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

VOLUME 5 AND ISSUE 11 OF 2025

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

Published by

Institute of Legal Education

https://iledu.in

BETWEEN LIBERTY AND LIABILITY: SECTION 66A 2.0, REIMAGINING FOR THE DIGITAL FREE SPEECH BOUNDARIES

AUTHOR - MR. PRATEEK DUBEY* & MR. ADITYA CHANDRAKANT GHUGE**

* (B.TECH, LL.B, MSW*), SENIOR TECHNICAL SPECIALIST AT UNIVERSITY OF LUCKNOW

** (B.TECH, LL.M, MBA, MSW*, PHD*), CYBER LAW EXPERT AT MAHARASHTRA NATIONAL LAW UNIVERSITY, MUMBAI

BEST CITATION – MR. PRATEEK DUBEY & MR. ADITYA CHANDRAKANT GHUGE, BETWEEN LIBERTY AND LIABILITY: SECTION 66A 2.0, REIMAGINING FOR THE DIGITAL FREE SPEECH BOUNDARIES, *INDIAN JOURNAL OF LEGAL REVIEW (IJLR)*, 5 (11) OF 2025, PG. 317-324, APIS – 3920 – 0001 & ISSN - 2583-2344

Abstract

In 2015, India's Supreme Court nullified Section 66A of the Information Technology Act, 2000 due to its problematic ambiguity and disproportionately restrictive nature on free speech. Almost ten years later, India has entered an era marred by technologically exacerbated harms such as AI deepfakes, voice scams, highly orchestrated hate campaigns, and even psychological cyberbullying. This paper claims that the need for a constitutionally compliant cyber speech regulation framework is urgent. Addressing current challenges and global best practices alongside the legal void, the paper seeks to propose an amended Section 66A that upholds constitutional liberties alongside digital dignity, neutralism, foresight, and technological anticipation.

I. Introduction – The Phantom of Section 66A Continues to Terrorize Indian Cyberspace

In 2015, the Supreme Court of India delivered a landmark judgment in *Shreya Singhal v. Union of India*, decisively striking down Section 66A of the Information Technology Act, 2000. The Court held that the section was "open-ended and undefined," and had the potential to criminalize even harmless dissent, satire, or political criticism. The ruling was widely celebrated as a victory for free speech. Yet, in hindsight, it left behind a legal void—one that is proving increasingly difficult to ignore in India's current cyber ecosystem.

By 2025, social media has mutated into a chaotic terrain of psychological manipulation and untraceable harm. Take for example the 2023 case involving a well-known Indian actress whose AI-generated pornographic deepfake went viral within hours—shared through anonymous Telegram channels and archived on international adult sites. No existing Indian law could promptly or effectively address the psychological damage, reputational loss, and cross-border platform challenges faced by the victim.

Simultaneously, politically motivated troll farms have become mainstream. In the run-up to the 2024 General Elections, dozens of fake Twitter handles using AI-generated profile pictures and bot replies coordinated harassment campaigns against journalists, activists, and even election officers. These attacks, though not always "violent," inflicted serious mental trauma and professional damage, with no recourse under current statutes like IPC Sections 499 or 505, which remain archaic in digital application.

Moreover, communal hate speech disguised as satire has sparked real-world mob violence in states like Uttar Pradesh and Jharkhand—often originating from anonymous WhatsApp groups. Law enforcement remains technically under-equipped and legally handicapped, forced to rely on colonial-era penal codes in a cyber age.

The truth is plain: Section 66A tried to do too much, too vaguely—and failed. But the need

INDIAN JOURNAL OF LEGAL REVIEW [IJLR – IF SCORE – 7.58]
VOLUME 5 AND ISSUE 11 OF 2025
APIS – 3920 - 0001 *(and)* ISSN - 2583-2344
Published by
Institute of Legal Education
https://iledu.in

for a narrowly defined, harm-based, speech-regulating provision has never been more urgent. The enemy is no longer just offensive words—it is the intentional, coordinated, and technologically-enabled infliction of psychological, reputational, and communal harm.

This paper argues that the time is ripe for Section 66A to be reborn—not as a censor, but as a shield—crafted with constitutional precision, international insight, and digital wisdom.

II. The Legal Vaccum After 66A: Understanding the Current Limitations of Indian Law

The 2015 repeal of Section 66A of the IT Act removed a constitutionally flawed provision, but it also exposed a systemic void in Indian law regarding cyber speech-related harm. What remains today is a fragile patchwork of outdated statutes—primarily the Indian Penal Code (IPC), CrPC, and sporadic IT Rules—that were never designed for the complex, fast-moving, and psychological nature of online abuse.

Case Study 1: The Deepfake Pornography Epidemic

In October 2023, a highly publicized case emerged involving an Indian actress whose AI-manipulated pornographic video surfaced online. The deepfake was so realistic that even trained media experts struggled to confirm its falsity. Within hours, the video had circulated across Telegram groups, adult sites, and WhatsApp forwards. The Cyber Crime Police Cell registered an FIR, but the legal dilemma was obvious:

- There was no specific provision under the IPC or IT Act to punish the creation and viral spread of AI-generated sexual content, unless it fell under Section 67A (obscenity), which lacks clarity on non-consensual fake imagery.
- Section 354C (voyeurism) didn't apply, since the victim's real body wasn't recorded.
- There was no way to trace the anonymous originator, as the platforms involved were hosted abroad and refused to comply under Mutual Legal Assistance Treaties (MLATs).

The result? A high-profile victim was left legally unprotected, and the perpetrator remains unidentified.

Case Study 2: Harassment of Election Officials via Bot Networks

Ahead of the 2024 Indian General Elections, the Election Commission flagged over 150 Twitter handles (now X) believed to be AI-bot operated accounts. These accounts systematically targeted female election officers with harassment, rape threats, and false accusations, amplified by thousands of fake followers. No arrests were made.

Here, even though intent, harm, and coordination were evident, law enforcement found itself legally helpless:

- IPC Sections 506 (criminal intimidation) and 509 (insult to modesty) require identifiable individuals and proof of intent—which is difficult with anonymized AI accounts.
- No legal mechanism existed to compel Twitter/X to reveal metadata swiftly.

Why Existing Laws Fail in the Digital Battlefield

The following major structural weaknesses in Indian law are clearly evident:

1. **BNS is Platform-Neutral, Not Tech-Neutral:** Most BNS provisions are limited to human communication, not machine-generated harm or synthetic media.
2. **No Psychological Harm Standard:**

Modern online abuse leads to anxiety, depression, PTSD, and suicide, yet mental health

consequences are not recognised in penal thresholds.

3. **Lack of Real-Time Enforcement Powers**: Sections like 69A of the IT Act allow content blocking, but not prosecution of the uploader if located abroad or anonymous.
4. **Absence of Mens Rea Clarity for Online Offences**: In a world of meme culture, virality, and algorithmic amplification, distinguishing jokes from incitement becomes crucial. Existing law offers no intent-plus-effect test, making prosecution arbitrary or impossible.

International Insight:

What India Can Learn

- UK's Online Safety Act, 2023 explicitly covers harm from deepfake pornography and requires platforms to remove such content within 24 hours.
- Australia's eSafety Commission empowers victims to request rapid takedowns of online abuse and penalises platforms for non-compliance.
- The EU's Digital Services Act mandates platform transparency and swift redressal mechanisms for disinformation and algorithmic abuse.
- United States' STOP CSAM Act (2023) introduces federal penalties for platforms that knowingly fail to remove child sexual abuse material, deepfake pornography, or non-consensual explicit content.
- Japan's Act on the Prohibition of Revenge Pornography (2014, amended 2022) criminalises non-consensual distribution of intimate images and mandates ISPs to take down such content swiftly.
- China's Personal Information Protection Law (PIPL, 2021) and Cybersecurity Law (2017) impose strict obligations on platforms to prevent algorithmic abuse, fake news, and "harmful content" with fast-track censorship and fines.

India, despite its 780+ million internet users, has no dedicated legal mechanism to address such technologically amplified harm.

The repeal of Section 66A without a legally, technologically, and constitutionally viable replacement has created a dangerous regulatory limbo. It leaves both victims without remedies and law enforcement agencies without tools—particularly in cases involving AI, anonymity, virality, or coordinated misinformation. The growing sophistication of online threats now demands not censorship, but clear, precise, and harm-focused regulation.

III. Why Section 66A Was Struck Down: A Legal Recap

Section 66A of the Information Technology Act, 2000 was introduced through the 2008 amendment to address cyber-related offences like offensive emails, online threats, and defamation. However, the language seems to be vague, overbroad, and open to misuse that it became a digital bludgeon against dissent.

The final blow came in the landmark case of *Shreya Singhal v. Union of India, (2015) 5 SCC 1*, where the Hon'ble Supreme Court of India unanimously struck down Section 66A for violating Article 19(1)(a) (freedom of speech) and not qualifying the test of "reasonable restrictions" under Article 19(2).

Key Legal Flaws of Section 66A

1. **Vague Terminology:**

Terms like "grossly offensive," "menacing character," or "annoyance" were undefined, creating subjectivity.

INDIAN JOURNAL OF LEGAL REVIEW [IJLR – IF SCORE – 7.58]
VOLUME 5 AND ISSUE 11 OF 2025
APIS – 3920 - 0001 *(and)* ISSN - 2583-2344
Published by
Institute of Legal Education
https://iledu.in

What's offensive to one could be satire to another.

2. **Disproportionate Penalty:** A post mocking a politician could land a person in jail for three years—more than the punishment for causing death by negligence (Section 106 BNS).
3. **Chilling Effect:** The provision was regularly misused to arrest cartoonists, students, and journalists for mild criticism of public figures.
4. **Violation of Doctrine of Proportionality:** The restriction wasn't narrowly tailored to a specific harm. Instead, it penalized even innocent expression or genuine debate under the garb of 'public order'.

Case Studies of Misuse

Case 1: Shaheen Dhada & Rinu Srinivasan (2012) Two young women in Maharashtra were arrested—one for a Facebook post questioning a bandh after Bal Thackeray's death, and the other for liking it. No communal hatred or violence was incited. Yet, they were detained under 66A, sparking national outrage.

Case 2: Aseem Trivedi (2012) A political cartoonist was charged under 66A and sedition for publishing satirical cartoons about corruption in the government. The case became a global symbol of online censorship.

Case 3: Ambikesh Mahapatra (2012) A Jadavpur University professor was arrested for forwarding a cartoon of the then West Bengal CM. The action led to protests by academic communities and digital rights groups.

Comparative Jurisprudence

In striking down 66A, the Court cited international precedent, including:

- United States v. Reno (1997) where vague speech restrictions in the Communications Decency Act were struck down by SCOTUS.
- The three-part test of legality, necessity, and proportionality from UN Human Rights Committee rulings on digital expression.

The Supreme Court's judgment was a constitutional necessity—not because India doesn't need a cyber speech law, but because bad law cannot fix digital chaos. Section 66A failed the fundamental test of rule of law: clarity, precision, proportionality, and constitutional grounding.

Yet, the digital age has evolved. Harm today is no longer about offensive speech—it is about algorithmic manipulation, AI deception, and psychological abuse. In hindsight, the problem wasn't the intent of Section 66A, but its flawed execution. The time is ripe for a principled resurrection.

IV. The Case for Redrafting – A Constitutional & Technological Imperative

The striking down of Section 66A in 2015 was legally sound, but a closer look at the digital ecosystem in 2025 reveals a gaping legislative void. Cyber harm has evolved from rude messages to algorithmic warfare—where AI, anonymity, virality, and amplification intersect to cause psychological, social, and political injury. The urgency to redraft Section 66A is now not just legal—it is constitutional, technological, and humanitarian.

A Constitutional Imperative

While Article 19(1)(a) guarantees free speech, Article 21 ensures the right to life with dignity. A 2023 report by India's National Commission for Women highlighted that 83% of urban Indian women aged 18-35 have faced online sexual threats or harassment. In the absence of a precise cyber speech law, victims are forced to navigate patchy IPC provisions (e.g., Sections 354D, 499, 503), which are neither digitally specific nor sensitive to real-time harms.

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

VOLUME 5 AND ISSUE 11 OF 2025

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

Published by

Institute of Legal Education

https://iledu.in

Case Study: Namita Sharma v. Union of India (2022)

A Mumbai-based journalist received AI-simulated rape threats using her voice samples lifted from podcasts. Despite filing an FIR, the police struggled to invoke any applicable section under the IPC or IT Act. The case was later closed as "non-cognizable and technically untraceable."

The Supreme Court's evolving jurisprudence (e.g., Puttaswamy v. Union of India, 2017) recognizes the right to privacy, mental safety, and digital dignity as part of fundamental rights. Any modern cyber law must now protect not just the speaker, but the silent sufferer—especially women, children, journalists, whistleblowers, and vulnerable communities.

A Technological Imperative

Technology today is not a mere tool, but a weapon. Deepfakes, AI-generated child porn, virtual mob-likes, and anonymous bot armies require a law that understands:

- Real-time virality vs. harm permanence
- Intent and design (mens rea) in AI-based abuse
- Platform accountability and traceability
- Psychological profiling as digital harm

Example: The 2024 Lok Sabha TrollBot Campaign

Ahead of the 2024 elections, thousands of pro- and anti-party bots flooded X (formerly Twitter) and YouTube with fake polls, AI-fabricated speeches, and communal triggers. Despite takedown requests, most content remained viral for 72+ hours. There was no criminal liability assigned due to legal grey areas.

Internationally, Australia's eSafety Act, the UK's Online Safety Act (2023), and the EU Digital Services Act (DSA) have codified real-time, platform-sensitive, and victim-centric speech regulation frameworks. India, as the world's largest democracy and the second-largest online population, cannot afford to fall behind.

Why Redrafting Must Be Precise, Not Populist

A redrafted 66A must:

- Define harm clearly and narrowly (e.g., targeted cyber harassment, AI-fabricated impersonation)
- Be content-neutral but impact-sensitive
- Focus on intent, reach, and repetition (not just content)
- Include graded penalties, mental trauma indicators, and swift complaint mechanisms

Otherwise, we risk repeating the same mistakes of overbreadth, leading to another legal demise—or worse, the chilling of dissent again.

V. A Model Redraft of Section 66A – Balancing Freedom and Digital Safety

To legislate in the digital age is to walk a tightrope between liberty and liability. India's past attempt through Section 66A was constitutionally fatal due to its vagueness and subjectivity. Yet, the digital harms it attempted to address have only grown—morphing from mere online annoyance into a threat to democratic discourse, mental health, and bodily autonomy.

A modern redraft must meet the twin goals of constitutional validity and technological responsiveness, while avoiding overreach. Below is a model provision, carefully crafted with inspiration from international practices (e.g., UK's Online Safety Act, EU DSA), Indian constitutional values, and contemporary cyber threats.

Proposed Section 66AA – Targeted Online Harassment and Harm Using Digital Means

(1) Any person who, through any electronic communication:

(a) Intentionally threatens another with injury to body, liberty, or property;

(b) Publishes false information with the specific intent to cause incitement of violence or hatred against any group based on religion, race, gender, or community;

(c) Knowingly circulates material adjudicated as defamatory by a competent court,

shall be punished with imprisonment up to two years, or fine, or both.

(2) The following conditions apply:

(a) No arrest shall be made without prior approval from a police officer not below the rank of Deputy Superintendent of Police or Deputy Commissioner of Police.

(b) Notice of intended action must be given to the accused, and a reasonable opportunity to respond must be provided, unless there is imminent danger to public order.

(c) All complaints under this section must be forwarded to a Judicial Magistrate for preliminary review within 48 hours.

(3) Explanations:

(i) "Threat" means an express and specific intention to cause imminent unlawful harm.

(ii) "Incitement" means advocacy of unlawful action likely to imminently produce such action.

(iii) Genuine opinion, satire, parody, artistic works, political criticism are excluded unless meeting the standards above.

(4) This section shall be interpreted strictly in line with permissible restrictions under Article 19(2) of the Constitution of India.

Clauses if needed:

1. The offence shall be **cognizable and bailable** unless committed against a minor, woman, or vulnerable person, in which case it shall be **non-bailable**.

2. The central government may, in consultation with the Data Protection Board and Cyber Appellate Tribunal, notify rules for expeditious complaint redressal, forensic preservation of evidence, and platform compliance.

Illustrative Case Studies for Application

Case 1: "Fake My Voice" Scam – Delhi, 2023 A young woman's AI-cloned voice was used to call her fiancé's relatives for money transfer, claiming she was in danger. The trauma led to medical intervention. Current IPC laws could not effectively prosecute the digital impersonation.

Case 2: Schoolgirl Deepfake Porn – Hyderabad, 2022 A Class 11 student's face was morphed into explicit videos using a freely available app. The content went viral on Telegram groups, severely affecting her education and mental health. FIRs under Section 354C IPC and IT Act Section 67 failed to capture the nature of automated synthetic harm.

Case 3: Journalist Harassment Ring – India, 2023

Investigative female journalists were targeted using coordinated bot armies, fake profiles, and AI-generated voice notes. The police struggled to book perpetrators without a specific speech harm law.

VI. Conclusion & Recommendations

The Resurrection of Section 66AA—Constitutionally Grounded, Technologically Aware

The Supreme Court's striking down of Section 66A in Shreya Singhal v. Union of India (2015) was a landmark for free speech in India. Yet, in the decade since, digital communication has outpaced legal comprehension, and the

INDIAN JOURNAL OF LEGAL REVIEW [IJLR – IF SCORE – 7.58]
VOLUME 5 AND ISSUE 11 OF 2025
APIS – 3920 - 0001 *(and)* ISSN - 2583-2344
Published by
Institute of Legal Education
https://iledu.in

threats that 66A clumsily tried to address have now become smarter, faster, and more brutal.

From AI-generated deepfake pornography to political troll bots and AI-assisted identity thefts, the spectrum of online harm has evolved. What hasn't evolved, unfortunately, is our legal ability to differentiate online dissent from digital abuse, or harmless mischief from algorithmic assault.

A new law must not resurrect the sins of the past. Rather, it must surgically target real harm, protect constitutional values, and create a rights-based framework for both victims and speakers.

Key Recommendations

1. **Redraft Section 66A Based on Digital Harm, Not Offence**

Use clear, narrow definitions like "synthetic impersonation", "emotional distress", and "coordinated cyber harassment". Focus on intended harm, pattern, and medium, not vague emotions like "annoyance" or "offence".

Example: Unlike the original Section 66A, the redraft should not criminalize a sarcastic meme but should address someone using AI to threaten a woman with morphed images.

2. **Incorporate AI and Automation in Cyber Law**

The rise of LLMs, voice-cloning, and image-generators demands that Indian cyber law explicitly recognize automated and AI-generated content as tools for abuse—not just as passive mediums.

Case in Point: In 2024, an AI-generated fake speech attributed to a sitting MP went viral hours before a state election. It took Twitter 72 hours to pull it down. The ECI had no tools to act.

3. **Integrate with Platform Accountability Framework**

Mandate collaboration with platforms like Meta, X, YouTube, and AI app providers. Create traceability mandates and real-time redressal systems without compromising end-to-end encryption or free expression.

4. **Establish a Digital Harm Tribunal or Fast-Track Cyber Courts**

Victims often abandon legal recourse due to slow trial processes. A specialized Digital Safety Tribunal with cyber-psychological support, evidence preservation standards, and platform notices can improve redressal.

Case Study: In Bengaluru (2023), a cyberstalking victim was asked to print 250 screenshots and 3 hours of video evidence to lodge a complaint—highlighting the need for digitally native procedures.

5. **Mandatory Training for Police and Prosecutors**

Even where laws exist (e.g., Sections 354D, 509 IPC), enforcement is weak due to lack of tech training. Include modules on AI detection, metadata preservation, and cyber victim psychology in regular IPS and law officer training.

The Road Ahead

A country with over 850 million internet users, 30 crore social media accounts, and rising access to generative AI cannot afford a legal vacuum for cyber speech. The chilling effect of bad laws like 66A must not lead to silence in reform. We don't need a digital gag—we need a digital shield.

India's next cyber speech law must be clear enough for the citizen, strong enough for the abuser, and fair enough to pass constitutional muster. This is not the return of Section 66A. This is its redemption.

References

1. Shreya Singhal v. Union of India, (2015) 5 SCC 1 (India).
2. Justice K.S. Puttaswamy (Retd.) v. Union of India, (2017) 10 SCC 1 (India).
3. The Information Technology Act, 2000, No. 21, Acts of Parliament, 2000 (India).
4. The Indian Penal Code, 1860, No. 45, Acts of Parliament, 1860 (India).
5. Digital Services Act, Regulation (EU) 2022/2065 of the European Parliament

and of the Council of 19 October 2022 on a Single Market for Digital Services.
6. Online Safety Act 2023, c. 44 (UK).
7. eSafety Act 2021 (Cth) (Australia).
8. National Commission for Women, "Report on Online Abuse and Harassment of Women in India," (2023).
9. Ministry of Electronics and Information Technology, "Advisory on Deepfake and AI Abuse," Government of India (2024).
10. Press Trust of India, "AI-generated Voice Scams Rise in Urban India," Hindustan Times, July 2023.
11. The Election Commission of India, "Cyber Misinformation during 2024 General Elections: Advisory Note," (2024).
12. Centre for Internet and Society, "Platform Accountability and Digital Rights in India," (2022).