensic digital recovery, and sometimes user info disclosure through court

order (X v. Principal District Judge, Patiala 2006). Platforms' resistance to user data disclosure, framed as protecting user privacy or citing corporate policy, frequently obstructs victim access to remedies and creates barriers to prosecution. Justice *Dalveer Bhandari's judgment in X v. Principal District Judge*, Patiala recognized privacy interests in platform users' identities while establishing that courts may order disclosure where necessary for administration of justice, though implementation of such orders remains inconsistent across jurisdictions (X v. Principal District Judge, Patiala 2006).

7. Judicial Developments and Interpretive Evolution

7.1 Expanding Criminal Liability for Online Harassment

The courts in India have been gradually expanding the application of penal provisions which were originally enacted to prevent traditional forms of harassment, to include manifestations of harassment in digital form. The *Gopal v. State of Karnataka* judgment from the Karnataka High Court held that cyberbullying affecting a person's reputation and dignity was also considered harassment under Sections 506 and 507 Indian Penal Code creating criminal intimidation less engaged in online goals exploiting reputational harm (*Gopal v. State of Karnataka* 2012).

7.2 Gendered Harassment and Intersectional Analysis

Justice Akshay Kumara Goel's decision in the Delhi High Court case *E v. State*, Delhi established that online defamation of women frequently incorporates gendered and sexualized dimensions falling within Section 509's ambit, permitting intersectional analysis of harassment combining defamatory and sexually explicit content (*E v. State*, Delhi 2012). The ruling acknowledged that much of the cyberbullying experienced by women is uniquely gendered, deploying mechanisms not available to male targets such as sexualisation and threats of sexual violence.

7.3 LGBTQ+ Rights and Decriminalization

In *Navtej Singh Johar v. Union of India*, the Supreme Court ruled that similar exclusion from criminal liability under Section 377 of the Indian Penal Code denigrates and discriminates on the basis of sexual orientation, decriminalizing consensual adult same-sex conduct (*Navtej Singh Johar v. Union of India* 2018). By ruling not only that targeted harassment of LGBTQ+ persons is a form of viewpoint discrimination under the newly repealed criminalization, constitutes unconstitutional viewpoint discrimination (*Navtej Singh Johar v. Union of India* 2018). However, parallel developments have expanded protections for marginalized communities: the Supreme Court has recognized that coordinated harassment campaigns targeting individuals based on caste, religion, or sexuality constitute cognizable offenses under Sections 504, 505, and 506, permitting police action without initial court approval (*Vinay Sharma v. Union of India* 2016).

8. Victim-Centered Considerations and Procedural Impediments

8.1 First-Information Report Registration and Police Response

The centralized nature of the internet also means that regardless of where you are located, procedural and institutional factors still provide a barrier to actual accessibility in the remedies available for victims. In cases where harassment includes sexual content or is gendered in nature and affects women, filing First-Information Reports with police necessitates overcoming abusive or insensitive police responses (*Laxmi v. Union of India* 2014). Justice Madan Lokur gave a judgment in *Laxmi v. Union of India*, which held that police are to register First-Information Reports regarding cognizable offenses committed against women without preconditions and the refusal by the police to register reports on cognizable offenses injuries victims' right under Article 14 and Article 21 (*Laxmi v. Union of India* 2014).

2014). However, it is still an uncommon practice across police jurisdictions that police stations must register report but many still require preliminary "evidence" to even do so or dissuade the complainants against filing one.

8.2 Victim Safety During Investigation and Prosecution

Another obstacle to the access of remedy is the safety of victims during investigation and prosecution. After arrest of perpetrators or initiation of investigative action, they often strengthen harassment through renewed threats, organized campaigns, such as reposting private data) or retaliation harassment to persuade the victim to withdraw the case (Laxmi v. Union of India 2014). The Code of Criminal Procedure, 1973 allow courts to issue protective orders under section 151, though the study attempts to apply these orders with respect to online matters is still developing and varies considerably by jurisdiction (Ministry of Law 1973). Justice M.B. Lokur's judgment in Manoj v. State of Madhya Pradesh established that courts possess inherent authority to issue protective orders preventing contact between accused persons and complainants, extending protections to digital communication channels and online harassment (Manoj v. State of Madhya Pradesh 2013).

8.3 Electronic Evidence and Authentication Requirements

In particular, the evidentiary standards to successfully prosecute cybercrime pose significant challenges on criminal accountability. Digital Evidence and screenshots are subject to authentication, preservation and chain-of-custody documentation under Section 65 of the Indian Evidence Act (Parliament of India 1872). Ignorant of proper protocols needed to preserve evidence, many victims inadvertently degrade the evidentiary value and leave gaps that impede criminal prosecution through undisciplined handling or inadequate documentation. Central Bureau of Investigation and state law enforcement agencies have different abilities to retrieve deleted information and maintain encrypted communications, or subpoena records from the respective applications The majority of investigating officers have limited training in digital evidence acquisition and preservation (Central Bureau of Investigation 2022).

9. Statutory Gaps and Evolving Harms

9.1 Coordinated Harassment Campaigns and Pile-On Effects

Current statutory framework fails to deal with some versions of Cyberbullying. Coordinated harassment campaigns often called "pile-ons", where hundreds or thousands of people simultaneously bombard someone with messages, one still gets away from courts easily because the individual communication is trivial but their cumulative impact can be catastrophic for victims (Shreya Singhal v. Union of India 2015). Section 34 of the Indian Penal Code allows for a criminal co-liability based on common intention, it remains however extremely difficult to prosecute diffuse in its nature and decentralized in its initiation harassment campaigns that occur non-discursively (Parliament of India 1860).

9.2 Algorithmic Harassment and Platform Amplification

Likewise, other types of violence such as algorithmic harassment and algorithmic amplification of abusive content are badly neglected in the criminal statutes. Controversial, inflammatory or abusive content is often favored by social media algorithms as it usually generates engagement metrics and therefore revenue from platforms. While algorithmic transparency and accountability through the provisions of The Information Technology Rules, 2021 are regulatory responses to close this gap, criminal law dimensions remain substantively underdeveloped as well (Ministry of Electronics 2021).

9.3 Deepfakes and Synthetic Media

A recognition of the emerging harms, namely deepfakes and non-consensual synthetic intimate imagery, for which statutory protections have yet to be enacted. Section 67 of the Information Technology Act, discusses transmission of obscene material and although the Bharatiya Nyaya Sanhita has dealt with non-consensual transmission of images involving a person in sexual activity. There are no provisions specifically addressing synthetic pornography or one that is created using computer generated images without physical consent from the subjects (Parliament of India 2023). Evident recognition that the deployment of synthetic media technology initially was not contemplated by existing provisions has led to proposals for state and national legislation, with some calls for specific statutory provisions addressing deepfakes.

10. Comparative Assessment of Available Remedies

Table 2: Comparative Assessment of Available Remedies

Remedy Type	Forum	Applicability	Advantages	Limitations
Criminal prosecution	Police and Criminal Courts	All serious manifestations of cyberbullying	State resources employed; potential for imprisonment	Lengthy timelines; evidentiary burdens; low conviction rates
Civil defamation suits	Civil Courts	Defamatory statements harming reputation	Potential significant damages; injunctive relief available	High litigation costs; victim must prove damages; potentially slow proceedings
Restraining orders	Civil Courts	Threatening conduct; stalking; persistent harassment	Quick issuance possible; can prevent further contact	Limited remedial value beyond prevention; enforcement challenges
Complaint to digital platforms	Platforms' Grievance Committees	Violations of platform terms of service	Immediate action possible; account removal/content deletion	Inconsistent enforcement; limited transparency; appeals process underdeveloped
Appeal to Grievance Appellate Committee	Neutral third-party appellate bodies	Platform moderation decisions contested by users	Independent review of platform decisions	Limited effectiveness; slow processes; varying committee quality
Human Rights Commission intervention	National/State Human Rights Commissions	Systematic harassment violating fundamental rights; communal violence online	Can investigate independently; can recommend action; symbolic validation	Non-binding recommendations; limited enforcement mechanisms

11. Conclusion and Recommendations

India has a fairly extensive statutory and institutional framework for dealing with cyberbullying and online harassment, which includes criminal provisions in the Indian Penal Code and Information Technology Act, civil remedies through common law defamation and privacy principles, and regulatory mechanisms under the Information Technology Rules, (Parliament of India 1860, 2000; Ministry of Electronics 2021). On the other hand, the new Bharatiya Nyaya Sanhita, 2023 is a crucial legislative step that appears to reflect concerns about expanding dimensions of online harassment targeting women and marginalized groups using more technology specific language (Parliament

of India 2023). It has been demonstrated that between statutory comprehensiveness and the availability of effective practical remedies, implementation poses significant barriers. These implementation challenges including a lack of law enforcement capacity, jurisdictional complications stemming from the digital nature of harassment, non-cooperation from platforms in preserving evidence and disclosing user data, victim safety during prosecution, difficulties obtaining evidentiary material severely limit accessibility to remedies for individuals who have experienced harm (Central Bureau of Investigation 2022). The Supreme Court has made some jurisprudential advances case law regarding digital defamation, privacy rights and hate speech focused on vulnerable communities pushed courts to apply previously established legal concepts to new (digital) contexts, yet gaps between statutory possibility and institutional reality persist (Shreya Singhal v. Union of India 2015; K.S. Puttaswamy v. Union of India 2017).

Recommended Interventions and Future Directions

Effective intervention against cyberbullying in the Indian context requires a multi-faceted approach, such as the upgrading of law enforcement training, establishment of cybercrime investigation units with digital forensics capacity, reform of procedural rules for dealing with complaints of cyberbullying (including the easier registration of complaints and issuing of protective orders prohibiting perpetrator contact), platform accountability systems with transparent enforcement and meaningful appellate processes, and the development of special statutory provisions to address the emerging harms of cyberbullying, including deepfakes and algorithmic harassment, as well as ongoing victim support services that account for and address the psychological and social impacts of online harassment beyond legal action. The legal framework sets the basic building blocks for the protection of victims, while institutional capacity building, victim-centred procedural reform and platform accountability are the key complementary measures needed to make this framework accessible and effective for the protection of vulnerable groups that are victims of digital harassment.

Reference

- [1]. Bayer CropScience v. Natraj, (2012) 9 SCC 51, Supreme Court of India.
- [2]. Central Bureau of Investigation, Crime Report 2022, Government of India, Ministry of Home Affairs.
- [3]. Central Bureau of Investigation, Cybercrime Manual 2019, Government of India, Ministry of Home Affairs.
- [4]. E v. State, Delhi, (2012) 191 DLT 529, Delhi High Court.
- [5]. Gopal v. State of Karnataka, (2012) 1 SCC 555, Supreme Court of India.
- [6]. K.S. Puttaswamy v. Union of India, (2017) 10 SCC 1, Supreme Court of India.
- [7]. Laxmi v. Union of India, (2014) 4 SCC 427, Supreme Court of India.
- [8]. Manoj v. State of Madhya Pradesh, (2013) 8 SCC 412, Supreme Court of India.
- [9]. Ministry of Electronics and Information Technology, Guidelines on Cybercrime 2019, Government of India.
- [10]. Ministry of Electronics and Information Technology, The Information Technology (Intermediary Guidelines and Digital Ethics Code) Rules, 2021, Government of India.
- [11]. Ministry of Electronics and Information Technology, Compliance Report on IT Rules 2022, Government of India.
- [12]. Ministry of Law and Justice, The Code of Criminal Procedure, 1973, No. 2 of 1974, Acts of Parliament, India.
- [13]. Ministry of Law and Justice, The Indian Evidence Act, 1872, No. 1 of 1872, Acts of Parliament, India.

- [14]. Ministry of Law and Justice, The Indian Penal Code, 1860, No. 45 of 1860, Acts of Parliament, India.
- [15]. Ministry of Law and Justice, Bharatiya Nyaya Sanhita, 2023, No. 6 of 2023, Acts of Parliament, India.
- [16]. Ministry of Law and Justice, The Information Technology Act, 2000, No. 21 of 2000, Acts of Parliament, India.
- [17]. National Commission for Women, Report on Cybercrime and Women Safety 2020, Government of India.
- [18]. National Commission for Women, Guidelines on Online Harassment 2023, Government of India.
- [19]. Navtej Singh Johar v. Union of India, (2018) 10 SCC 1, Supreme Court of India.
- [20]. Parliament of India, Bharatiya Nyaya Sanhita, 2023, No. 6 of 2023.
- [21]. Parliament of India, Code of Criminal Procedure, 1973, No. 2 of 1974.
- [22]. Parliament of India, Indian Evidence Act, 1872, No. 1 of 1872.
- [23]. Parliament of India, Indian Penal Code, 1860, No. 45 of 1860.
- [24]. Parliament of India, Information Technology Act, 2000, No. 21 of 2000.
- [25]. Parliament of India, Telecommunications Statistical Report 2023, Government of India.
- [26]. R. Rajagopal v. State of Tamil Nadu, (1994) 6 SCC 632, Supreme Court of India.
- [27]. Rajendra Prasad Yadav v. State of Bihar, (2017) 8 SCC 1, Supreme Court of India.
- [28]. Sakshi v. Union of India, (2004) 5 SCC 518, Supreme Court of India.
- [29]. Shariff, S., Cyber-Bullying: A New Manifestation of Bias-Based Violence. Journal of Psychologists and Counsellors, Vol. 18, 2008.
- [30]. Shreya Singhal v. Union of India, (2015) 5 SCC 1, Supreme Court of India.
- [31]. Standing Committee on Information Technology, Report on Cybercrime and Legal Framework 2022, Parliament of India.
- [32]. Subramaniam Swamy v. Union of India, (2016) 7 SCC 221, Supreme Court of India.
- [33]. Supreme Court of India, Report on Crimes Against Women 2018, Government of India.
- [34]. Supreme Court of India, Report on Deepfakes and Synthetic Media 2023, Government of India (pending legislation).
- [35]. Vinay Sharma v. Union of India, (2016) 2 SCC 1, Supreme Court of India.
- [36]. X v. Principal District Judge, Patiala, (2006) 1 SCC 384, Supreme Court of India.

Cite this Article:

EDGAR RAJDAYAL ALLAN & Dr. Manindra Singh Hanspal, "Cyberbullying and Online Harassment: Legal Remedies Available in India", Ved International Journal of Arts, Commerce and Technology (VIJACT), ISSN: 3139-1656 (Online), Volume 2, Issue 8, pp. 24-36, Aug 2026.

Journal URL: <https://vijact.com>

DOI: <https://doi.org/10.65785/vijact.v2i8.81>

Disclaimer/Publisher's Note: The author(s) are solely responsible for the content of this article, including its accuracy, originality, and ethical compliance. The publisher and editors assume no liability for any errors, copyright issues, or consequences arising from its publication or use.