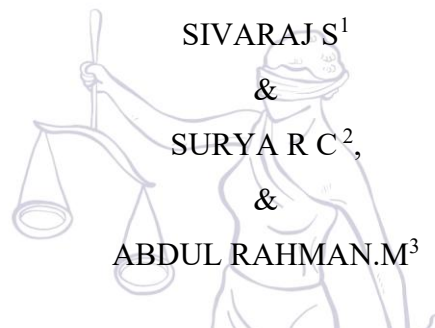


FREEDOM OF SPEECH IN THE INTERNET ERA: A COMPARATIVE LEGAL ANALYSIS OF THE INDIAN DIGITAL PUBLIC SQUARE

by



SIVARAJ S¹

&

SURYA R C²,

&

ABDUL RAHMAN.M³

ABSTRACT

The transition from analog to digital telecommunications has fundamentally disrupted traditional speech jurisprudence. While early internet discourse celebrated a decentralized, boundaryless forum for expression, modern online communication is mediated by centralized platform monopolies and heavily regulated by sovereign states. This research paper investigates the legal and constitutional dimensions of digital free speech in India under Article 19(1)(a) and the reasonable restrictions of Article 19(2) of the Constitution of India. It critically examines the shift from statutory safe harbour protections under Section 79 of the Information Technology Act, 2000, to proactive state-mandated censorship frameworks under the IT Rules of 2021 and 2023. Through a comparative legal analysis involving the United States' First Amendment doctrine through Section 230 CDA and the European Union's co-regulatory framework (Digital Services Act, 2022), this paper identifies structural vulnerabilities in Indian digital governance. It concludes with

¹ Author: Student of S. Thangapazham Law College, affiliated to Dr.Ambedkar Law University, Chennai, Tamilnadu,India. loken565655@gmail.com

² CoAuthor: Student of S. Thangapazham Law College, affiliated to Dr.Ambedkar Law University, Chennai, Tamilnadu,India. abdulrahuman6384@gmail.com

³ Coauthor: Student of S. Thangapazham Law College, affiliated to Dr.Ambedkar Law University, Chennai, Tamilnadu,India. suryaadv2003@gmail.com

actionable legislative, regulatory, and judicial reforms designed to protect constitutional speech in an increasingly algorithmic digital ecosystem.

Keywords: Freedom of Speech and Expression, Article 19(1)(a), Information Technology Act 2000, Intermediary Liability, Safe Harbour, Digital Services Act, First Amendment, *Shreya Singhal*, Content Moderation, Internet Shutdowns.

1. INTRODUCTION

1.1 Context and Background

Classical free speech doctrine, championed by philosophical traditions from John Milton to John Stuart Mill, rests on the ideal of an open "marketplace of ideas" where uninhibited debate allows truth to prevail over falsehood.⁴ In the late 20th century, cyberspace was heralded as the physical realization of this market—an incorporeal space naturally immune to governmental coercion.⁵

However, the architecture of the modern internet has inverted this paradigm. The digital public square is neither public nor decentralized; it is owned and operated by private multinational corporations whose platforms operate on algorithmic engagement loops that frequently reward sensationalism, polarization, and misinformation.⁶ Simultaneously, nation-states have developed sophisticated tools of digital sovereignty, shifting away from standard post-publication prosecution toward proactive online censorship, network shutdowns, and the delegation of policing duties to private intermediaries.⁷ The state often justifies these expansive powers as necessary tools to combat hate speech, mob violence, and digital radicalization, which are amplified by algorithmic ecosystems.⁸

⁴ John Stuart Mill, *On Liberty* (1859); John Milton, *Areopagitica: A Speech for the Liberty of Unlicensed Printing* (1644).

⁵ John Perry Barlow, *A Declaration of the Independence of Cyberspace*, Electronic Frontier Foundation (1996).

⁶ Shoshana Zuboff, *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power* (PublicAffairs 2019); Tarleton Gillespie, *Custodians of the Internet: Platforms, Content Moderation, and the Hidden Decisions That Shape Social Media* (Yale Univ. Press 2018).

⁷ Jack M. Balkin, *Old-School/New-School Speech Regulation*, 127 Harv. L. Rev. 2296 (2014).

⁸ *Tehseen S. Poonawalla v. Union of India*, (2018) 9 SCC 501

1.2 Statement of the Problem

In India, the tension between democratic discourse and digital governance has intensified. With over 800 million internet users, India represents one of the world's most dynamic digital markets. However, the constitutional guarantee of free expression under Article 19(1)(a) is increasingly strained by delegated legislation, ambiguous statutory blocking provisions under Section 69A of the Information Technology Act, frequent local network blackouts, and executive-driven fact-checking mechanisms. The fundamental legal problem lies in determining how to balance legitimate state security interests against individual expressive liberties without forcing private platforms into becoming state-coerced censors.

The scale of this executive intervention is substantial and growing. According to a parliamentary disclosure made by the Ministry of Electronics and Information Technology in December 2023, the Central Government restricted 7,502 accounts, websites, and URLs in 2023 alone under Section 69A of the IT Act.⁹ Between 2018 and 2023, a cumulative total of 36,800 URLs were subjected to blocking orders, representing an accelerating pattern of executive content removal that operates entirely outside any framework of pre-decisional judicial scrutiny or public justification. This numerical trajectory demonstrates that the structural tension between constitutional protections for online expression and the operational mechanics of Indian digital governance is not merely theoretical but is a large-scale, daily phenomenon.

2. Research Framework

2.1 Research Objectives

1. **To examine** the constitutional scope of digital free speech in India under Article 19(1)(a) and evaluate whether the reasonable restrictions under Article 19(2) are properly calibrated for the internet era.
2. **To evaluate** the judicial trajectory of digital rights in India, tracing the evolution from *Shreya Singhal v. Union of India* to *Anuradha Bhasin v. Union of India* and *Kunal Kamra v. Union of India*.

⁹ Freedom House, 'India: Freedom on the Net 2024' (Freedom House, 2024) <<https://freedomhouse.org/country/india/freedom-net/2024>> accessed 6 September 2026.

3. **To conduct a comparative doctrinal analysis** of digital speech governance by evaluating the laissez-faire approach of the United States and the fundamental rights/risk-management model of the European Union.
4. **To critique** the erosion of intermediary safe harbour protections under the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021, and its 2023 Amendments.
5. **To formulate** concrete policy, legislative, and institutional recommendations to ensure procedural due process, platform transparency, and robust free speech protections in India.



2.2 Research Hypotheses



Hypothesis 1 (H₁): Delegated legislation in India (specifically the IT Rules, 2021/2023) has systematically curtailed the safe harbour doctrine of Section 79, transforming private intermediaries into proactive, risk-averse censors and creating an impermissible chilling effect on protected speech.

Hypothesis 2 (H₂): Existing statutory mechanisms governing content takedowns (Section 69A) lack adequate procedural safeguards, natural justice protections, and transparency, thereby failing the proportionality test established in modern Indian constitutional jurisprudence and amounting to unconstitutional prior restraint.

Hypothesis 3 (H₃): Neither absolute platform immunity (U.S. Model) nor executive-heavy administrative censorship (Indian Model) provides an optimal equilibrium; rather, a procedural accountability and algorithmic transparency model (EU DSA Model) offers the most effective constitutional safeguard for digital expression.

2.3 Research Methodology

This paper adopts a **doctrinal and comparative legal research methodology**:

Primary Sources: The Constitution of India, 1950; Information Technology Act, 2000 (and subsequent amendments); Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021 & 2023; statutory provisions from the United States (47 U.S.C. § 230) and the European Union (Regulation (EU) 2022/2065 - Digital Services Act); and binding judicial precedents from the Supreme Court of India, the Bombay High Court, the U.S. Supreme Court, and the European Court of Human Rights (ECtHR).

Secondary Sources: Scholarly treatises, peer-reviewed law review articles, reports from independent digital rights organizations, and parliamentary standing committee reports.

Analytical Framework: The legal analysis applies constitutional tests developed by the Indian Supreme Court, specifically the tests of **arbitrariness (Article 14)**, **overbreadth and vagueness (Article 19(1)(a))**, and the **four-pronged proportionality test** (*Modern Dental College* and *Puttaswamy* standards).

2.4 Scope and Limitations

This study focuses on regulatory, statutory, and constitutional jurisprudence governing intermediary liability, state content-blocking regimes, and free speech online. While it touches upon data protection and privacy under the Digital Personal Data Protection Act (DPDPA), 2023, detailed technical evaluations of cryptographic standards, antitrust dynamics, and intellectual property enforcement fall outside the core scope of this paper.

3. Constitutional and Statutory Architecture of Digital Speech in India

3.1 Article 19(1)(a) vs. Article 19(2): The "Reasonable Restrictions" Test

The Constitution of India does not contain an express, separate provision for digital or press freedom; rather, speech across all mediums is protected under Article 19(1)(a). Unlike the near-absolute text of the First Amendment of the U.S. Constitution, Indian free speech is expressly constrained by the eight exhaustive grounds under Article 19(2): Sovereignty and integrity of

India, Security of the State, Friendly relations with foreign States, Public order, Decency or morality, Contempt of court, Defamation, and Incitement to an offence. As constitutional scholars have noted, Indian free speech jurisprudence has historically grappled with the tension between individual liberty and the state's paternalistic desire to preserve societal harmony.¹⁰

In *Superintendent, Central Prison, Fatehgarh v. Ram Manohar Lohia* (1960), the Supreme Court ruled that for a restriction under "public order" to be reasonable, the link between the prohibited speech and the anticipated disorder must be **proximate, direct, and immediate**, akin to a "spark in a powder keg," rather than far-fetched or hypothetical.¹¹ Applying this doctrine to cyberspace is complex because online speech can be archived, indexed, shared globally, and amplified instantaneously.

3.2 The Magna Carta of Digital Rights: *Shreya Singhal v. Union of India* (2015)

The foundational milestone of Indian digital jurisprudence is *Shreya Singhal v. Union of India*.^{12,13} The Supreme Court invalidated Section 66A of the IT Act, which criminalized the sending of information that was "grossly offensive" or had a "menacing character." The Court established three vital principles:

The Tripartite Distinction of Speech: The Court distinguished between *discussion*, *advocacy*, and *incitement*. Mere discussion or advocacy of an unpopular cause cannot be restricted; speech can only be curtailed when it reaches the threshold of clear incitement to an offence.

¹⁰ Gautam Bhatia, *Offend, Shock, or Disturb: Free Speech under the Indian Constitution* (Oxford Univ. Press 2016).

¹¹ *Superintendent, Central Prison, Fatehgarh v. Ram Manohar Lohia*, AIR 1960 SC 633 (India).

¹³ *Shreya Singhal v. Union of India*, (2015) 5 SCC 1 (India).

The Doctrine of Vagueness and Overbreadth: Section 66A was struck down because terms like "offensive" or "annoyance" were unconstitutionally vague, failing to provide clear boundaries for what citizens were permitted to say.

Reading Down Safe Harbour (Section 79): The Court read down Section 79(3)(b) of the IT Act to mandate that an intermediary loses safe harbour protection *only* if it fails to take down content after receiving actual knowledge by way of a court order or a formal government directive under **Section 69A**, completely eliminating intermediary liability based on private user complaints.

Despite the categorical invalidation of Section 66A, empirical evidence has documented a significant failure of implementation in its aftermath. Research by the Internet Freedom Foundation, drawing on data from the National Crime Records Bureau across eleven states, identified at least 1,307 cases registered under the unconstitutional provision after the Shreya Singhal judgment, making it one of the most extensively misused zombie provisions in Indian criminal law.¹⁴ The Supreme Court was subsequently compelled to intervene again in October 2022, issuing directions to all state governments, high courts, and lower courts to cease prosecutions under the provision and directing that the Shreya Singhal ruling be formally communicated through the judicial hierarchy. The persistence of Section 66A enforcement years after its judicial nullification illustrates the deep implementation gap between constitutional adjudication and ground-level enforcement in Indian digital law.

3.3 Access to Digital Space: *Anuradha Bhasin v. Union of India* (2020)

In *Anuradha Bhasin*, the Supreme Court reviewed the prolonged suspension of internet and telecommunication services in Jammu & Kashmir.¹⁵ The Court held:

¹⁴ Internet Freedom Foundation, 'SC's Direction: Stop Prosecuting People Under S.66A' (IFF, 12 October 2022) <<https://internetfreedom.in/sc-direction-stop-prosecuting-people-under-the-unconstitutional-s-66a/>> accessed 6 September 2026; Supreme Court Observer, 'Section 66A: The Dead Law That Still Haunts India' (SC Observer, 9 October 2023) <<https://www.scobserver.in/journal/section-66a-the-dead-law-that-still-haunts-india/>> accessed 6 September 2026.

1. The right to freedom of speech and expression under Article 19(1)(a) and the right to practice any profession or carry on any trade under Article 19(1)(g) over the medium of the internet are constitutionally protected fundamental rights.
2. Indefinite suspension of internet services is impermissible under the Temporary Suspension of Telecom Services (Public Emergency or Public Safety) Rules, 2017.
3. Any restriction on internet access must satisfy the **doctrine of proportionality**: it must pursue a legitimate state aim, be the least restrictive measure available, have a rational nexus to the objective, and not disproportionately impact fundamental liberties.



3.4 Section 69A and Confidential Blocking Regimes

Section 69A of the IT Act empowers the Central Government to issue directions to block public access to online information on grounds tracking Article 19(2). However, under Rule 16 of the Information Technology (Procedure and Safeguards for Blocking for Access of Information by Public) Rules, 2009, strict confidentiality is maintained regarding all blocking requests and actions.

This statutory confidentiality creates an administrative black box, which critics argue operates as an unconstitutional form of prior restraint.¹⁶ In *X Corp. v. Union of India* (2023), Twitter challenged several sweeping blocking orders issued by the Ministry of Electronics and Information Technology (MeitY) that targeted entire accounts rather than specific individual URLs.¹⁷ The Karnataka High Court dismissed the petition, imposing costs and affirming broad executive latitude. The absence of an open hearing or public justification prevents users from contesting unjust censorship and leaves publishers unaware of why their speech was suppressed.

The operational scale of this confidential blocking architecture has expanded considerably. Parliamentary records reveal that over 36,800 URLs were blocked under Section 69A between 2018 and 2023, with 7,502 new orders issued in 2023 alone, of which over 13,600 targeted content on X (formerly Twitter).¹⁸ The disproportionate targeting of a single platform's accounts, rather than specific infringing URLs, demonstrates a pattern of broad-brush executive content

¹⁶ *Brij Bhushan v. State of Delhi*, AIR 1950 SC 129

¹⁷ *X Corp. v. Union of India & Ors.*, W.P. No. 13710 of 2022 (Karn. H.C. June 30, 2023).

¹⁸ Freedom House, 'India: Freedom on the Net 2024' (Freedom House, 2024) <<https://freedomhouse.org/country/india/freedom-net/2024>> accessed 6 September 2026.

[management that the structural confidentiality of the regime places entirely beyond the reach of affected parties to contest or even identify.](#)

4. The Regulatory Shift: Intermediary Liability and State Censorship

The regulatory trajectory of intermediary liability in India demonstrates a systematic centralization of executive power. This shift originated from the conditional safe harbour protection under Section 79 of the IT Act, moved through the strict, proactive mandates of the IT Rules, 2021, and culminated in the highly controversial 2023 Amendments. Legal scholars observe that by weaponizing the threat of safe harbour revocation, the state effectively deputizes private platforms to police speech on its behalf, circumventing judicial scrutiny.¹⁹

4.1 The IT Rules 2021: Dilution of the *Shreya Singhal* Safe Harbour

Promulgated under delegated authority without parliamentary debate, the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021, fundamentally reorganized internet governance:

The Traceability Mandate (Rule 4(2)): Significant Social Media Intermediaries (SSMIs) providing messaging services must enable the identification of the "first originator" of information upon executive or judicial order. Major messaging platforms (such as WhatsApp) argued that compliance requires breaking end-to-end encryption (E2EE) by compromising security protocols or implementing client-side scanning, violating the fundamental right to privacy established in *K.S. Puttaswamy v. Union of India*.²⁰

Abridged Takedown Windows: The 2021 Rules impose aggressive compliance windows (24 hours for non-consensual intimate imagery; 36 to 72 hours for broader statutory categories). Faced with strict criminal and civil liability for non-compliance, intermediaries default to automated over-blocking of user content to preserve their corporate safe harbour.

¹⁹ Chinmayi Arun, *Gatekeeper Liability and Article 19(1)(a) of the Constitution of India*, 7 NUJS L. Rev. 73 (2014).

²⁰ *Justice K.S. Puttaswamy (Retd.) v. Union of India*, (2017) 10 SCC 1 (India).

The traceability mandate under Rule 4(2) has also generated significant constitutional litigation. In May 2021, WhatsApp LLC filed a writ petition before the Delhi High Court challenging Rule 4(2) as unconstitutional, arguing that compliance would require the platform to build and retain a record of the originator of every single message sent in India, which would necessitate breaking end-to-end encryption and fundamentally undermining user privacy.²¹ As of the time of writing, the petition remains pending before the Delhi High Court, having last been heard in August 2024, leaving both the platform and over 530 million Indian users in legal uncertainty regarding the constitutional status of the traceability obligation. The prolonged pendency of this challenge in the absence of any interim relief exemplifies the structural imbalance between the pace of executive digital regulation and the timelines of judicial oversight.

4.2 The 2023 Amendments & Fact-Checking Units: *Kunal Kamra v. Union of India* (2024)

In April 2023, MeitY amended Rule 3(1)(b)(v) of the IT Rules to require intermediaries to take down any information identified as "fake, false or misleading" with respect to "any business of the Central Government" by a state-appointed Fact-Check Unit (FCU). Non-compliance stripped the platform of Section 79 safe harbour protection.

The constitutional validity of this amendment was challenged in *Kunal Kamra v. Union of India* (and connected petitions by the Editors Guild of India and Association of Indian Magazines) before the Bombay High Court.²² Following a split verdict between Justice Gautam Patel and Justice Neela Gokhale, the third-referral judge, Justice A.S. Chandurkar, delivered the decisive opinion on September 20, 2024, holding the amendment unconstitutional:

²¹ LiveLaw, 'Traceability Rule Will Break End-To-End Encryption; Can Put Privacy Of Journalists, Activists, Politicians At Risk: WhatsApp Tells Delhi High Court' (LiveLaw, 10 June 2021) <<https://www.livelaw.in/news-updates/whatsapp-delhi-high-court-traceability-end-to-end-encryption-privacy-risk-174743>> accessed 6 September 2026; MediaNama, 'Delhi HC Flags Privacy Risks in WhatsApp Contact Access' (MediaNama, 8 April 2026) <<https://www.medianama.com/2026/04/223-delhi-hc-saving-number-whatsapp-police-right-privacy/>> accessed 6 September 2026.

²² *Kunal Kamra v. Union of India*, W.P.(L) No. 9792 of 2023

1. **Violation of Article 19(1)(a):** The rule placed the state as the sole arbiter of truth regarding its own affairs, denying citizens the right to criticize, question, or satirize government actions.
2. **Violation of Article 14:** It created an arbitrary classification by creating special protections exclusively for the speech and narrative of the Central Government while excluding all other public and private entities.
3. **Vagueness and Overbreadth:** Terms like "fake, false, or misleading" are undefined in the IT Act, creating an unconstitutional chilling effect on political commentary, investigative journalism, and democratic dissent.

The constitutional consequences of the Bombay High Court ruling remain contested at the apex court level. The Union of India filed a Special Leave Petition on 24 December 2024, seeking to reverse the judgment. While the Supreme Court issued notice in the matter, it declined to stay the High Court's ruling, thereby allowing the order striking down the Fact-Check Unit to operate pending final adjudication.²³ The pendency of this challenge before the Supreme Court means that the constitutional limits of state-appointed fact-checking in Indian digital governance remain an actively litigated and politically contested question, and that the Kunal Kamra judgment, while landmark, does not represent a final resolution of the underlying tension between executive content management and the constitutional guarantee of free expression.

5. Comparative Jurisprudential Analysis: Distinct Global Paradigms

To fully contextualize the Indian regulatory framework, it is necessary to examine the distinct legal philosophies governing the internet in other major democratic and authoritarian jurisdictions.

²³ Internet Freedom Foundation, 'Supreme Court of India issued notice but refused any stay in Union of India's challenge to the Bombay High Court judgement holding Fact Check Unit to be ultra vires' (IFF, March 2026) <<https://internetfreedom.in/supreme-court-of-india-issued-notice-but-refused-any-stay-in-union-of-indias-challenge-to-the-bombay-high-court-judgement-holding-fact-check-unit-to-be-ultra-vires/>> accessed 6 September 2026.

5.1 The United States: Section 230 and Laissez-Faire Immunity

The U.S. approach reflects First Amendment absolutism, where viewpoint discrimination by the state is strictly unconstitutional.^[44] Online platforms are governed by Section 230 of the Communications Decency Act (47 U.S.C. § 230):

Section 230(c)(1) ensures that "no provider or user of an interactive computer service shall be treated as the publisher or speaker of any information provided by another information content provider."

Section 230(c)(2) protects platforms from liability when they voluntarily act in good faith to restrict access to "obscene, lewd, lascivious, filthy, excessively violent, harassing, or otherwise objectionable" material.

This statutory shield decoupled platform moderation from publisher liability, giving platforms broad discretion to curate feeds, demote hate speech, or leave political discussions largely unregulated. While this approach protects expression from state interference, it leaves democratic discourse vulnerable to algorithmic radicalization, corporate monopolies, and coordinated disinformation campaigns, as analyzed in *Moody v. NetChoice, LLC* (2024).²⁴

5.2 The European Union: Fundamental Rights and the Digital Services Act (DSA)

The European Union rejects both absolute corporate immunity and direct executive censorship, operating under a human-rights-balancing doctrine anchored in Article 10 of the European Convention on Human Rights (ECHR).²⁵

The **Digital Services Act (Regulation (EU) 2022/2065)** represents a shift toward **procedural co-regulation and systemic risk management**:

²⁴ *Moody v. NetChoice, LLC*, 603 U.S.(2024); Tim Wu, *Is the First Amendment Obsolete?*, 117 Mich. L. Rev. 547 (2018).

²⁵ European Convention on Human Rights art. 10, Nov. 4, 1950; Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market For Digital Services (Digital Services Act), 2022 O.J. (L 277) 1.

Categorized Obligations: The DSA scales regulatory obligations based on platform size, imposing the strictest rules on Very Large Online Platforms (VLOPs) and Search Engines (VLOSEs) with over 45 million active monthly EU users.

Algorithmic Auditing and Risk Mitigation: VLOPs must conduct annual, independent risk assessments evaluating how their recommender systems and user-interface designs affect elections, public security, gender violence, and mental health.

Procedural Due Process: When removing content, platforms must provide a detailed "statement of reasons" to the affected user and support access to an internal complaint-handling system and out-of-court dispute settlement bodies.

No General Monitoring: The DSA expressly retains the prohibition against general monitoring obligations, preventing platforms from being forced into indiscriminate mass surveillance.

5.3 Authoritarian Cyber-Sovereignty: The Chinese Model

In contrast to democratic systems, authoritarian frameworks (exemplified by the People's Republic of China) operate on the principle of **cyber sovereignty**. Under the Cybersecurity Law of 2016 and Data Security Law of 2021, platforms are integrated directly into the state's security and ideological apparatus. Intermediaries must deploy strict real-name registration, enforce automated keyword filtering, and maintain absolute compliance with government directives to prevent the spread of "harmful information." The sovereign state maintains complete control over network boundaries via the Great Firewall.²⁶

²⁶ Ronald Deibert, *Black Code: Surveillance, Privacy, and the Dark Side of the Internet* (Signal Books 2013).

5.4 Comparative Synthesis

The ideological differences between these jurisdictions can be synthesized across several key regulatory metrics:

Constitutional Standard: The United States employs Strict Scrutiny, where the First Amendment fiercely prevents state content restrictions. The European Union relies on Proportionality, balancing Free Expression (Art. 10 ECHR) against human dignity and privacy. India utilizes the test of Reasonable Restrictions under Article 19(2), with proportionality doctrines applied by constitutional courts.

Safe Harbour Standard: The U.S. grants broad statutory immunity under CDA Section 230, allowing platforms to curate at will. The EU offers conditional safe harbour, attaching liability only upon a platform's failure to act on illegal content after receiving notice. India formally provides conditional safe harbour under Section 79 of the IT Act, but this has been heavily curtailed by the strict executive mandates of the IT Rules, 2021 and 2023.

State Oversight Mechanism: The U.S. features minimal direct state regulation over speech, with primary federal enforcement limited to consumer protection (via the FTC). The EU utilizes independent Digital Services Coordinators (DSCs) and the European Commission. India's oversight is overwhelmingly executive-directed, managed by the Ministry of Electronics and Information Technology (MeitY) and Inter-Ministerial Committees, with limited independent regulatory oversight.

User Redressal & Due Process: In the U.S., redressal is dictated entirely by private Terms of Service with no statutory right to appeal takedowns. The EU guarantees comprehensive statutory rights, including mandatory statements of reasons, internal appeals, and out-of-court disputes. India relies on Grievance Appellate Committees (GACs), which are heavily criticized for being executive-controlled appellate bodies.

Algorithmic Transparency: U.S. platforms protect their algorithms as proprietary trade secrets with minimal mandatory state disclosure. The EU mandates annual risk audits and vetted researcher access to algorithmic data for VLOPs. India currently lacks any mandatory algorithmic auditing frameworks for platform recommender systems.

6. Critical Analysis and Major Findings

6.1 Findings on Hypotheses

1. **Confirmation of H₁:** The research confirms that the IT Rules (2021–2023) have eroded the safe harbour protections established in *Shreya Singhal*. By conditioning intermediary immunity on tight takedown deadlines and compliance with broad, undefined categories, platforms default to proactive over-censorship, suppressing lawful speech to mitigate corporate liability.
2. **Confirmation of H₂:** The statutory architecture governing Section 69A blocking orders fails the *Puttaswamy* and *Anuradha Bhasin* proportionality tests. The blanket confidentiality mandated by Rule 16 of the 2009 Blocking Rules insulates executive decisions from meaningful judicial review and violates natural justice.
3. **Confirmation of H₃:** The comparative analysis demonstrates that the U.S. laissez-faire model is ill-equipped to curb systemic disinformation and algorithmic manipulation, while India's executive-heavy model risks structural authoritarian creep. The European Union's DSA provides the most balanced framework by focusing on systemic accountability, independent audits, and user due process without letting the executive dictate content truth.

Legal and Social Issues

The global speech governance spectrum reveals a stark contrast. The United States anchors the laissez-faire end of the spectrum, defined by market self-regulation and broad platform immunity. The European Union occupies the middle ground, prioritizing co-regulation, procedural due process, and systemic risk audits. Conversely, India is increasingly drifting toward the executive-driven end of the spectrum, characterized by delegated legislative control, confidential blocking orders, and state-appointed appellate committees.

6.2 Structural Vulnerabilities in India's Digital Architecture

Executive Centralization over Independent Oversight: The Grievance Appellate Committees (GACs) introduced under the 2022 IT Rules amendments are entirely staffed by central government appointees. This makes the executive the final appellate authority over speech decisions on social media, violating the core principle that the state cannot sit as an impartial judge in matters involving political dissent and public criticism.

The Normalization of Network Disruptions: India continues to record more localized internet blackouts than any other democratic nation.²⁷ Routine deployment of shutdown orders for law-and-order control or to prevent cheating in public examinations bypasses the high threshold of "public emergency or public safety" mandated by the Telegraph Act and *Anuradha Bhasin*.

Empirical data reinforces the severity of this pattern. According to Access Now's annual report, 'Emboldened Offenders, Endangered Communities: Internet Shutdowns in 2024', India imposed 84 internet shutdowns across 16 states and territories in 2024, the highest number recorded in any democratic nation that year.²⁸ Of those shutdowns, 41 were imposed in the context of protests, 23 during episodes of communal violence, and five during government recruitment examinations, with Manipur, Haryana, and Jammu and Kashmir accounting for the largest share. India had held the global record for the most shutdowns for six consecutive years from 2018, until Myanmar surpassed it for the first time in 2024. The sustained use of network blackouts at a scale unmatched among democracies represents a structural challenge to the necessity and proportionality principles articulated in *Anuradha Bhasin*.

²⁷ Software Freedom Law Center, India (sfli.in), *Internet Shutdowns Tracker*

²⁸ Access Now and #KeepItOn Coalition, 'Emboldened Offenders, Endangered Communities: Internet Shutdowns in 2024' (Access Now, 24 February 2025) <<https://www.accessnow.org/wp-content/uploads/2025/02/KeepItOn-2024-Internet-Shutdowns-Annual-Report.pdf>> accessed 6 September 2026.

7. Suggestions and Policy Recommendations

7.1 Structural Legislative Reforms to the Information Technology Act

Repeal and Replace Delegated Overreach: Parliament should replace the patchwork of delegated IT Rules with a unified, comprehensive **Digital Services and Intermediary Code**. This legislation must clearly re-anchor intermediary safe harbour to objective, statutory conditions that cannot be altered by executive notifications.

Codification of Strict Proportionality: The statutory grounds for content blocking under Section 69A must be amended to require that every blocking order specify the exact ground under Article 19(2), the evidence considered, and the reason less restrictive measures (such as labeling, warning tags, or demoting) were insufficient.

7.2 Introducing Transparency and Reforming Section 69A

Abolition of Blanket Confidentiality (Rule 16): Rule 16 of the 2009 Blocking Rules must be amended to establish a default of public transparency. Blocking orders, redacted for national security secrets where strictly necessary, should be published in a searchable, public repository to enable affected users and content creators to pursue judicial review under Article 226 or Article 32.

Mandatory Pre-Decisional Notice: Unless a genuine emergency exists (with reasons recorded in writing), the originator of the content must be given prior notice and a reasonable opportunity to be heard before a blocking order takes effect.

7.3 Adopting the European Model: Algorithmic Accountability and Risk Auditing

- **Independent Audits of Large Platforms:** India should mandate that Significant Social Media Intermediaries (SSMIs) submit to regular, independent audits evaluating how their engagement, ranking, and recommender algorithms affect user rights, public health, and social stability.

- **Researcher Data Access:** Regulated frameworks should be established to give independent academic researchers and accredited civil society organizations access to platform data to track disinformation networks and study systemic risks.

8. Conclusion

The modern digital ecosystem has disrupted the historical dynamic of free expression. Protecting freedom of speech and expression in the 21st century can no longer rely solely on shielding citizens from direct sovereign censorship; it requires defending public discourse against the dual risks of opaque corporate algorithms and overreaching executive control.

In India, constitutional protections established in *Shreya Singhal*, *Anuradha Bhasin*, and reinforced in *Kunal Kamra* show that the fundamental guarantees of Article 19(1)(a) apply fully in cyberspace. To prevent the digital public square from degrading into an arena of state-mandated narratives or corporate manipulation, Indian digital jurisprudence must move toward systemic transparency, independent regulatory oversight, and procedural due process. By learning from comparative models like the European Union's Digital Services Act, India can build a digital governance framework that protects national security and public order while preserving the robust, uninhibited speech essential to a constitutional democracy.



Indian Journal of Contemporary
Legal and Social Issues