



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

BitChat Takedown Rekindles Debate over Digital Privacy, National Security, Due Process and Free Speech in India

Published On: 29-07-2026

Recent Developments:

- The **Indian Cyber Crime Coordination Centre (I4C)**, under the **Ministry of Home Affairs**, directed **GitHub** to disable repositories hosting **BitChat**, a decentralised Bluetooth mesh messaging application developed by **Jack Dorsey**, citing concerns relating to national security, lawful interception and public order.
- The notice was issued under **Section 79(3)(b) of the Information Technology Act, 2000**, read with **Rule 3(1)(d) of the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021**, directing removal of three repositories within three hours.
- The action has triggered a nationwide debate on the balance between **digital privacy, freedom of speech, cybersecurity, national security and procedural safeguards** governing online content regulation.

About BitChat:

Features and Working Mechanism:

- **BitChat** is a **decentralised peer-to-peer messaging application** that operates through **Bluetooth mesh networking** without requiring internet connectivity, mobile networks or centralised servers.
- Every connected device simultaneously functions as both a **client** and a **relay node**, forwarding encrypted messages across multiple nearby devices to expand communication range.
- The application does not require **phone numbers, user registration or centralised data storage**, making communication resistant to network disruptions and server failures.
- The platform remains operational during **internet shutdowns, natural disasters, emergency situations and low-connectivity environments**, thereby improving communication resilience.

Government's Concerns Regarding BitChat:

Security and Law Enforcement Challenges:

- The Government argues that anonymous and decentralised communication significantly limits **lawful interception, attribution and criminal investigation** capabilities.
- Authorities have expressed concern that such platforms may facilitate **organised crime, terrorism, violent protests, misinformation campaigns, radicalisation and activities affecting national sovereignty and public order**.
- The Government also considers decentralised mesh communication capable of bypassing conventional internet restrictions and surveillance mechanisms during emergency situations.

Legal Framework Governing the Takedown:

Section 79(3)(b) of the Information Technology Act, 2000:

Kamaraj IAS Academy

Plot A P.127, AF block, 6 th street, 11th Main Rd, Shanthi Colony, Anna Nagar, Chennai, Tamil Nadu 600040

Phone: **044 4353 9988 / 98403 94477 / Whatsapp : 09710729833**

- **Section 79** provides **safe harbour protection** to intermediaries for third-party content, subject to compliance with statutory obligations.
- Under **Section 79(3)(b)**, an intermediary loses safe harbour protection if it fails to remove unlawful content after receiving actual knowledge through a court order or lawful government notification.
- The present order invoked this provision together with **Rule 3(1)(d)** of the **Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021**.

Section 69A and Blocking Rules, 2009:

- **Section 69A** specifically empowers the Government to block public access to online information in the interests of **sovereignty, integrity, defence, security of the State, friendly relations with foreign States or public order**.
- The **Information Technology (Procedure and Safeguards for Blocking for Access of Information by Public) Rules, 2009** require **recorded reasons, opportunity of hearing and periodic review**, providing greater procedural safeguards than Section 79-based takedown notices.
- The distinction between intermediary liability and statutory blocking powers has emerged as a central issue in the present controversy.

Important Judicial Pronouncements:

Shreya Singhal v. Union of India (2015):

- The Supreme Court declared **Section 66A** of the Information Technology Act unconstitutional for violating **freedom of speech and expression**.
- The Court clarified that intermediaries are required to remove online content only upon receiving **court orders or lawful government directions issued through due process**.
- The judgment recognised that online expression enjoys the same constitutional protection as offline speech and warned against arbitrary restrictions producing a **chilling effect**.

Anuradha Bhasin v. Union of India (2020):

- The Supreme Court held that restrictions on internet access must satisfy the doctrine of **proportionality** and remain **necessary, reasonable and temporary**.
- The Court emphasised that restrictions should be proportionate with respect to **territorial scope, duration, urgency and legitimate public purpose**, while remaining subject to periodic review.

Criticism of the Takedown Order:

Procedural and Constitutional Concerns:

- Critics argue that the order relies primarily on the **potential misuse of the technology** rather than identifying any specific unlawful content contained in the repositories.
- Digital rights organisations contend that restricting an entire communication platform merely because it could potentially be misused raises concerns regarding **due process, proportionality and freedom of expression**.
- Questions have also been raised regarding the use of **Section 79(3)(b)** instead of the more procedurally robust **Section 69A** mechanism.

Significance of the Issue:

Governance and Cybersecurity Dimensions:

- The controversy highlights the growing governance challenge of regulating **decentralised digital technologies** that operate beyond conventional communication infrastructure.

- It reflects the increasing tension between **individual privacy, encrypted communications and legitimate national security requirements**.
- The issue also demonstrates the need for clear legal standards governing **digital platforms, intermediary liability, open-source software and emerging communication technologies**.

Constitutional and Technological Significance:

- The matter directly involves balancing **Article 19(1)(a)** guaranteeing freedom of speech with the **reasonable restrictions** permitted under **Article 19(2)**.
- It also raises broader concerns regarding **digital rights, technological innovation, internet governance, cyber resilience and democratic accountability**.
- The emergence of decentralised communication platforms indicates that future cybersecurity regulation must increasingly address **distributed digital ecosystems** rather than conventional server-based services.

Way Forward:

Strengthening Digital Governance:

- Develop a comprehensive legal framework specifically addressing **decentralised communication technologies**, balancing innovation with national security requirements.
- Ensure greater transparency, procedural fairness and judicial oversight in content-blocking and intermediary liability decisions.
- Strengthen institutional capacity for **cyber forensics, lawful digital investigations and privacy-preserving surveillance technologies**.
- Promote international cooperation for regulating emerging digital platforms while protecting constitutional rights and technological innovation.
- Encourage periodic review of cyber laws to keep pace with developments in **distributed networks, encryption technologies and open-source software ecosystems**.

Value Addition for UPSC:

Important Constitutional, Legal and Institutional Linkages:

- **Article 19(1)(a):** Freedom of Speech and Expression.
- **Article 19(2):** Reasonable Restrictions relating to sovereignty, security of the State and public order.
- **Article 21:** Protection of Life and Personal Liberty, including informational privacy as recognised in **Justice K.S. Puttaswamy v. Union of India (2017)**.
- **Information Technology Act, 2000:** Sections 69A, 79 and intermediary liability framework.
- **Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021:** Due diligence obligations of intermediaries.
- **Indian Cyber Crime Coordination Centre (I4C):** National cybercrime coordination platform under the Ministry of Home Affairs.
- **GS Paper II:** Fundamental Rights, Governance, Digital Governance, Judiciary and Government Policies.
- **GS Paper III:** Cyber Security, Internal Security, Science & Technology, Data Governance and Emerging Technologies.
- **Keywords:** Decentralisation, Bluetooth Mesh Network, End-to-End Encryption, Intermediary Liability, Safe Harbour, Due Process, Proportionality, Digital Privacy, Internet Governance, Cyber Security, Open-Source Software, Lawful Interception.