Information Technology Act, 2000

Important enactments of the Indian Parliament are crucial topics coming under the polity and governance segments of the UPSC syllabus. The Information Technology Act, 2000, also known as the IT Act, 2000 in short, is an important legislation that is frequently referred to in the daily news. In this article, you can read the salient features of the act and also about the controversial Section 66A of the act.

IT Act, 2000

The Information Technology Act, 2000 was enacted by the Indian Parliament in 2000. It is the primary law in India for matters related to cybercrime and e-commerce.

- The act was enacted to give legal sanction to electronic commerce and electronic transactions, to enable e-governance, and also to prevent cybercrime.
- Under this law, for any crime involving a computer or a network located in India, foreign nationals can also be charged.
- The law prescribes penalties for various cybercrimes and fraud through digital/electronic format.
- It also gives legal recognition to digital signatures.
- The IT Act also amended certain provisions of the Indian Penal Code (IPC), the Banker's Book Evidence Act, 1891, the Indian Evidence Act, 1872 and the Reserve Bank of India Act, 1934 to modify these laws to make them compliant with new digital technologies.
- In the wake of the recent Indo-China border clash, the Government of India banned various Chinese apps under the Information Technology Act. Read more about this in an RSTV titled, 'TikTok, Other Chinese Apps Banned'.

IT Act - 2008 Amendments

The IT Act, 2000 was amended in 2008. This amendment introduced the controversial Section 66A into the Act.

Section 66A

- Section 66A gave authorities the power to arrest anyone accused of posting content on social media that could be deemed 'offensive'.
- This amendment was passed in the Parliament without any debate.
- As per the said section, a person could be convicted if proved on the charges of sending any 'information that is grossly offensive or has menacing character'.
- It also made it an offence to send any information that the sender knows to be false, but for the purpose of annoyance, inconvenience, danger, obstruction, insult, injury, criminal intimidation, enmity, hatred or ill-will, through a computer or electronic device.
- The penalty prescribed for the above was up to three years' imprisonment with fine.

Arguments against Section 66A

- Experts stated that the terms 'offensive', 'menacing', 'annoyance', etc. were vague and ill-defined or not defined at all.
- Anything could be construed as offensive by anybody.
- There was a lot of scope for abuse of power using this provision to intimidate people working in the media.
- This also curbed the freedom of speech and expression enshrined as a fundamental right in the Constitution.

- The section was used most notably to arrest persons who made any uncharitable remarks or criticisms against politicians.

The government contended that the section did not violate any fundamental right and that only certain words were restricted. It stated that as the number of internet users mushroomed in the country, there was a need to regulate the content on the internet just like print and electronic media. The Supreme Court, however, in 2015, struck down this section of the IT Act saying it was unconstitutional as it violated Article 19(1)(a) of the Constitution. This was in the famous **Shreya Singhal v Union of India case (2015)**.

Section 69A

- Section 69A empowers the authorities to intercept, monitor or decrypt any information generated, transmitted, received or stored in any computer resource if it is necessary or expedient to do so in the interest of the sovereignty or integrity of India, defense of India, the security of the State, friendly relations with foreign states or public order or for preventing incitement to the commission of any cognizable offence or for investigation of any offence.
- It also empowers the government to block internet sites in the interests of the nation. The law also contained the procedural safeguards for blocking any site.
- When parties opposed to the section stated that this section violated the right to privacy, the Supreme Court contended that national security is above individual privacy. The apex court upheld the constitutional validity of the section. Also read about privacy laws and India.
- The recent banning of certain Chinese Apps was done citing provisions under Section 69A of the IT Act.
- **Note:-** The Indian Telegraph Act, 1885 allows the government to tap phones. However, a 1996 SC judgement allows tapping of phones only during a 'public emergency'. Section 69A does not impose any public emergency restriction for the government.

Information Technology Intermediary Guidelines (Amendment) Rules, 2018

The Rules have been framed under Section 79 of the Information Technology Act. This section covers intermediary liability.

- Section 79(2)(c) of the Act states that intermediaries must observe due diligence while discharging their duties, and also observe such other guidelines as prescribed by the Central Government.
- **Online Intermediaries:**
    - An intermediary is a service that facilitates people to use the Internet, such as Internet Services Providers (ISPs), search engines and social media platforms.
    - There are two categories of intermediaries:
        - Conduits: Technical providers of internet access or transmission services.
        - Hosts: Providers of content services (online platforms, storage services).
- Information Technology Intermediary Guidelines (Amendment) Rules were first released in 2011 and in 2018, the government made certain changes to those rules.
- In 2018, there was a rise in the number of mob lynchings spurred by fake news & rumours and messages circulated on social media platforms like Whatsapp.
- To curb this, the government proposed stringent changes to Section 79 of the IT Act.

What do the Rules say?

- According to the 2018 Rules, social media intermediaries should publish rules and privacy policy to curb users from engaging in online material which is paedophilic, pornographic, hateful, racially and ethnically objectionable, invasive of privacy, etc.

- The 2018 Rules further provide that whenever an order is issued by the government agencies seeking information or assistance concerning cybersecurity, then the intermediaries must provide them the same within 72 hours.
- The Rules make it obligatory for online intermediaries to appoint a 'Nodal person of Contact' for 24X7 coordination with law enforcement agencies and officers to ensure compliance.
- The intermediaries are also required to deploy such technologies based on automated tools and appropriate mechanisms for the purpose of identifying or removing or disabling access to unlawful information.
- The changes will also require online platforms to break end-to-end encryption in order to ascertain the origin of messages.
- Online Intermediaries are required to remove or disable access to unlawful content within 24 hours. They should also preserve such records for a minimum period of 180 days for the purpose of investigations.

Rationale behind the Rules

- The government intends to make legal frameworks in order to make social media accountable under the law and protect people and intermediaries from misusing the same.
- The government wants to curb the spread of fake news and rumours, and also pre-empt mob violence/lynching.
- There is a need to check the presentation of incorrect facts as news by social media, that instigates people to commit crimes.

There has been **criticism of the Rules** from certain quarters, that says that the State is intruding into the privacy of the individual. Some also say that this law widens the scope of state surveillance of its citizens. These criticisms are notwithstanding the fact that the new Rules are in line with recent SC rulings.

- Tehseen S. Poonawalla case (2018): SC said that authorities have full freedom to curb the dissemination of explosive and irresponsible messages on social media, that could incite mob violence and lynchings.
- Prajwala Letter case (2018): SC ordered the government to frame the necessary guidelines to "eliminate child pornography, rape and gang rape imagery, videos, and sites in content hosting platforms and other applications".