## 4. Using Call data is to Improve Quality and not for Surveillance

**Prelims Syllabus:** Policies

**Mains Syllabus:** GS-III Challenges to internal security through communication networks, role of media and social networking sites in internal security challenges, basics of cyber security; money-laundering and its Prevention.

### Why in News?

- Bulk call data records (CDR) being sought by the Department of Telecommunications (DoT), was only being collected to analyse and improve the quality of telecom services and not for any form of surveillance, says Government.

### What is the Issue?

- Some local units of the DoT "continue to seek voluminous CDR details from the licensees on regular basis in contravention" of the standard operating procedure for providing CDRs to law enforcement agencies.
- In a reply, the DoT said that given the numerous complaints about quality of service on the country's telecommunications networks including call drops, echo, cross connections, incomplete or poor caller experience, the DoT had developed a software tool to analyse big data and accurately ascertain call drops in any area.
- For this purpose, data on calls made from mobiles in any tower coverage area is analysed to ascertain calls terminated within 30 seconds and made again.
- The government stressed that this data was anonymous and did not contain the names of either the maker or receiver of calls.
- It is alleged that there is infringement of privacy of an individual which is the violation of the Fundamental Right under Article 21.
  - ✓ The right to privacy is protected as an intrinsic part of the right to life and personal liberty under Article 21 and as a part of the freedoms guaranteed by Part III of the Constitution.

### Is there any Legal Backup for such provision?

- The Government is empowered under **Rule 419 of the Indian Telegraph Rules, 1951**, to access such anonymous data for improving network quality.
- Any authorisation of such access to call drop data can be approved only by very senior officers.

- Further, it has been decided to seek such data only for short time period i.e. three to six hours normally covering the peak load of traffic on the network for any cell tower.

## What are the Concerns Regarding Surveillance?

- Surveillance is done as per due process of law; that any interception, monitoring, decryption of computer resource is done only by authorised agencies and with approval of competent authority; to prevent unauthorised use of these powers by any agency, individual or intermediary so that the right to privacy of citizen is not violated.

## Who are Empowered for Surveillance?

- The Ministry of Home Affairs (MHA), in December 2018, issued an order authorising ten security and intelligence agencies of the country to access any information stored in any computer for the purpose of monitoring, decrypting and interception.
- The 10 agencies include **Intelligence Bureau, Narcotics Control Bureau, Enforcement Directorate, Central Board of Direct Taxes, Directorate of Revenue Intelligence;, Central Bureau of Investigation, National Investigation Agency Cabinet Secretariat (RAW), Directorate of Signal Intelligence (For service areas of Jammu & Kashmir, North-East and Assam only), and Commissioner of Police, Delhi**.

## Why Surveillance Needed?

- Surveillance is necessary in the modern world where modern tools of information communication, including encryption are used. Surveillance is done only in the defence of India, to maintain public order, etc.
- There are grave threats to the country from terrorism, radicalisation, cross border terrorism, cybercrime, drug cartels", and these cannot be ignored or under-stated. There is a need for "speedy collection of actionable intelligence" to counter threat to national interests.

## How it is against the judgement of Supreme Court's right to privacy?

- SC in **Puttuswamy judgment** had asked the government to always carefully and sensitively balance individual privacy and the legitimate concerns of the state.
- Government has clarified that existing processes will be followed and every case of interception would continue to require permission from the home secretary and review by a panel headed by the cabinet secretary. However, even these processes do not have adequate safeguards against misuse.

- An individual may not even know if her electronic communications are being intercepted or monitored. If such surveillance comes within the person's knowledge, due to the obligation to maintain confidentiality and provisions in the **Official Secrets Act**, the person would not be able to know the reasons for such surveillance. This can make surveillance provisions prone to misuse.