
ADMINISTRATIVE NECESSITY OR EXECUTIVE OVERREACH: DECODING THE CONSTITUTIONAL MECHANICS OF SECTION 69A OF THE INFORMATION TECHNOLOGY ACT, 2000

Mitali Mishra, LLB, Dayanand College of Law, Kanpur University

ABSTRACT

The Section 69A of the IT Act, 2000 can be considered the core of the legal regime governing India's internet regulation (online content). It vests sovereign powers on the State enabling it to restrict access to internet content. Although this section was constitutionally justified in **Shreya Singhal v. Union of India (2015)** based on the procedural guarantees available, the present day use of this section demonstrates a growing disparity between the legislative intention and execution. In this paper, the constitutional dynamics of Section 69A will be analysed in order to ascertain whether its operation today amounts to an indispensable requirement of administration of the State for ensuring national security or executive overreach.

In the context of the changes in regulations including the abolishment of the intermediary safe harbor and the introduction of the notion of "architectural liability," this paper discusses the systematic violation of the principle of procedural fairness. The focus is on the **2009 Blocking Rules** under which the general confidentiality provision (**Rule 16**) and the frequent resorting to emergency powers (Rule 9) silence the right to audi alteram partem (hearing).¹

Through a test of these provisions in light of the proportionality doctrine laid down in **Justice K.S. Puttaswamy (Retd.) vs Union of India (2017) case**, this study shows how the obfuscation and heavy-handedness of such a procedure act as a deterrent to the fundamental right to freedom of speech and expression under **Article 19(1)(a)**. What the Journal seeks to say is that the obsolete structure of the IT Act is simply incapable of handling the modern realities of algorithmic filtering and encryption.

Keywords: Section 69A, Information Technology Act, Executive Overreach, Article 19(1)(a), Digital Rights, Proportionality Doctrine, Intermediary Liability, Architectural Blocking, National Security, Administrative Necessity.

¹ CSJMU Kanpur University

I. INTRODUCTION

In today's world, any criticism of the Indian Government through satirical memes, comedy is seen as a threat to the sovereignty and integrity of the nation, and the government uses its power to block the concerned social media accounts. This puts the arise in debate to a critical constitutional question Whether Section 69A of the IT Act is an administrative necessity of the Government of India in order to protect national interests in the age of technology or if it is a tool of executive overreach which enables the government to have too much control over the Internet. This is something which needs to be understood through the analysis of executive power, procedure, judicial review, and constitutional mechanics.

The phrase Administrative Necessity or Executive Overreach: Decoding the Constitutional Mechanics of Section 69A is the name of the dilemma that exists between granting the powers to the Indian State to regulate cyberspace to serve public interests and protecting fundamental rights from being violated and the constitutional constraints on executive power. Through this research, it is sought to know whether Section 69A is an administrative necessity under the Constitution or whether it can be used as an executive overreach in India.²

It is in the light of above scenario, this study hopes to provide an input into the discourse around digital constitutionalism in India. This study seeks to explore whether the provisions of Section 69A are a legitimate means of exercising administrative action or whether there is room for executive overreach within this provision. Through a constitutional analysis of legal and judicial reasoning, this study hopes to identify whether the exercise of blocking powers by virtue of Section 69A adheres to the principles of constitutional democracy.

II. EVOLUTION OF CYBER LAWS AND INTERNET REGULATION IN INDIA

Late 1990's encountered a drive for the development of cyber law in India, to create strict laws for probing internet usage. The Parliament passed the bill after getting the assent of the President on June 09, 2000, especially with an eye on the Act coming into force on October 17, 2000. With the IT Act, e-governance received a legal framework; electronic records and digital signatures were acknowledged; e-commerce was facilitated; and further 27 other types of cybercrimes were defined along with the penalties.

² Reports on internet censorship and blocking orders by Internet Freedom Foundation (IFF)

Foundational Era: The IT Act, 2000

India was ahead of many nations in terms of digital laws as it enacted the Information Technology (IT) Act, 2000 based on the model of the United Nations Commission on International Trade Law (UNCITRAL).

The IT Act 2000: Objectives and Provisions

An Act to provide legal recognition for transactions carried out by means of electronic data interchange and other means of electronic communication, commonly referred to as electronic commerce which involve the use of alternatives to paper-based methods of communication and storage of information, to facilitate electronic filing of documents with the Government agencies.

The IT Act 2000 sought to provide a legal basis for the process of e-governance by recognising electronic documents and digital signature in its provisions. The Act also defined various offenses in the cyber space and prescribed punishments for the same in order to facilitate e-commerce and counter cyber crimes.³

The Turning Point: The IT (Amendment) Act, 2008⁴

With the growing prevalence of data thefts and internet fraud, The IT Act, 2000 made substantial amendments to the original legislation in order to address new crimes.

- **Accountability of Companies:** Introduced **Section 43A** that mandated companies to ensure "reasonable security practices" regarding sensitive information about users.
- **Novel cybercrimes:** Criminalised identity theft, phishing, cyber-terrorism, and communication of offensive material on the internet (**Section 66A**).
- **Introduction of Safe Harbor:** Introduced **Section 79** ensuring intermediaries were not responsible for user-generated content provided they did due diligence.

³ Information Technology Act 2000, s 69A.

⁴ Information Technology Amendment Act 2008.

Intermediary Liability Era: IT Rules, 2021

In order to control misinformation, hate speech, and platform abuse, the government took an alternative route and implemented the IT (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021.

- **Tiered Significant Social Media Intermediaries (SSMIs):** Established a stringent tier of social media intermediaries with more than 5 million users.
- **Mandated Grievance Redressal Requirements:** Compelled the SSMIs to designate Indian employees as their Chief Compliance Officer and Grievance Officer.
- **Traceability Clause:** Made the encrypted messaging services trace and determine the "first originator" of malicious information at the command of the state.
- **Digital Media Code:** Subsumed the Over-the-Top (OTT) content providers and digital news publishers into a stringent three-tier regulatory system.⁵

III. JUDICIAL INTERPRETATION OF SECTION 69A

The fast-growing use of the Internet in India has changed the essence of governance. In this connection, the Indian judiciary has a key function of the interpretation of constitutional values and making sure that the government regulation of the internet space is consistent with the Constitution of India. The judicial influence on the governance of the Internet is determined by a balance between regulations and fundamental freedoms.

1. Shreya Singhal v. Union of India (2015)

Shreya Singhal v. Union of India (AIR 2015) represents an important judgment of the Supreme Court of India of the **Information Technology Act, 2000**. This decision helped redefine the scope of freedom of speech on the internet and made it clear that all forms of expression on the internet are protected by Article 19(1)(a) of the Indian constitution.

According to Justice Nariman, the **section 66A of the act** violates **Article 19(1)(a)** and cannot be justified under **Article 19(2)**. However, **sections 69A (blocking of websites) and 79**

⁵ Intermediary Liability Era: IT Rules, 2021

(liability of intermediaries) of the Act were found to be constitutional with procedural safeguards. The decision is considered a significant landmark in Indian constitutional law.⁶

2. Anuradha Bhasin v. Union of India (2020)

It was decided by the Supreme Court that internet connectivity is an essential component of freedom of speech and trade guaranteed under Article 19(1)(a) and 19(1)(g). Indefinite suspension of internet is not permissible and the orders must meet the criteria of proportionality. The authorities were asked to publish the orders and reconsider them after a period of time.

In this case, there was the first recognition by the Supreme Court that internet connectivity enjoys constitutional protection in relation to freedom of expression. It provided some procedural protections for restricting orders of executive action.⁷

3. X Corp. vs. Union of India (2025)

X (formally known as Twitter) questioned the Government's process of removal of content, claiming that it was circumventing the process laid out by Section 69A through other means. The Karnataka High Court ruled against the petition made by X Corp and supported the Government's blocking orders that Entire accounts can be blocked under Section 69A.

The court concluded that “any information generated, transmitted, received, stored or hosted” in Section 69A requires a purposive interpretation. In order to prevent any ongoing damage, the Government can block entire social media accounts, not just individual posts.⁸

IV. UNDERSTANDING SECTION 69A OF THE INFORMATION TECHNOLOGY ACT: CONSTITUTIONAL MECHANIC OF SECTION 69A

Section 69A empowers the Union Government to block the public from accessing “any information” on the internet when: (1) the Government believes it is “necessary or expedient”; and (2) it is in the interests of the defence, sovereignty, integrity, or security of India or its relations with foreign states, public order, or the incitement of a cognisable offence relating to

⁶ Shreya Singhal v Union of India (2015) 5 SCC 1.

⁷ Anuradha Bhasin v Union of India (2020) 3 SCC 637.

⁸ X Corp. vs. Union of India (2025)

these categories. When the government decides to block content, it must follow the procedure set out under the Information Technology (Procedure and Safeguards for Blocking for Access of Information by Public) Rules, 2009 (“Blocking Rules”).⁹

Constitutional Mechanics of Section 69A

The constitutionality of Section 69A was challenged and upheld by the Supreme Court in *Shreya Singhal v the Union* (2015)¹⁰. The Court observed that blocking could only be resorted to in the interests of the security or defence of India, public order etc., which the Court highlighted were the same interests Article 19(2) of the Constitution permitted free speech to be restricted on. According to the Court, this demonstrated that Section 69A restricted expression in line with constitutional standards on free speech. In other words, if the government’s decision to block specific content was ever in doubt as impermissibly restricting free speech, the blocking order in question could be challenged before a court under its writ jurisdiction.

Freedom of Speech and Expression under Article 19(1)(a)

- According to Article 19(1)(a), every individual is entitled to the right to freedom of speech and expression in India. The above-mentioned right is the foundation of the democratic system prevailing in India because it allows citizens to express their opinions, exchange thoughts, critique government actions, obtain information, and take part in civic matters.
- The digital era has broadened the above-mentioned right beyond the scope of conventional media into internet-based forums, social media, blogs, websites of news organizations, and other digital communication tools which constitute the digital public square.
- Over the years, the Supreme Court has adopted an expansive interpretation of the above-mentioned constitutional right as well as the right to receive and impart information through it.
- The reason why Article 19(1)(a) plays such a vital role when analysing Section 69A is the

⁹ Section 69A of the Information Technology Act 2000

¹⁰ *Shreya Singhal v Union of India* (2015) 5 SCC 1.

fact that every blockage infringes upon the right of citizens to information and debate.¹¹

Reasonable Restrictions under Article 19(2)

- The right under Article 19(1)(a) cannot be considered as absolute. According to Article 19(2), reasonable restrictions may be imposed on such rights in the interest of the sovereignty and integrity of India, the security of the State, friendly relations with foreign States, public order, decency or morality, contempt of court, defamation or incitement to an offence.
- Section 69A takes almost similar approach since it provides for the blocking of public access to any information through any computer resource if the Central Government considers it necessary or expedient so to do in the interest of the sovereignty or integrity of India, defense of India, security of the State, friendly relations with foreign States or public order.

Constitutional Morality in Digital Governance

- The principles of constitutional morality require that government action be governed not only by the authority of the law but also by the principles embodied in the Constitution, such as liberty, equality, dignity, transparency, accountability, and the rule of law.
- Under digital governance, constitutional morality dictates that any regulation of online speech shall not be employed for any form of political censorship or repression of legitimate dissent. This means that government action relating to the digital public sphere needs to strike a balance between national security and democracy through which restrictions shall be exceptional, reasonable, and proportionate.
- The principle is also concerned about transparency in government decision-making and accountability of the exercise of digital regulatory powers. With digital technology having a bearing on democratic participation, constitutional morality is the guiding principle in the interpretation and application of Section 69A.

V. ADMINISTRATIVE NECESSITY—JUSTIFICATION FOR SECTION 69A

Administrative necessity is another reason provided in support of the use of section 69A and is also heavily criticised by constitutional law scholars on the grounds that Section 69A is an

¹¹ Constitution of India bare act article 19, 21.

important “fire extinguisher” that is essential to deal with the modern digital crisis where traditional legal systems fail to cope up with the situation. The State can say that Section 69A of the Information Technology Act is not an arbitrary tool of censorship but a necessary one.

Combating the "New Dark Web"

In June 2026 government's regulatory authority orders to block Telegram amidst the NEET-UG re-examination controversy. According to some government sources telegram is using as source as an unregulated hub for syndicated cheating. Telegram's features like encrypted channels, editing capabilities in message, high capacity file sharing features. Fraudsters were allegedly exploiting this feature to alter historic messages, inserting actual exam papers into old posts after the fact to manufacture a false timeline of pre-exam leaks. Because the platform's architecture inherently frustrates surgical intervention, the State requires comprehensive authority, such as Section 69A, to suspend specific features or block entire platforms to safeguard institutional credibility.¹²

Cross-Border Jurisdiction and Cyber Warfare

There are international cybercrime gangs that perpetrate large-scale financial fraud. Since the perpetrators actually operate from outside India's jurisdiction, it is difficult for the state to easily arrest them or seize their servers. Mutual Legal Assistance Treaties (MLATs) are slow and politically complex. Therefore, the only administratively feasible defense is to force the intermediaries operating within India to act as a geographical firewall. Section 69A provides the legal teeth to mandate this compliance, granting intermediaries safe harbor immunity if they obey, and threatening criminal liability if they refuse.

Protecting Institutional Integrity

This has been made evident through the shift in the recent judicial philosophy where the wide application of Section 69A in response to massive coordination of leaks of national examinations has been noted. In the State's view, the reason behind the application of 69A is the need to protect important national institutions from a coordinated attack of digital sabotage.

¹² Telegram FZ LLC v Union of India (Delhi High Court, June 2026)

Asymmetric Information Warfare and Sovereignty

In modern day geopolitics, “the sovereignty and integrity of India” is often threatened from outside of its actual territory. The administrative structure is dependent upon Section 69A to deal with asymmetric warfare. As the State cannot launch raids against servers that are located in the enemy territories or those where cooperation may not be forthcoming, the only recourse left for the sovereign is to use Section 69A.

VI. EXECUTIVE OVERREACH CONSTITUTIONAL CONCERNS

The issue of executive overreach in the case of section 69A of the IT Act revolves around how a clause that was initially meant for limited censorship is increasingly being used as a general means of control. The central government relies on rule 16 of the Blocking Rules of IT ACT 2000 to block an entire online platform without even disclosing the reasons for such blocking to the creators.

The 2026 Paradigm Shift: From Content to Entire Platforms

The most prominent recent example of executive encroachment on authority through Section 69A is the decision in the case of Telegram FZ LLC v. Union of India by the Delhi High Court in June 2026. In the context of the dispute around the NEET-UG examination, the Central Government exercised its emergency powers to bar access to the whole Telegram network throughout India. The High Court justified the decision by declaring that any application can be considered as "information" in terms of the IT Act. Thus, Section 69A could be justified as constitutional from the perspective of being a scalpel to excise certain, unauthorised information. The executive can now rely on a court decision that would justify using the provision as a hammer to bar the whole network, which is not what legislators intended.

The Black Box of Rule 16: Denial of Natural Justice

The “procedural protections” that have “saved” Section 69A in 2015 are greatly weakened in view of Rule 16 of the 2009 Blocking Rules, which requires strict confidentiality of all blocking orders and measures.¹³ As long as the executive acts in complete secrecy, there is no administrative accountability at all. The content providers are often deprived of the opportunity

¹³ Rule 16 of the 2009 Blocking Rules under of the Information Technology (Procedure and Safeguards for Blocking for Access of Information by Public) Rules, 2009

to be heard before the decision-making and receive the reasons for it. Without being aware of the precise constitutional provision (Article 19(2)) used against them, citizens are left without a possibility of filing a petition under Article 226 of the Constitution.¹⁴

Absence of Independent Oversight

These decisions are subject to an appeals procedure through a "Review Committee" that has been set up under the regulations. The Review Committee comprises executive members only (namely, the Cabinet Secretary and other Secretaries from different ministries). There is no judicial member or ombudsman in the process of appeal.

VII. CHALLENGES IN THE PRESENT FRAMEWORK OF SECTION 69A of the INFORMATION TECHNOLOGY Act, 2000

The critical challenges plaguing the framework of Section 69A are outlined below.

Balancing with National Security and Civil Liberties

One of the most important challenges regarding Section 69A is maintaining a proper balance between to maintain the nation's security and constitutional rights of people. It cannot be denied that the State has a genuine concern for protection against sovereignty and integrity of nation.

From the constitutional perspective, the major problem is to make sure that the restrictions provided under Article 19(2) of the Constitution are not arbitrary because they can be seen as violating people's rights to freedom of speech and expression guaranteed by Article 19(1)(a) or Article 19(1)(g), and Article 21.

Platform Accountability

Digital platforms, including social media firms, have become important intermediaries for public discussions today. It is necessary to maintain a balance between adherence to legal directions from the government and safeguarding the constitutional rights of the citizens. Overadherence will result in censorship, but lack of adherence can threaten the safety of the public or even national security. The issue here is to find a regulatory regime that allows

¹⁴ Article 226 of Constitution of India

responsible governance without making companies tools of the government's will.¹⁵

Cross-Border Digital Regulation

The enforcement of digital regulations across borders is one of the greatest challenges for the IT Act 69A. Given that the internet crosses many jurisdictions, executing domestic take-down orders, responding to encryptions coming from beyond the Indian territory, and managing them in the light of international laws is very difficult.

Digital Rights and Privacy

The landmark decision of the Supreme Court recognising the right to privacy as a fundamental right in Justice K.S. Puttaswamy (Retd.) v. Union of India (2017) has had a major impact on digital governance in India. Restrictions placed on the use of Section 69A could have an indirect impact on many digital rights, such as: freedom of expression; privacy of information; right to information; freedom of association; participation in democracy through digital media.

VIII. RECOMMENDATIONS and REFORMS FOR SECTION 69A of INFORMATION TECHNOLOGY ACT 2000

Legislation relating to privacy

Privacy and protection of data are significant areas that must be considered in the contemporary world. In addition, it should also be noted that the absence of specific privacy legislation in India has become one of the major factors that led to the decrease in the amount of foreign investment and other business transactions for the country. It also became an obstacle to the development of electronic commerce. Thus, adoption of a law regulating issues connected with privacy becomes crucial nowadays. Therefore, it is highly recommended to adopt such statute as quickly as possible.

Law relating to Extraterritorial Jurisdiction

It has been observed that many instances of digital law violations involve computer systems operating across national borders, necessitating their monitoring. However, in India, Section 69A of the IT Act, 2000, addresses data breaches or cyber-related violations rather than cross-

¹⁵ WP(C) No. 12223/2021 Anivar Aravind v. Union of India

border (territorial) infractions. Therefore, there is a critical need for legislation addressing extra-territorial jurisdiction for offences committed and penalised under other statutes.

Ensure Audi Alteram Partem (Right to be Heard)

At present, the intermediary (platform) always gets an opportunity to be heard, whereas the person who created the material does not get the opportunity in most cases even though he is needed in Mandate pre-decisional hearings. In the case of emergency, where there is a need to take down the material immediately, there should be post-decisional hearing within 48 to 72 hours.

Amendment to Blanket Confidentiality (Rule 16)

The creation of a Transparency Register that will make the blocking orders public. However, in situations where there are significant national security concerns, certain sensitive information may be deleted from the register; however, the reasoning behind the block has to be published.

International Treaty Participation

The issue of cybercrime is a worldwide problem, as hackers and cyber criminals do not limit their actions to any geographical boundaries and therefore need cooperation on an international level. Therefore, India needs to take an active part in international treaties such as the Budapest Convention on Cybercrime or United Nations' treaty negotiations. Active participation in international treaties will assist India to become more involved in cyber diplomacy and to increase cooperation on an international level.¹⁶

IX. CONCLUSION

In this context, the key issue of focus in the research pertains to whether Section 69A can be termed as an administrative necessity or represents executive overreach. In relation to the same, it is important to note that the research shows that there is no answer to this question in absolute terms.

¹⁶ www.jetir.org (ISSN-2349-5162) research paper on Cyber Law in 2025: Challenges and Legal Responses in the Age of AI, Data Breaches, and Digital Governance

On the one hand, Section 69A is obviously an administrative necessity. It must be borne in mind that in today's world of technological revolution and cyber attacks, the government needs to have some legal provision which enables it to deal quickly with the situation of cyber attacks, terrorism, hate speech, child sexual abuse materials, misinformation about national security and other acts that affect public order. Without having any legal provision for the blocking of online content that may cause harm to people, the government would fail in its constitutional duty of protecting people and maintaining public order.

On the other hand, exercising such powers entails the risk of executive overreach if constitutional safeguards are not taken care of. Excessive secrecy, broad executive discretion, inadequate transparency, prolonged restrictions, and insufficient independent oversight may undermine fundamental rights guaranteed under Articles 14, 19, and 21 of the Constitution.

It is evident from the study that Section 69A of the Information Technology Act, 2000 has been framed for providing the Central Government with the power to deny public access to online information in case of issues relating to the sovereignty and integrity of India, defence, security of the State, friendly relations with foreign States, public order, or for preventing the commission of cognizable offences. This legislative framework has been seen as a critical response by the country to overcome the problems associated with the challenges of the digital age.

However, there are many difficulties in the current scenario. The secrecy associated with blocking orders, lack of public disclosure, executive dominance in decision-making, new technology like artificial intelligence and deepfakes, algorithmic moderation of contents, and transnational character of digital communications have revealed the inadequacies of the current legal framework. This means that despite being constitutionally valid, Section 69A needs regular reforms in order to keep pace with constitutional requirements and technological advancements.

REFERENCES

- Reports on internet censorship and blocking orders by Internet Freedom Foundation (IFF).
- Information Technology Act 2000, Section 69A.
- Information Technology Amendment Act 2008.
- Intermediary Liability Era: IT Rules, 2021.
- Shreya Singhal v Union of India (2015) 5 SCC 1.
- Anuradha Bhasin v Union of India (2020) 3 SCC 637.
- X Corp. vs. Union of India (2025).
- Section 69A of the Information Technology Act 2000.
- Constitution of India, bare act, Articles 19, 21.
- Telegram FZ LLC v Union of India (Delhi High Court, June 2026).
- Rule 16 of the 2009 Blocking Rules under of the Information Technology (Procedure and Safeguards for Blocking for Access of Information by Public) Rules, 2009
- Article 226 of Constitution of India.
- WP(C) No. 12223/2021 in Kerala High Court Anivar Aravind v. Union of India.
- WWW.JETIR.ORG (ISSN-2349-5162) research paper on Cyber Law in 2025: Challenges and Legal Responses in the Age of AI, Data Breaches, and Digital Governance.