Ending encryption – Traceability Provision in Intermediary Guidelines

What is the issue?

- The Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules 2021 recently came into force.
- WhatsApp has moved the Delhi High Court against the rules, especially the traceability clause; here is a look at the various aspects of it.

What is the traceability rule?

- It applies to significant social media intermediary providing services primarily in the nature of messaging.
- A "significant social media intermediary" is one with more than 50 lakh registered users.
- These "shall enable the identification of the first originator of the information on its computer resource as may be required by a judicial order."

Why has WhatsApp challenged this?

- For compliance and traceability, WhatsApp will have to break its end-to-end encryption service.
- The encryption service allows messages to be read only by the sender and the receiver.
- Its argument is that the encryption feature allows for privacy protections.
- So, breaking it would mean a violation of privacy.

What are the concerns?

- The question to be asked is whether the traceability guidelines (by breaking encryption) are vital to law enforcement in cases of harmful content.
- The problem with enforcing traceability is that, there are no safeguards like any independent or judicial oversight.
- So, government agencies could seek any user's identity on vague grounds.
- This could compromise the anonymity of whistle-blowers and journalistic

sources acting in public interest.
- It fundamentally undermines users' right to privacy.

What is the government's stance?

- The traceability measure will be used by law enforcement as the "last resort."
- It will come by only in specific situations.
- These may include prevention, detection, investigation, prosecution or punishment of an offence related to the sovereignty and integrity of India.
- Child sexual abuse material, punishable with imprisonment could also be a case.
- The assertion suggests that this requirement is in line with the Puttaswamy judgment.
- The judgement clarified that any restriction to the right of privacy must be necessary, proportionate and include safeguards against abuse.

Is there no other alternative?

- The Government, as the law stands now, can already seek access to encrypted data.
- It is provided under Section 69(3) of the IT Act, and Rules 17 and 13 of the 2009 Surveillance Rules.
- These require intermediaries to assist with decryption when they have the technical ability to do so.
- It is carried out when law enforcement has no other alternative.
- Besides, the government can still seek unencrypted data, metadata and digital trails from intermediaries.

What is the way forward?

- The Government needs to revisit its position on traceability commitments of intermediaries.
- It could instead revise the IT Act, 2000 in line with existing global best practices.
- Besides, the government should finalise the long-pending Data Protection Bill.

Source: The Hindu

SHANKAR
IAS PARLIAMENT
Information is Empowering