

General Studies-2; Topic– Government policies and interventions for development in various sectors and issues arising out of their design and implementation.

Surveillance Framework in India

1) Introduction

- Recently the Ministry of Home Affairs issued an order authorising 10 Central agencies to intercept, monitor, and decrypt “any information generated, transmitted, received or stored in any computer.”
- The notification was described as an incremental step towards a surveillance state.

2) MHA Order

- According to the order, any person in charge of the computer resource will be bound to extend all facilities and technical assistance to the agencies and failing to do will invite seven-year imprisonment and fine.
- The MHA gave the authorisation under 69 (1) of the Information Technology Act, 2000.
- The act says that the Central government can direct any agency after it is satisfied that it is necessary to do so in the “interest of the sovereignty or integrity of India, defence of India, security of the state, friendly relations with foreign states or public order or for preventing incitement to the commission of any cognizable offence relating to above or for investigation of any offence.”

3) Concerns Raised

- Only data in motion could be intercepted earlier.
- But now data revived, stored and generated can also be intercepted as powers of seizure have been given.
- The sweeping powers given to agencies to snoop phone calls and computers without any checks and balances is extremely worrisome. This is likely to be misused.

4) Surveillance Framework in India

- Two statutes control the field: telephone surveillance is sanctioned under the 1885 Telegraph Act (and its rules), while electronic surveillance is authorised under the 2000 Information Technology Act (and its rules).
- The procedural structure in both cases is broadly similar, and flows from a 1997 Supreme Court judgment.
- Surveillance requests have to be signed off by an official who is at least at the level of a Joint Secretary.

5) Problems with the Present Regime

- Current regime is bureaucratised.
- Decisions about surveillance are taken by the executive branch (including the review process), with no parliamentary or judicial supervision.
- The fact that an individual will almost never know that she is being surveilled.
- The surveillance regime is vague and ambiguous.
- Under Section 69 of the IT Act, the grounds of surveillance have been lifted from Article 19(2) of the Constitution, and pasted into the law.
- The regime is opaque.

- There is almost no information available about the bases on which surveillance decisions are taken, and how the legal standards are applied.

6) Arguments in favour of Surveillance

- The right to privacy is not absolute.
- Surveillance is essential to ensure national security and pre-empt terrorist threats.
- It is in the very nature of surveillance that it must take place outside the public eye.
- The regime is justified as it strikes a pragmatic balance between the competing values of privacy and security.

7) Arguments against Surveillance

- Heavily bureaucratized and minimally accountable regime of surveillance does not enhance security, but does have significant privacy costs.
- For example, while examining the U.S. National Security Agency's programme of mass surveillance, an American court found that out of more than 50 instances where terrorist attacks had been prevented, not even a single successful pre-emption was based on material collected from the NSA's surveillance regime.
- Such a system often has counterproductive effects
- A government that is not checked in any meaningful way will tend to go overboard with surveillance.
- In the process it can gather so much material that actually vital information can get lost.

8) Way Forward

- In its 2017 judgment, the apex court had asked the government to always carefully and sensitively balance individual privacy and the legitimate concerns of the state.
- Any impingement upon the right to privacy must be proportionate.
- The government's action must be the least restrictive method. i.e., protecting national security — by a smaller infringement upon fundamental rights.
- There must be parliamentary oversight over the agencies that conduct surveillance.
- All surveillance requests must go before a judicial authority, which can apply an independent legal mind to the merits of the request.
- Every surveillance request must mandatorily specify a probable cause for suspicion.
- To implement the suggestions above will require a comprehensive reform of the surveillance framework in India.
- In India, we have the Supreme Court's privacy judgment, which has taken a firm stand on the side of rights.
- Citizens' initiatives such as the Indian Privacy Code have also proposed legislative models for surveillance reform.
- We now need the parliamentary will to take this forward.