

5. Section 79 of the it Act Of 2000

Prelims Level: Information Technology

Mains Level: GS-III Awareness in the fields of IT, Space, Computers, Robotics, Nano-Technology, Bio-Technology and issues relating to Intellectual Property Rights.

Why in News?

- The Supreme Court held that internet intermediaries like Google cannot be protected from criminal defamation cases registered against them prior to October 27, 2009.

About:

- It was only on October 27, 2009 that Parliament amended the Information Technology Act of 2000 to protect online intermediaries from liability for criminally defamatory content published in them by third parties.
- The amended Section 79 of the 2000 Act provided that “an intermediary shall not be liable for any third party information, data, or communication link made available or hosted by him.”
- The amendment gave almost blanket protection to intermediaries from legal action under Section 499/500 (criminal defamation) of the Indian Penal Code.

Who is the Intermediary?

- “Intermediary” is defined in Section 2(1) (w) of the Information and Technology Act 2000.
- "Intermediary" with respect to any particular electronic message means any person who on behalf of another person receives stores or transmits that message or provides any service with respect to that message.
- The liability of the intermediaries is lucidly explained in section 79 of the Act.
- There are different kinds of internet intermediaries which fall into two categories: “conduits” and “hosts”.
- “Conduits” are technical providers of internet access or transmission services. “Hosts” are providers of content services – for instance, online platforms and storage services.

Too big, too fast

What the government said in the Supreme Court on the Internet traffic and the role of intermediaries

■ Internet offers information on a mind-boggling variety of subjects. High speed and high volume render pre-censorship difficult

■ Viewers exercise choice as to what content they wish to view or read. There is automatic uploading without any application of mind on the part of the website/platform



■ 3.5 billion people in the world accessed the Internet in 2015

■ 3 million photographs were uploaded on Facebook per day

■ 510 comments, 2,93,000 statuses are posted per minute

What is the Concern?

- With concerns over “rising incidents of violence and lynching in the country due to misuse of social media platforms and Child Pornographic Contents in Social Media Platforms” there is now need for online platforms to shoulder the “responsibility, accountability and larger commitment to ensure that its platform is not misused on a large scale to spread incorrect facts projected as news and designed to instigate people to commit crime”.

The Information Technology [Intermediaries Guidelines (Amendment) Rules] 2018:

- Social media intermediaries should publish rules, privacy policy to stop users from engaging in online material which is pedophilic, pornographic, hateful, racially and ethnically objectionable, invasive of privacy, etc.
- The online intermediaries should provide information or assistance within 72 hours when asked by any government agency for reasons of State security, cyber security, investigation, detection, prosecution or prevention of offenses.
- These offenses may include mob violence, lynching, online sexual abuse, etc. The “originator of the information” can be traced to register an FIR.
- The social media intermediaries should take all reasonable measures to protect individual privacy as required under the Information Technology Rules of 2011.
- The online intermediaries should appoint in India, a nodal person of contact for 24X7 coordination with law enforcement agencies and ensure compliance with their orders.
- Online Intermediaries should remove or disable access to unlawful content, within 24 hours, relatable to Article 19(2) of the constitution of India such as in the “interests of the sovereignty and integrity of India, the security of the State, friendly relations with foreign States, public order, decency or morality, or in relation to contempt of court, defamation or incitement to an offense.” The intermediary is also expected to preserve such information and associated records for at least 180 days for investigation purposes.
- The intermediary should deploy technology based automated tools for identifying and removing or disabling public access to unlawful information or contents.
- The intermediary should report cyber security incidents with the Indian Computer Emergency Response Team.
- On their website, the intermediary should publish the name of the Grievance Officer and his contact details and the mechanism by which users or any victim who suffers can notify their complaints against such usage.

Supreme Court Orders:

- These draft rules are in line with various judgments given by the Supreme Court (SC) to deal with malicious online content.
- In July 2018 judgment in the Tehseen S. Poonawalla case, the SC gave the government full freedom to stop/curb dissemination of “irresponsible and explosive messages on various social media platforms, which have a tendency to incite mob violence and lynching of any kind.”
- In December 2018 in Re: Prajwala Letter case, the SC ordered the government to frame the necessary guidelines/Standard Operating Procedure (SOP) and implement them to “eliminate child pornography, rape and gang rape imagery, videos, and sites in content hosting platforms and other applications”.

