CENTER BLOCKS 200 ONLINE PLATFORMS UNDER SECTION 69(A) OF IT ACT

The Ministry of Electronics and Information Technology (MeitY) recently issued orders to block 138 online betting platforms and 94 money lending apps on an "urgent" and "emergency" basis under Section 69(A) of the Information Technology Act, 2000. The decision was based on a recommendation of the Ministry of Home Affairs (MHA), which had received inputs from central intelligence agencies that some of the sites and apps were allegedly linked to China and contained "material prejudicial to the sovereignty and integrity of India".

What is The Danger Posed by Lending Apps?

Over the past three years, several police complaints have been received of extortion and harassment from people who borrowed small amounts through such money-lending apps, often at exorbitantly high interest rates. In December 2020, DNM Santosh Kumar, a native of Visakhapatnam, died by suicide allegedly after facing harassment by lending apps. Similarly, the Cyber Police Station of Pune received 699 complaints of loan app crimes in 2020. The number increased to 928 in 2021. As many as 3,151 complaints were filed against the loan app operatives till August 2022. Following this, the MHA started investigating Chinese loan-lending apps and found out that while only 94 are available on e-stores, others are operating through third-party links or websites.

What is Section 69 of the IT Act?

- Section 69 of the IT Act allows the government to issue content-blocking orders to online intermediaries such as Internet Service Providers (ISPs), telecom service providers, web hosting services, search engines, online marketplaces, etc.
- However, the Section requires the information or content being blocked to be deemed a threat to India's national security, sovereignty, or public order.
- As per the law, If the Centre or state government are satisfied that blocking the content is "necessary" and "expedient" on grounds of -

1. Sovereignty or integrity of India, defense of India,
2. Security of the State,
3 Friendly relations with foreign States or public order or
4 For preventing incitement to the commission of any cognizable offense relating to above or for investigation of any offense,"
5. It may, for reasons to be recorded in writing, direct any agency "to intercept, monitor or decrypt or cause to be intercepted or monitored or decrypted any information generated, transmitted, received or stored in any computer resource,"

What is the procedure to block such apps?

Since 2009, the MeitY has possessed blocking powers similar to those of the Ministry of Information & Broadcasting. Although MeitY derives these powers from the IT Act, it is the Information Technology (Procedure and Safeguards for Blocking for Access of Information by Public) Rules, 2009 or the IT Rules, 2009, which explain the process to issue such orders. The IT Rules include provisions such as review committees, the opportunity for a fair hearing, strict confidentiality, and maintenance of records by designated officers. However, there are no recorded instances of the MeitY providing individuals with pre-decisional hearings even while blocking non-emergency content.

Information Technology Act, 2000

It was enacted by the Indian Parliament in 2000. It is the primary law in India for matters relating to cybercrime and e-commerce. The Act was also enacted to give legal sanction to electronic commerce and electronic transactions, enable e-governance and prevent cyber crime. Under this law, foreign nationals can also be charged for any offense involving a computer or network located in India. The law prescribes punishment for various cyber crimes and frauds through digital/electronic format. It also gives legal recognition to digital signatures.

Other Key Points of IT Act 2000

- The Government enacted the original IT Act in the year 2000. Intermediary has been defined in section 2(1) (w) of the IT Act 2000. The term 'intermediary' includes providers of telecommunication services, network services, internet services and web hosting, apart from search engines, online payment and auction sites, online marketplaces and cyber cafes. This includes any person who "receives, stores or transmits" any electronic record on behalf of another. Social media platforms would come under this definition.
- The Information Technology Intermediate Guidelines (Amendment) Rules were first issued in 2011 and in 2018 the government made some changes in those rules. This section covers intermediary liability. Section 79 (2) (c) of the Act states that intermediaries shall exercise due care while discharging their duties, and shall also comply with such other guidelines as may be prescribed by the Central Government. In 2018, there was an increase in the number of mob lynchings due to fake news and rumors and messages being circulated on social media platforms like WhatsApp.
- Section 79: This is now at the heart of the ongoing intermediary liability battle between the Center and micro-blogging platform Twitter, which defines key rules for the relationship between governments and commercial internet platforms. Section 79 states that no intermediary shall be held liable, legally or otherwise, for any third party information, data, or communication link made available or hosted on its platform.

What have the courts said?

In a landmark 2015 ruling, the Supreme Court in "Shreya Singhal vs Union of India" struck down Section 66A of the Information Technology Act of 2000, which entailed punishment for sending offensive messages through communication services, etc. "Section 66A of the Information Technology Act, 2000 is struck down in its entirety being violative of Article 19(1)(a) and not saved under Article 19(2)," the Court held.

The plea had also challenged Section 69A of the Information Technology Rules 2009, but the SC held this to be "constitutionally valid". "It will be noticed that Section 69A unlike Section 66A is a narrowly drawn provision with several safeguards. First and foremost, blocking can only be resorted to where the Central Government is satisfied that it is necessary to do so. Secondly, such necessity is relatable only to some of the subjects set out in Article 19(2). Thirdly, reasons have to be recorded in writing in such blocking order so that they may be assailed in a writ petition under Article 226 of the Constitution," the Court noted.

The debate over Section 69A was revisited in July 2022 when Twitter sued the MeitY in the Karnataka HC over blocking orders that failed to adhere to the procedural requirement of giving users a hearing. In response, the Centre told the HC that Twitter was a foreign corporation and did not have any fundamental right or legal remedy. After that, Twitter clarified that their arguments under Articles 14, 19, and 21 were in relation to the rights of the citizens who had Twitter accounts. On February 8, the most recent date of hearing in this matter, the Centre questioned Twitter's locus standi to argue the fundamental rights of account holders and also questioned what the jural relationship between Twitter and its account holders would be.

What are some other instances of the government using Section 69A?

Following cross-border tensions with China, the MeitY banned 59 apps on June 29, 2020, including TikTok, Shareit, Shein, Xiaomi Mi Community, Clash of Kings, Weibo, Likee, etc. Similarly, on September 1, 2020, the government banned 118 apps, including the gaming app PUBG, followed by another ban on 49 apps on November 19, 2020.

More recently on February 14, 2022, the MHA recommended a ban on 54 Chinese mobile applications, including the popular game Garena Free Fire, a Singapore-based app, invoking Section 69A on account of possible concerns surrounding privacy issues and security threats.

Expected Question

Que. In India, which of the following is legally mandated to report cyber security incidents?

1. Service provider
2. Data centers
3. Body corporate

Select the correct answer using the code given below :

(a) 1 only

(b) 1 and 2 only

(c) 3 only

(d) 1, 2 and 3

Answer : D

Mains Expected Question & Format

Que.: State the importance of Information Technology Act, 2000 in maintaining the security and privacy of the country and suggest measures to make it more effective?

Answer Format :

- Why was the Information Technology Act brought?
- State the importance of this act in maintaining the security and privacy of the country.
- Suggest ways to make this act more effective
- Give a balanced conclusion considering its need at present.

Note: - The question of the main examination given for practice is designed keeping in mind the upcoming UPSC mains examination. Therefore, to get an answer to this question, you can take the help of this source as well as other sources related to this topic.