INDIAN JOURNAL OF LEGAL REVIEW

VOLUME 6 AND ISSUE 2 OF 2026

INSTITUTE OF LEGAL EDUCATION

INDIAN JOURNAL OF LEGAL REVIEW

APIS – 3920 – 0001 | ISSN - 2583-2344

(Open Access Journal)

Journal's Home Page – https://ijlr.iledu.in/

Journal's Editorial Page - https://ijlr.iledu.in/editorial-board/

Volume 6 and Issue 1 of 2026 (Access Full Issue on - https://ijlr.iledu.in/volume-6-and-issue-1-of-2026/)

Publisher

Prasanna S,

Chairman of Institute of Legal Education

No. 08, Arul Nagar, Seera Thoppu,

Maudhanda Kurichi, Srirangam,

Tiruchirappalli – 620102

Phone : +91 73059 14348 - info@iledu.in / Chairman@iledu.in

INDIAN JOURNAL OF LEGAL REVIEW [IJLR – IF SCORE – 7.58]

VOLUME 6 AND ISSUE 2 OF 2026

APIS – 3920 - 0001 *(and)* ISSN - 2583-2344

Published by

Institute of Legal Education

https://iledu.in

NAVIGATING CYBERBULLYING LAWS IN INDIA: ADDRESSING CHALLENGES AND REFORM OPPORTUNITIES POST-REPEAL OF SECTION 66A

AUTHOR - SHRIYA JAYASHANKAR, STUDENT AT SCHOOL OF LAW, CHRIST (DEEMED TO BE UNIVERSITY)

BEST CITATION – SHRIYA JAYASHANKAR, "NAVIGATING THE NEXUS: THE ROLE OF WTO JURISPRUDENCE IN HARMONIZING INTERNATIONAL TRADE AND CLIMATE CHANGE POLICIES", *INDIAN JOURNAL OF LEGAL REVIEW (IJLR)*, 6 (2) OF 2026, PG. 918-928, APIS – 3920 – 0001 & ISSN - 2583-2344.

ABSTRACT

The explosive growth of digital technology has revolutionized communication in India, both empowering and subjecting people to the risks of new vulnerabilities. Perhaps the most urgent of these threats is cyberbullying, which takes the form of repeated online harassment, defamation, intimidation, and abuse. Compared with traditional bullying, cyberbullying's anonymity, amplification, and permanence cause intense psychological and reputational damage. India originally dealt with this issue under Section 66A of the Information Technology Act, 2000, which criminalized "grossly offensive" or "menacing" computer programme messages[2487]. The provision's vagueness and overbreadth resulted in its abuse for silencing dissent, and the Supreme Court in ***Shreya Singhal v. Union of India (2015)*** invalidated it as unconstitutional. Although this protected freedom of expression under Article 19(1)(a), it also left a vacuum in law, making victims of cyberbullying dependent upon dispersed provisions under the IT Act and the Bharatiya Nyaya Sanhita that fail to encapsulate the continuous, composite character of the offence.[2488]

This paper examines the extent to which statutory law deals with cyberbullying after Shreya Singhal's case, how judicial interpretations have shifted in the absence of a codified offence, and whether India needs a specific law to reconcile Article 19's protections with the right to dignity and privacy under Article 21[2489]. Taking a doctrinal approach, the study examines statutory law, constitutional jurisprudence, and leading judicial pronouncements, while taking into account academic scholarship and comparative models from jurisdictions like the UK and Australia.

Keywords

Cyberbullying, Information Technology Act (2000), Section 66A - Shreya Singhal, Freedom to Speech, Article 21

[2487] Information Technology Act, 2000, § 66A (India)
[2488] **Shreya Singhal v. Union of India** *(2015) 5 SCC 1 (India).*
[2489] India Const. art. 21, art. 19

INDIAN JOURNAL OF LEGAL REVIEW [IJLR – IF SCORE – 7.58]

VOLUME 6 AND ISSUE 2 OF 2026

APIS – 3920 - 0001 *(and)* ISSN - 2583-2344

Published by

Institute of Legal Education

https://iledu.in

Introduction

The broad expansion of technology has transformed communication in India, leading to production in both empowerment and vulnerability. Among the grave consequences is cyberbullying, a phenomenon that exhibits harassment, intimidation, defamation, and abuse through online platforms. Cyberbullying seeps into intimate spheres of life through digital connectivity, which results in greater reputational as well as psychological harm, unlike traditional bullying, making legal regulation not only a policy priority but a constitutional necessity since it directly implicates the right to live with dignity under Article 21 of the Constitution[2490].

India's early legislative regime tried to curb dangerous expression on the internet with Section 66A of the Information Technology Act, 2000, that punished "grossly offensive" or "menacing" messages or communications via the medium of electronic machines. This law was enacted seeking to safeguard citizens from online bullying and generally encompassing cases of cyberbullying. However, the law was extremely loosely phrased, and the undue breadth facilitated its abuse by the authorities to suppress genuine expression, which resulted in nationwide criticism[2491]. In *Shreya Singhal v Union of India (2015)*, the Supreme Court held Section 66A of the IT Act, 2000, to be unconstitutional on the basis that it did not pass tests of reasonableness and proportionality under Article 19(2)[2492].

Whilst the judgment safeguarded freedom of speech, it also dismantled the only statutory provision that could be invoked against cyberbullying. The absence of a substitute mechanism has left the victims dependent on general provisions relating to obscenity, defamation, or criminal intimidation under the IT Act and Bharatiya Nyaya Sanhita. These provisions do not adequately capture the various stems of cyberbullying or online abuse[2493].

I. Problem Statement

A twofold legal challenge emerged from the Shreya Singhal case: first, how the courts and other authorities navigate the absence of a cyberbullying offence; second, how to restore the balance between the protection of free speech under Article 19 of the Constitution and the protection of dignity and privacy under Article 21[2494]. The failure to address this legal gap has resulted in inconsistent judicial interpretations, underenforcement of existing laws, and inadequate remedies for victims. The issue has thus become whether the absence of Section 66A has left a void that the legislature has failed to fill[2495].

II. Conceptual and Historical Background

Cyberbullying can be defined as the use of technology, including social media platforms, texting, and gaming forums, to harass, threaten, and defame individuals, resulting in psychological and reputational harm. Unlike traditional bullying, cyberbullying is augmented by the features of the internet, like anonymity, wider audience reach, and tuning of algorithms.

The IT Act, 2000, was India's first legislation addressing online harassment, giving legal recognition to electronic transactions and regulating misuse of digital platforms. Initially, the Act dealt with commerce-oriented activities like e-signatures, authentication, and cyber fraud. Eventually, with the proliferation of social media and e-communication, the focus expanded to personal harassment and abuse[2496].

To address this, the government introduced provisions criminalizing obscene content, such as Sections 67, 67A, 67B, and other forms of harmful communication[2497]. Nevertheless, the

[2490] India Const. art. 19(1)(a)
[2491] Information Technology Act, 2000, § Section 66A (India)
[2492] **Shreya Singhal v. Union of India** *(2015) 5 SCC 1 (India)*
[2493] Bharatiya Nyaya Sanhita, 2023 (India)
[2494] India Const. art. 21
[2495] Supra note 2
[2496] Information Technology Act, 2000 (India)
[2497] Information Technology Act, 2000, § Section 67, 67A, 67B (India)

absence of a specific and direct provision on offensive speech led to the addition of Section 66A in 2008 through an amendment, specifically aimed at regulating the transmission of "offensive" and "menacing" messages. This marked the beginning of a statutory response to online abuse[2498].

III. Standpoint of Section 66A

Section 66A of Information Technology Act, 2000 criminalized any individual who sent computer messages that were "grossly offensive" or of "menacing character", as well as those that were likely to cause "annoyance, inconvenience, danger, insult, injury, obstruction, enmity, criminal intimidation, hatred, or ill will". The sentence under this section was imprisonment for a term not exceeding 3 years, with a fine.

The objective of this section was rooted in the state's concern over the increasing misuse of digital platforms for harassment, threats, and defamation. The enactment of this section was with the intention to serve as a "catch-all" mechanism for protecting individuals from harm caused by online communications, including instances of cyberbullying. While this section was in practice during 2008-2015, it was the most widely invoked provision against online harassment.

From the perspective of cyberbullying, Section 66A offered as a relatively straightforward legal tool. Its ambiguous and unspecific wording meant that any form of virtual harassing communication could be prosecuted under it[2499].

IV. Criticism and misuse of Section 66A

While the motive behind the enactment of Section 66A was to protect individuals, it drew criticism for its vagueness and ambiguity. The key terms such as "grossly offensive" and "annoyance" lacked legal clarity – leaving their interpretation to the subjective discretion of legal authorities. This resulted in the misuse of the provision, where individuals were penalized for posting political satire, criticism of public personalities, or even just sharing memes. Legal scholars and civil society organizations protested, stating that the law became a tool for suppressing dissent, expressing opinions, and curbing legitimate speech. In many instances, this provision was used in situations that had little to nothing to do with harassment or cyberbullying, thereby straying away from its original purpose. [2500]

V. Landmark Repeal: Shreya Singhal v. Union of India, 2015

The constitutional challenge to Section 66A ended in the Supreme Court's decision in Shreya Singhal v Union of India, 2015, where the court struck down the provision as unconstitutional and held that it violated Article 19(1)(a) of the Constitution, and it could not be justified as a reasonable restriction as mentioned in Article 19(2). The judgment highlighted the importance of clear wording and precision of legal statute, especially of those curtailing fundamental rights.

With respect to cyberbullying, the judgment focused on two major issues: firstly, it protected the freedom of speech and expression from arbitrary restrictions due to the vague nature of the provision, which affirmed that ambiguous laws cannot serve as constitutional regulatory tools. Secondly, it eliminated the only statutory provision that broadly addressed cyberbullying, without introducing any alternative framework. This created a significant legislative gap in specifically targeting cyberbullying[2501].

VI. Contribution and Limitations of Section 66A in Cyberbullying Regulation

Section 66A legislatively recognized that harmful online communication could warrant a criminal penalty. Its existence reflected an acknowledgement that digital harassment was a unique category of harm, which required state intervention. However, the contribution of this

[2498] Supra note 2
[2499] Supra note 2
[2500] Harsh Vardhan Rathi, Need of Special Provisions for Cyberbullying in India, 18 Supremo Amicus 388, 392 (2020)
[2501] **Shreya Singhal v. Union of India** *(2015) 5 SCC 1 (India).*

INDIAN JOURNAL OF LEGAL REVIEW [IJLR – IF SCORE – 7.58]

VOLUME 6 AND ISSUE 2 OF 2026

APIS – 3920 - 0001 *(and)* ISSN - 2583-2344

Published by

Institute of Legal Education

https://iledu.in

section was subverted by its misuse. By failing to clearly distinguish between harmful bullying and legitimate criticism, Section 66A collapsed into a generic offensive speech prohibitory provision. While this violated free speech and expression, it also diluted its effectiveness in protecting victims. The absence of targeted and clear statutory language meant that whilst the law was available, its application was inconsistent and often unjust.

VII. Gap Created Post-Repeal

The repeal of Section 66A created a void in the field of cyber law. While certain sections under the IT Act, 2000, such as Section 67 and Section 67A, address obscene material, and BNS provisions deal with defamation and criminal intimidation, none of these provisions directly capture the harm caused by cyberbullying.

This gap is evident in judicial decisions post-2015, where courts quite often acknowledged the limitations of the existing laws in providing appropriate remedies. The victims are left to navigate through fragmented provisions, where the outcomes depend upon the judicial interpretation rather than the statutory mandate. The gap disproportionately impacts victims, including women and minors, who face a higher level of online abuse[2502].

VIII. Theoretical lens: Legal Realism

The background in history is also what brings out the importance of considering the problem from the perspective of legal realism. Legal realism looks at how law works in practice, as opposed to how it looks on paper. Section 66A, although aimed at tackling cyberbullying, was used in practice more to suppress dissent than help victims. On the other hand, the abolition of Section 66A, as doctrinally correct as it was, left victims without a definite legal recourse in practice. This separation of legislative intention, judicial rationale, and everyday experience highlights the need for a realist approach to analyzing existing cyberbullying regulation[2503].

IX. Statutory Framework Post-2015

The repeal of Section 66A in the case Shreya Singhal v Union of India, 2015, is a pivotal point in India's cyber law framework. While this judgment was aimed at protecting free speech and expression, it created a vacuum, leaving the question of how to regulate harmful online conduct like cyberbullying unresolved. Since 2015, the judicial authorities have depended on the patchwork of provisions under the Information Technology Act, 2000, the Bharatiya Nyaya Sanhita, 2023 (earlier referred to as the Indian Penal Code), and other legislations.

Information Technology Act, 2000

The IT Act, 2000, is the primary and only legislation governing online misconduct. Post the repeal of Section 66A, the following provisions are most relevant:

- Section 67: This section penalizes publishing or transmission of obscene material through electronic means
- Section 67A: This section penalizes publishing or transmission of sexually explicit content
- Section 67B: This section addresses child sexual abuse material
- Section 66D: This section punishes cheating by impersonation using computer resources.
- Section 66E: This section penalizes the violation of privacy by capturing or transmitting images of private areas without consent[2504].

Bharatiya Nyaya Sanhita, 2023

When IPC was replaced with BNS, the motive was to modernize criminal law. Certain provisions can be invoked in cyberbullying cases, such as:

- Section 356 (Defamation): This section criminalizes false statements harming a person's reputation.

[2502] Junaid Raja, *Cyberbullying and the Law (Legal Framework and Challenges)* (Seminar Paper, ICFAI Univ. Sikkim, 2025), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=5362203

[2503] Radin Max, Legal Realism, JSTOR, Vol.31, No.5, 1931, pp 824-828

[2504] Information Technology Act, 2000, § Section 66D, 66E, 67, 67A, 67B (India)

- Section 351 (Obscene content): This section extends to the digital context
- Section 352 (criminal intimidation): This section covers threats made online
- Section 353 (insulting the modesty of a woman): This section can be applied to online harassment
- Section 124 (voyeurism) and 125 (stalking): This section addresses sexual harassment through digital means

Despite these provisions, none of them directly address cyberbullying as a distinct offence. They cover general types of harm, but are unable to cover the different stems, areas, and trends of the nature of bullying, where harm is not caused by one action. Additionally, the use of classic offences pushes courts to fit offline categories to online actions, usually resulting in inconsistent interpretations[2505].

Digital Personal Data Protection Act, 2023

The recently introduced Data Protection Act, 2023, consists of provisions addressing the protection of informational privacy, such as regulating the misuse of personal data as well as mandating consent for data processing. While this may indirectly protect individuals from certain kinds of online abuse, it does not address cyberbullying directly. The Act's focus primarily lies on state and corporate accountability rather than individual harassment. Hence, it does very little to fill the legislative vacuum[2506].

X. Judicial Interpretation of Cyberbullying Laws after the repeal of Section 66A

The 2015 judgment of the ***Shreya Singhal v Union of India*** was a breakpoint in India's free speech jurisprudence. By repealing Section 66A of the Information Technology Act, 2000 the Supreme Court reaffirmed Article 19(1)(a) as fortification against ambiguous and overbroad criminalization of online expression. Nevertheless, the decision created a regulatory vacuum where, while the freedom of speech was protected, it left the victims vulnerable to harassment without a clear statutory remedy. Without a dedicated law, the Courts have been asked to stretch existing provisions to address digital harms.

Post-2015, the Indian courts often rely on provisions like defamation, obscenity, or criminal intimidation to address online abuse[2507]. For instance:

In ***Shibani Barik v State of Orissa (2020)***, the Orissa High Court acknowledged the absence of a specific law penalizing cyberbullying, instead having to rely on IPC provisions[2508].

In ***Tajinder Pal Singh Bagga v State of Karnataka (2016)***, the court prosecuted the offender under criminal intimidation provisions instead of the targeted statute for online harassment[2509].

These cases illustrate the struggle of the judiciary to stretch the existing laws, inadequately covering cyberbullying, leading to inconsistent enforcement.

Despite the existence of provisions under the IT Act and BNS, the statutes are limited in addressing cyberbullying specifically. This has created a legislative gap where the current laws are fragmented into defamation, obscenity, intimidation, and hence ignore the cumulative trends of cyberbullying. This leads to ignorance of sexual harassment, body-shaming, or hate-driven bullying. The courts have a wide discretion in the application of existing limited laws to the cases of cyberbullying, often leading to inconsistent rulings. The existing laws are not victim-centric and do not consist of remedies like takedown mechanisms and victim support.

XI. Judicial Approach

The judicial approach following the repeal of Section 66A in 2015 has resulted in an imbalance between constitutional ideals and practical enforcement needs. The Indian courts have repeatedly acknowledged the absence of

[2505] Bharatiya Nyaya Sanhita, § Section 356, 351, 352, 353, 124 (India)
[2506] Digital Personal Data Protection Act, 2023, No. 22 of 2023 (India)
[2507] **Shreya Singhal v. Union of India** *(2015) 5 SCC 1 (India)*
[2508] Shibani Barik v. State of Orissa, 2020 SCC OnLine Ori 846 (India)
[2509] Tajinder Pal Singh Bagga v. State of Karnataka, Crl. P. No. 1117 of 2016 (Kant. HC) (India)

INDIAN JOURNAL OF LEGAL REVIEW [IJLR – IF SCORE – 7.58]
VOLUME 6 AND ISSUE 2 OF 2026
APIS – 3920 - 0001 *(and)* ISSN - 2583-2344
Published by
Institute of Legal Education
https://iledu.in

a specific provision addressing cyberbullying, which forces them to stretch the existing laws to cover cyberbullying. Courts, in various cases, have highlighted the limitations and ingenuity of judicial interpretation in filling the legislative vacuum.

Shreya Singhal v. Union of India (2015)

The decision of this case is the foundation for any judicial engagement with cyberbullying. The Supreme Court struck down Section 66A of the Information Technology Act, 2000, recognizing it to be vague and a broad restriction on online communication. The court held that these restrictions violate Article 19(1)(a) of the Constitution and do not fall under the ambit of reasonable restrictions mentioned in Article 19(2). While this judgment was widely celebrated for upholding free speech, it also left courts with no specific statutory tool to address cyberbullying. In cases post-2015, the courts have cited the Shreya Singhal case judgment, underlining the need for precision in drafting laws, while also acknowledging that the absence of a substitute statutory law has resulted in hindrance to victim protection[2510].

People's Union for Civil Liberties v Union of India

Though filed earlier than Shreya Singhal, the PUCL case became relevant after 2015 because the Supreme Court needed to deal with surveillance and monitoring provisions under the IT Act. The Court cited Shreya Singhal while emphasizing the need to avoid abuse of vague statutory provisions. Though the case was more focused on surveillance, its application is to be found in cyberbullying since it emphasized the principle that offensive laws cannot be upheld, even when covering dangerous digital behavior[2511].

Tajinder Pal Singh Bagga v State of Karnataka (2016)

In this case, the petitioner was accused of posting derogatory and threatening remarks online. The High Court of Karnataka dealt with the case under IPC provisions relating to criminal intimidation. The Court avoided invoking broad provisions of the IT Act, following the constraints imposed by the Shreya Singhal case. Although relief was provided, this case exhibits the judiciary's reliance on existing statutory laws, which are insufficient and inadequate to capture the unique features of online harassment. The Court highlighted the inadequacy of the existing statutory framework by stretching it to fit the cyberbullying behavior[2512].

Shibani Barik v State of Odisha (2020)

The Petitioner in this case moved to court to seek relief against abusive and defamatory messages she received on social media. The Orissa High Court held that since Section 66A was no longer in force, they had to rely on provisions relating to defamation and obscenity. The Court observed that the existing laws are "general and do not specifically target the menace of cyberbullying."

This case instantiates the judicial recognitions of the legislative gap. While the Court made an attempt to provide relief through the existing IPC provisions, it also acknowledged that the absence of targeted provisions limits the effectiveness of redress[2513].

Farkudheen Panthavoor v State of Kerala (2025)

In this recent case, the High Court of Kerala confronted offensive digital communications that did not fall within the ambit of obscenity or defamation categories. The Court explicitly held that ten years after the repeal of Section 66A, there is no sufficient, comprehensive, and effective legislation to combat cyberbullying.

[2510] **Shreya Singhal v. Union of India** *(2015) 5 SCC 1 (India)*
[2511] People's Union for Civil Liberties v. Union of India, (1997) 1 SCC 301 (India)
[2512] Tajinder Pal Singh Bagga v. State of Karnataka, Crl. P. No. 1117 of 2016 (Kant. HC) (India)
[2513] Shibani Barik v. State of Orissa, 2020 SCC OnLine Ori 846 (India)

INDIAN JOURNAL OF LEGAL REVIEW [IJLR – IF SCORE – 7.58]

VOLUME 6 AND ISSUE 2 OF 2026

APIS – 3920 - 0001 *(and)* ISSN - 2583-2344

Published by

Institute of Legal Education

https://iledu.in

The ruling put emphasis on the fact that judicial ingenuity cannot replace legislation's lucidity and urged legislation to pass specific provisions. This ruling is a forceful judicial recognition of the legislative vacuum and further enforces the sense of urgency to reform[2514].

Judicial responses after Shreya Singhal reflect creativity as well as constraint. Courts have been aware of the legislative gap, sought to apply existing law, and invoked the legislature to step in. However, judicial solutions are still piecemeal, inconsistent, and limited in scope. The uniform recognition of the legislative vacuum by the High Courts highlights the imperative necessity for a dedicated statutory response. In the absence of legislation, victims of cyberbullying are still insufficiently protected, and the constitutional promise of dignity under Article 21 is still underenforced.

This paper aims to weave together the doctrinal, judicial, and constitutional strands to address pressing questions, such as to what extent the existing laws fill the gap left behind by the repeal of Section 66A, how the courts have interpreted these laws to respond to the emerging digital harms, and whether we require a specific statute to criminalize cyberbullying. Regulatory responses must reconcile freedom of speech and expression with the right to dignity and privacy. Consequently, it is important to address the legal vacuum created by the repeal of Section 66A.

The issue cannot be reduced to a simple binary between free speech and censorship. Instead, it requires a nuanced understanding of various stems and trends of cyberbullying as a unique phenomenon. Instances of obscenity, defamation, or intimidation are already covered under Indian law, whereas cyberbullying is characterized by persistence and anonymity. It is a kind of harassment that thrives on hiding behind the mask of a social media username and the viral nature of digital platforms, where a single message can be circulated and magnified across networks infinite times. Cyberbullying is a composite harm, where victims face reputational damage as well as psychological harm. Hence, this kind of harassment cannot be captured by the existing fragmented provisions.

Judicial engagement with cyberbullying has repeatedly highlighted a pressing concern of absence of a specific and direct statutory framework to combat cyberbullying post – ***Shreya Singhal v Union of India (2015).*** These precedents ascertain the judiciary's recognition of a legal vacuum. Against this judicial backdrop, academic literature plays a vital role here: while the court addresses individual cases, academic writers have examined broader patterns, have proposed frameworks, and evaluated constitutional tensions. A review of key contributions reveal recurring themes, such as, legislative insufficiency, constitutional dilemmas and the need for reforms, while also emphasizing gaps that this research seeks to fill.

Shrivastava and Kushwaha in their research paper "Cyberbullying in India: Drawbacks of applying statutory approach to Cyberbullies" have argued that India's statutory approach towards cyberbullying is flawed because it relies on piecemeal provisions rather than recognizing cyberbullying as a distinct offence. They observe that fragmented provisions like obscenity or defamation criminalizes individual acts only but fail to capture the recurring dimension of cyberbullying. The authors' key observation lies in their insistence that cyberbullying cannot be merely addressed by extending offline offences in online context. They have provided a strong foundation by clarifying why the statutory patchwork is inadequate[2515].

Even where laws exist, victims often hesitate to report abuse due to social stigma or lack of confidence in legal remedies. The enforcement of laws are weak due to lack of awareness and

[2514] Farkudheen Panthavoor v. State of Kerala, 2025 SCC OnLineKer (India)

[2515] Shambhavi Shrivastava & Vivek Kushwaha, Cyberbullying in India: Drawbacks of Applying Statutory Approach to Cyberbullies, 3 Indian J.L. & Legal Rsch. 1 (Dec. 2021–Jan. 2022)

procedural hurdles. This sheds light on the practical accessibility of legal provisions to combat cyberbullying and recognizing it as a distinct offence[2516].

One of the major issue that is not often debated upon is "legal silence". India's failure to enact a cyberbullying legislation post – Shreya Singhal case amounts to a dereliction of constitutional responsibility. Pallavi Gupta and Amrita, in their article, propose a comprehensive statute consisting of both criminal and remedial elements, drawing from models like UK's Online Safety Act and Australia's safety Act. They argue that any new law must balance Article 19 and Article 21, while avoiding the vague nature of Section 66A and also ensuring victim protection. They emphasize the disproportionate impact of cyberbullying on members of vulnerable community like women and children[2517].

These literatures converge on several themes, together they paint a comprehensive picture of the problem like insufficiency of fragmented laws, need for constitutional harmonization and other enforcement challenges. By bridging judicial and literary insights, the synthesis links court recognitions of legislative gaps with academic suggestive reforms. It offers a roadmap for reform by highlighting detailed procedural and substantive safeguards to avoid Section 66A-like misuse.

XII. The Case for a Specific Anti-bullying Law and its Constitutional Design

A decade after the Supreme Court repealed Section 66A of the Information Technology Act, 2000, India remains without a dedicate legal framework for cyberbullying. Courts have repeatedly emphasized on this legislative gap; academic writes have called and proposed reforms and social harm due to digital harassment has increased exponentially. Yet the Parliament hesitates to legislate over this issue under the fear of overbreadth and possibility of conflict with Article 19(1)(a).

The preceding sections have established that IT Act, BNS and other statutes are inadequate for key reasons, firstly, they are conceptually misfit – the provisions on defamations, obscenity and criminal intimidation address specific acts rather than the recurring harm of cyberbullying. Secondly, there are many trends and stems of cyberbullying, which do not fall under the existing legal threshold. Due the fragmentation of existing laws, the victims are left at vulnerable place where they must navigate through multiple legal routes, leading to uncertain and under-enforced rulings. These problems have been judicially acknowledged in multiple cases as mentioned in previous sections. The Courts have been clear in stating that piecemeal adaptation of existing provisions cannot meet the contemporary challenge of digital abuse.

The major reason Parliament hesitates to legislate over the cyberbullying laws is due to the memory of Section 66A's failure. The Court clarified the reason for striking down the provisions was due to its vagueness and overbroad approach. It even stated that the speech maybe restricted under Article 19(2) on the grounds of defamation, decency, morality, and public order. The key takeaways of Shreya Singhal case are, firstly, terms like "grossly offensive" and "annoying" are very indeterminate. Secondly, the complaint mechanisms must avoid exploitation against legitimate dissent. And the restrictions must have a direct tie to the tangible harm like reputation, mental health, etc. A diligently drafter anti-cyberbullying law can meet these standards, whilst avoiding Section 66A's misfiring and protecting victims at the same time.

XIII. Core Elements of Constitutionally Sound Anti-Cyberbullying Statute

Considering the judicial guidance, academic suggestions and comparative models, the following elements can be incorporated into the Indian anti-cyberbullying law:

[2516] Harsh Vardhan Rathi, Need of Special Provisions for Cyberbullying in India, 18 SUPREMO AMICUS 388 (2020)
[2517] Pallavi Gupta & Amrita, Digital Abuse and Legal Silence: Addressing Cyberbullying Through Indian Law, 5 Int'l J. Advanced Legal Rsch. 1 (May 2025)

INDIAN JOURNAL OF LEGAL REVIEW [IJLR – IF SCORE – 7.58]
VOLUME 6 AND ISSUE 2 OF 2026
APIS – 3920 - 0001 *(and)* ISSN - 2583-2344
Published by
Institute of Legal Education
https://iledu.in

a. Clear wording and precise definition of cyberbullying: By defining cyberbullying as targeted, repeated and intentional use of abusive language online towards an individual to cause substantial harm to their reputation and work, it allows us to clearly differentiate between cyberbullying and defamation or obscenity. The words "repetition" and "intentional" are required elements to avoid criminalization of trivial speech. It excludes mere disagreement or criticism, protecting free speech.
b. Tiered offence: Cyberbullying can be divided into two layers
    - Basic Offence: persistent online harassment like troll comments or messages, that can be punished with fines.
    - Aggravated Offence: bullying involving threats, sexualized content, can be punished with stricter penalties.
c. Procedural safeguards: By mandating a prima facie review by the magistrate before the registration of FIR, it helps to prevent misuse of the legislation and categorize the issue between the two tiers.
d. Integration with intermediary obligations: The online platforms must be mandated to maintain rigorous reporting tools, transparency in moderation as well as cooperation with law enforcement. This element will allow to impose penalties on platforms that default to act on substantiated bullying complaints.

By including these elements, the statute would target the offence in its actual sense rather than vague offensiveness, aligning with Article 19 (2) and protecting Article 19 (1) (a).

At the heart of the debate of constitutional balance, lies the tension between Article 19 and Article 21. Shreya Singhal's case protects speech from being subjected to vague censorship by insisting that speech can only be restricted under the reasonable restrictions established under Article 19(2). Cyberbullying directly undermines Article 21 rights, where the state has positive obligation to protect these rights by providing the citizens with effective remedies.

Thus, the challenge is not whether cyberbullying can be regulated, but it is how to do so with precision and proportionality. A law that is narrowly tailored to penalize intentional, repeated and harmful online harassment, falls within defamation, decency or moral grounds under Article 19(2), whilst safeguarding freedom of speech and expression under Article 19(1)(a).[2518]

Legal realism, as discussed earlier, underscores that laws must respond to social realities and not to abstract ideals. The Court post-*Shreya Singhal* have shown realist sensitivity by recognizing harm but respecting legislative boundaries. This research uses realism to argue that constitutional awareness should not mean legislative dormancy. Victims experience real harm, yet Courts are powerless to help without a statutory backing. A fresh, carefully drafted law is therefore a realist response to contemporary needs[2519].

XIV. Comparative Perspective of Cyberbullying

While India brawls with the legislative vacuum left after the *Shreya Singhal* case, many democratic countries have adopted specific statutory approaches to grapple cyberbullying. These models focus on criminalization, platform regulation, civil remedies and education. By comparing various legislative models, it helps illuminate opportunities and constitutional challenges for India.

United Kingdom: Online Safety Act, 2023

The UK's Online Safety Act (OSA) is a shift from criminalization at user level to platform responsibility. It places responsibilities on social media platforms to stop and handle harmful content, including bullying. Ofcom, the regulator

[2518] Divya Yadav, Cyberbullying Laws in India: Current Challenges, 2 Int'l J. Legal Rsch. & Analysis 23 (Mar. 2025), https://www.doi-ds.org/doilink/03.2025-16118857/CYBERBULLYING
[2519] Supra note 14

ensures compliance with sanctions for non-compliance. This Act has a systemic approach by shifting responsibility from victims to platforms. Although, it is widely criticized for potential over censorship by platforms for being anticipatory in nature. It also depends heavily on regulator's capacity. India can adopt intermediary duties with due process, while avoiding broad censorship powers.[2520]

Australia: eSafety Act, 2021

Australia's eSafety Commissioner has wide powers to order for removal of cyber abuse, especially against members of vulnerable community like children and women, within 24 hours. Failure to do so attracts penalties. This Act has rapid takedown mechanism while focusing on vulnerable demographics, allowing it to protect victims quickly. Nevertheless, the con of this Acts is that it relies on administrative discretion, raising due process concerns. Its enforcement against global platforms remains uneven. Indian law makers can seek inspiration from this Act by introducing fast-track takedown body integrated with judicial oversight in order to protect constitutional rights.[2521]

The optimal path for India is to adopt a hybrid model where, a clear statutory offence is codified for intentional, repeated harassment. Civil remedies like injunctions and takedowns are implied and intermediary accountability with due process safeguards is mandated. Constitutionally, these kinds of legislation are possible if narrowly framed to meet proportionality and avoid ambiguity. The need for a particular anti-cyberbullying law in India is therefore both a democratic imperative and a constitutional imperative.

Conclusion

The development of India's law governing online speech, specifically under Section 69A of the Information Technology Act, 2000, is a reflection of constitutional freedoms being pitted against the compulsions of state security, sovereignty, and public order. Judicial and legislative incursions have repeatedly insisted that the right of freedom of speech pursuant to Article 19(1)(a) is not unfettered, but the limitations under Article 19(2) are to be narrow, specific, and proportionate. The absence of transparency in the process of making blocking orders, the lack of strong means of appeal, and the limited role of judicial review continue to throw doubt on whether these mechanisms meet the test of reasonableness and procedural fairness contemplated in the Constitution.

Simultaneously, difficulties of the digital era cannot be downplayed. The unimaginable speed and span of internet communication merely intensify the dangers of misinformation, hate speech, and terrorist propaganda, putting states at odds with themselves. Comparative study goes to prove that although democracies everywhere struggle with the same issues, India's paradigm continues to be executive-driven, with few checks from parliament or judiciary on discretion. This raises the risk of abuse, especially when the restrictions are pre-emptive with not enough justification being made publicly available or to the implicated platforms.

The jurisprudence also shows an uneasy equilibrium between the state and fundamental rights. While courts have generally defended the constitutionality of Section 69A, their willingness to defer to executive judgments provides room for arbitrariness. The lack of published detailed reasoning in block orders makes accountability more difficult and forestalls effective public debate over the proportionality of the restriction. In addition, the secrecy involved in such decisions perpetuates a culture of secrecy that is incompatible with democratic principles of openness and transparency in governance.

The future lies in re-calibrating the regulatory mechanism through a hybrid model that

[2520] Saran Errakot & Rahoof VK, Cyber Bullying: A Need for Separate Provision in Indian Law, 5 GLS L.J. 38 (2023), https://doi.org/10.69974/glslawjournal.v5i1.81
[2521] Pallavi Gupta & Amrita, Digital Abuse and Legal Silence: Addressing Cyberbullying Through Indian Law, 5 Int'l J. Advanced Legal Rsch., no. 4, 1 (2025).

acknowledges the need for restrictions in exceptional situations but is ensured to be based on explicit statutory protections. A system of having statutory offences explicitly laid down for deliberate and repetitive instances of online harm, along with open oversight and independent channels of redress, would reconcile state practice more with constitutional values. Increased parliamentary oversight, judicial review, and public disclosure (wherever national security is not truly threatened) can assist in reestablishing the balance between order and liberty.

Finally, the Indian legal order needs to work towards balancing the need for measures protecting the country with the risk that they pose to the very freedom they are designed to uphold. Finding this balance is important not just for the legitimacy of state institutions but also for supporting a democratic public digital sphere that holds on to individual autonomy while defending against reasonable danger. The search for such a balance is a perpetual constitutional endeavor, one that necessitates watchfulness, openness, and upright dedication by all aspects of the state.