KAMARAJ IAS ACADEMY
Only IAS Academy by Grandson of "Peruntholaivar Kamarajar"

Section 69A of the IT Act and the Telegram Controversy: Balancing Digital Security, Public Order and Fundamental Rights

Published On: 21-06-2026

Recent Developments:

- The **Delhi High Court** upheld the Union Government's temporary restriction on **Telegram** ahead of the **NEET-UG 2026 re-examination**, holding that the action was legally justified under **Section 69A of the Information Technology Act, 2000**.
- The Ministry of Electronics and Information Technology (**MeitY**) invoked emergency powers under the IT framework following recommendations from the **National Testing Agency (NTA)**, citing organized misuse of Telegram by examination fraud networks.
- The restriction remained effective until **22 June 2026**, while Telegram's message-editing feature was separately disabled until **30 June 2026** to prevent manipulation of examination-related content.
- The Court observed that the temporary restriction satisfied the legal requirements of necessity and proportionality in the specific circumstances of protecting examination integrity and maintaining public order.

Background of the Issue:

Why Did the Government Restrict Telegram?

- Authorities alleged that organized cheating networks were using Telegram channels, groups and automated bots to circulate leaked or fabricated examination material related to the NEET-UG re-examination.
- Investigative agencies highlighted misuse of Telegram's message-editing feature to alter previously posted messages and falsely create the impression that examination papers had been leaked before the conduct of examinations.
- The government argued that such activities threatened public order, examination integrity and public confidence in national competitive examinations.
- Telegram challenged the decision, contending that the restriction adversely affected more than **150 million users** in India and disproportionately impacted legitimate users.

Section 69A of the Information Technology Act, 2000:

Meaning and Scope:

- **Section 69A** empowers the Central Government or its authorized officers to direct any intermediary or agency to block public access to information hosted, transmitted, received or stored through computer resources.
- The provision constitutes one of the principal legal mechanisms available to the Government for regulating harmful online content.
- The power extends to digital platforms, websites, applications and online information resources under specified legal conditions.

- Blocking directions are legally binding upon intermediaries and service providers operating within India.

Grounds for Invoking Section 69A:

- **Sovereignty and Integrity of India**.
- **Defence of India**.
- **Security of the State**.
- **Friendly Relations with Foreign States**.
- **Public Order**.
- **Prevention of Incitement to the Commission of Cognizable Offences** connected with the above grounds.

Procedural Safeguards:

- Blocking orders must ordinarily follow a prescribed procedure under the **Information Technology (Procedure and Safeguards for Blocking for Access of Information by Public) Rules, 2009**.
- Authorities are generally required to record reasons in writing before issuing blocking directions.
- A review mechanism exists to examine the legality and necessity of blocking orders.
- The framework seeks to balance national security concerns with constitutional freedoms.

Emergency Blocking Powers under the 2009 Rules:

Rule 9 and Emergency Procedure:

- **Rule 9** permits the Government to bypass the normal pre-decisional hearing process in cases requiring immediate intervention.
- Emergency blocking directions may be issued when delay could result in significant harm to public interest.
- Such orders are subject to subsequent review by the designated committee.
- The Telegram restriction was implemented through this emergency route because authorities considered the threat to examination integrity to be immediate.

Judicial Position on Section 69A:

Shreya Singhal v. Union of India (2015):

- The **Supreme Court of India** upheld the constitutional validity of Section 69A while striking down Section 66A of the Information Technology Act.
- The Court observed that Section 69A contains procedural safeguards that reduce the possibility of arbitrary action.
- Written reasons, limited statutory grounds and review mechanisms were considered important constitutional protections.
- The judgment remains the foundational precedent governing online content-blocking powers in India.

Delhi High Court's Position in the Telegram Case:

- The Court held that the temporary restriction complied with statutory requirements under Section 69A.
- The Court accepted the Government's argument that extraordinary circumstances justified temporary intervention.
- The judgment reinforced the principle that digital platforms may be restricted when statutory conditions are satisfied.

Concerns Associated with the Telegram Restriction:

Proportionality and Fundamental Rights:

- Critics argue that restricting an entire platform because of the actions of a limited number of users raises concerns regarding the constitutional doctrine of proportionality.
- Millions of legitimate users, including students, businesses and content creators, depend upon the platform for communication and economic activities.
- Questions have been raised regarding whether targeted removal of harmful content could have achieved the same objective with fewer restrictions on lawful users.

Freedom of Speech and Expression:

- Digital platforms serve as important channels for exercising rights under **Article 19(1)(a)** of the Constitution.
- Temporary platform-wide restrictions may affect access to information and communication for individuals unconnected with unlawful activities.
- Civil society organizations have argued that broad restrictions must remain exceptional and narrowly tailored.

Addressing Symptoms Rather than Causes:

- Critics contend that examination paper leaks often arise from institutional vulnerabilities within examination systems.
- Platform restrictions alone cannot eliminate systemic weaknesses in examination administration.
- Long-term reforms require stronger examination security mechanisms, digital monitoring and institutional accountability.

Why is Telegram Referred to as the "New Dark Web"?

Features Facilitating Misuse:

- Hidden identities and encryption features can complicate law-enforcement investigations.
- Certain communication channels allow large-scale dissemination of information with limited visibility to regulators.
- Automated bots can facilitate rapid coordination and mass distribution of content.
- Large file-sharing capacity enables circulation of high-resolution documents, databases and multimedia content.
- Message-editing capabilities have been exploited to manipulate digital records and create misleading narratives regarding examination leaks.

Cybercrime and Financial Fraud Concerns:

- Government agencies have reported increasing cybercrime complaints linked to Telegram-based networks.
- Criminal groups have allegedly used the platform for financial fraud, money laundering, extortion and illegal gambling activities.
- Encrypted communication channels may be exploited by organized cybercriminal syndicates for operational secrecy.

Dark Web: Meaning and Characteristics:

What is the Dark Web?

- The **Dark Web** is a concealed segment of the internet that cannot be accessed through conventional search engines.
- Specialized software such as **The Onion Router (Tor)** is generally required for access.
- Traffic is routed through multiple encrypted layers to conceal user identities and locations.
- Strong anonymity protections make attribution and investigation significantly more difficult.

Difference between Deep Web and Dark Web:

- The **Deep Web** consists of online content not indexed by search engines but accessible through standard browsers using valid credentials or direct links.
- The **Dark Web** requires specialized access tools and intentionally conceals user identity and location.
- Not all Deep Web content is illegal, whereas the Dark Web is frequently associated with illicit marketplaces and anonymous criminal activity.

Legitimate Uses of the Dark Web:

- Protection of whistle-blowers and investigative journalists.
- Secure communication in authoritarian environments.
- Privacy protection for activists and vulnerable groups.
- Intelligence gathering and cybercrime investigations by law-enforcement agencies.

Challenges Posed by the Dark Web:

- Anonymous trade in drugs, weapons and counterfeit products.
- Distribution of ransomware, malware and cyberattack tools.
- Facilitation of money laundering through cryptocurrencies.
- Difficulty in enforcing jurisdiction across national boundaries.

India's Approach to Cyber Governance and Digital Security:

Institutional and Legal Measures:

- The **Information Technology Act, 2000** provides the foundational legal framework for cyberspace governance.
- The **Indian Computer Emergency Response Team (CERT-In)** serves as the national nodal agency for cybersecurity incident response.
- The **Indian Cyber Crime Coordination Centre (I4C)** strengthens cybercrime investigation and coordination.
- The **Digital Personal Data Protection Act, 2023** contributes to the evolving framework for digital governance and privacy protection.

International Cooperation:

- Cybercrime investigations increasingly require cross-border cooperation due to the transnational nature of digital networks.
- India promotes cooperation through multilateral forums such as **BRICS**, **G20**, **Shanghai Cooperation Organisation** and the **United Nations**.
- Information sharing, cyber forensics and legal cooperation remain essential for combating online criminal networks.

Way Forward:

Balancing Security and Digital Rights:

- Regulatory interventions should remain proportionate, transparent and subject to effective judicial review.
- Governments should prioritize targeted content removal and platform cooperation wherever feasible.
- Examination security systems should be strengthened through encryption, digital audits and real-time monitoring.
- Intermediaries should develop robust mechanisms for detecting coordinated criminal misuse.

- Greater transparency regarding blocking orders can improve public trust while preserving national security interests.

Value Addition for UPSC:

Important Terms:

- **Section 69A:** Statutory provision empowering the Government to block public access to online information under specified conditions.
- **Intermediary:** Digital platform that hosts, transmits or enables access to user-generated information.
- **Rule 9:** Emergency provision permitting immediate blocking without prior hearing in exceptional circumstances.
- **Dark Web:** Encrypted and anonymous segment of the internet requiring specialized access tools.
- **Deep Web:** Non-indexed internet content accessible through ordinary browsers using direct access credentials.
- **Tor:** Privacy-focused network that routes internet traffic through multiple encrypted layers