

## Indian Laws and Blocking of Internet Content: Centre vs Twitter

## Why in News

Recently, the **government of India reprimanded Twitter (micro-blogging website) for not complying with its order to block more than a thousand accounts** for alleged spread of provocative content and misinformation on the **farmers' protest**.

## TOTAL 709 ACCOUNTS DEACTIVATED

- ➤ Of 257 handles that had originally tweeted with the hashtag #ModiPlanning-FarmerGenocide, 126 have been deactivated
- ➤ Of 1,178 handles that government suspected to have links with Khalistani, Pak elements to spread misinformation and provocative content, 583 deactivated

IT ministry said 'motivated campaigns' on platform and hashtag around PM were being run to 'abuse, inflame and create tension in society on unsubstantiated grounds'

of action under IT Act
Section 69A[3], under which
senior company officials can be
jailed for up to 7 years, apart
from financial penalty

## **Key Points**

- Current Issue:
  - The Centre has issued notice to the micro-blogging site after it restored more than 250 accounts that had been suspended earlier on the government's 'legal demand'.
  - The government wants the platform (Twitter) to comply with its earlier order of 31<sup>st</sup>
     January, 2021 by which it was asked to block accounts and a controversial hashtag
     that spoke of an impending 'genocide' of farmers for allegedly promoting misinformation
     about the protests, adversely affecting public order.
  - The micro-blogging site reinstated the accounts and tweets on its own and later refused to go back on the decision, contending that it found no violation of its policy.
- Law Related to Blocking of Internet Services/Content:
  - Information Technology Act, 2000:

- In India, the <u>Information Technology (IT) Act, 2000</u>, as amended from time to time, governs all activities related to the use of computer resources.
- It covers all **'intermediaries'** who play a role in the use of computer resources and electronic records.
- The **role of the intermediaries** has been spelt out in separate rules framed for the purpose in 2011- **The Information Technology (Intermediaries Guidelines) Rules, 2011.**
- Section 69 of the IT Act:
  - It confers on the Central and State governments the **power to issue directions "to intercept, monitor or decrypt any information** generated, transmitted, received or stored in any computer resource".
  - The grounds on which these powers may be exercised are:
    - In the interest of the sovereignty or integrity of India, defence of India, the security of the state.
    - Friendly relations with foreign states.
    - Public order, or for preventing incitement to the commission of any cognizable offence relating to these.
    - For investigating any offence.
- Process of Blocking Internet Websites:
  - Section 69A, for similar reasons and grounds (as stated above), enables the Centre to ask any agency of the government, or any intermediary, to block access to the public of any information generated, transmitted, received or stored or hosted on any computer resource.
  - Any such request for blocking access must be based on reasons given in writing.
- Intermediaries as per the IT Act 2000:
  - Intermediary is defined in **Section 2(1) (w)** of the IT Act 2000.
  - The term 'intermediaries' includes providers of telecom service, network service, Internet service and web hosting, besides search engines, online payment and auction sites, online marketplaces and cyber cafes.
  - It includes any person who, on behalf of another, "receives, stores or transmits" any electronic record. Social media platforms would fall under this definition.
- Obligations of Intermediaries under the Law:
  - Intermediaries are required to preserve and retain specified information in a manner and format prescribed by the Centre for a specified duration.
    - Contravention of this provision may attract a prison term that may go up to three years, besides a fine.
  - When a direction is given for monitoring, the intermediary and any person in charge
    of a computer resource should extend technical assistance in the form of giving access or
    securing access to the resource involved.
    - Failure to extend such assistance may entail a **prison term of up to seven** years, besides a fine.
    - Failure to comply with a direction to block access to the public on a government's written request also attracts a prison term of up to seven years, besides a fine.
- Liability of Intermediaries:
  - Section 79 of the IT Act 2000 makes it clear that "an intermediary shall not be liable for any third-party information, data, or communication link made available or hosted by him".

- **Third party information** means any information dealt with by a network service provider in his capacity as an intermediary.
- This **protects intermediaries** such as Internet and data service providers and those hosting websites **from being made liable** for content that users may post or generate.
- Sections 79 also introduced the concept of "notice and take down" provision.
  - It provides that an **intermediary would lose its immunity** if upon receiving actual knowledge or on being notified that any information, data or communication link residing in or connected to a computer resource controlled by it is being used to **commit an unlawful act** and it fails to expeditiously remove or disable access to that material.
- Supreme Court's Stand Related to Intermediaries in IT Act 2000:
  - In Shreya Singhal vs Union of India (2015), the <u>Supreme Court</u> read down the provision to mean that the intermediaries ought to act only upon receiving actual knowledge that a court order has been passed, asking [them] to expeditiously remove or disable access to certain material.
- Reason for Intermediaries to Show Compliance to IT Act:
  - International Requirement:
    - Most nations have framed laws mandating cooperation by Internet service providers or web hosting service providers and other intermediaries to cooperate with law and order authorities in certain circumstances.
  - To Fight Cybercrime:
    - Cooperation between technology services companies and law enforcement agencies is now deemed a vital part of fighting cybercrime and various other crimes that are committed using computer resources.
    - These cover hacking, digital impersonation and theft of data.
  - To Prevent Misuse of Internet:
    - The potential of the misuse has led to law enforcement officials constantly seeking to curb the ill-effects of using the medium.

Source:TH

PDF Refernece URL: https://www.drishtiias.com/printpdf/indian-laws-and-blocking-of-internet-content-centre-vs-twitter