Safeguards for Lawful Interception of Union

Government notified the **Telecommunications (Procedures and Safeguards for Lawful Interception of Messages) Rules, 2024 that allows interception in India.**

Key provisions of New Rules 2024

- **Legal Basis**: Notified under Section 56 of the **Telecommunications Act, 2023**. Supersedes **Rules 419 & 419A** of the Indian Telegraph Rules, 1951.
- **Authorised Agencies**: The **Central Government** may authorize agencies to **intercept messages** in case of a **public emergency** or **public safety concerns**, with approval from the **Competent Authority**.

Legality of interception in India

- **Telecommunication Act 2023:** It repealed Indian Telegraph Act 1885 and Indian Wireless Telegraph Act 1933, which allowed the government to monitor communications.
    - It provides for intercepting telecom devices on occurrence of any **public emergency or in interest of public safety**.
- **Information Technology (IT) Act 2000:** It allows interception of **all electronic transmission of data.**
    - **Section 69** empowers central or state government to intercept or monitor or decrypt any information generated, transmitted, received or stored in any computer resource.
    - **IT (Procedure and Safeguards for Interception, Monitoring and Decryption of Information) Rules 2009** provides that the **competent authority may authorise an agency of the Government** to intercept, monitor or decrypt information generated, transmitted, received or stored in any computer resource.
- **People's Union for Civil Liberties (PUCL) vs Union of India (1996) Case:** Supreme Court held that **phone tapping is an infringement on the right to freedom of speech and expression** under Article 19 of the Constitution.

- However, it is **permissible only** if it comes within the grounds of **restrictions under Article 19(2)**.

Concerns with Interception Rules

- **Privacy Concerns:** Telecommunication Act's **definition** of telecommunications as the "transmission, emission, or reception of any messages, by wire, radio, optical, or other electromagnetic systems" is so **broad** that it could **cover all mobile phone traffic**, including Internet-based activity.
  - This could extend interception orders to encrypted messaging platforms like WhatsApp, **bringing encrypting systems under surveillance**.
- **Lack of clarity:** Lack of definition of public emergency and public order may allow the state to justify intercepting communications **for trivial or politically motivated reasons** rather than legitimate national security concerns.
- **Concentration of powers:** It gives officials of similar rank within the **executive branch the power to both issue and review** interception orders, **undermining impartiality** in the review process.
  - It creates an environment where **politically motivated or unlawful interceptions may go unchecked, bypassing independent oversight from Parliament or the judiciary**—key pillars of democratic accountability.
- **Indefinite retention in some cases:** Rules allow the indefinite retention of intercepted messages for functional purposes with no clear time limit.
- **Lack of protection for Telecom Service Providers (TSPs):** Without safeguards for TSPs, they may be tempted to collude with authorities, ignoring unauthorized surveillance.
- **Lack of Accountability:** Deletion of records of interception could place the interception of private information by the Competent Authorities **beyond the scope of public scrutiny** by mechanisms such as the RTI.

Way Forward

- **Limit subjective interpretation:** Clearly define the terms such as public emergency and public order etc. to ensure interception is **strictly for national security**, not political misuse.

- **Establish an independent oversight body:** Establish a parliamentary or judicial review board to oversee interception orders and ensure compliance with legal provisions.
- **Protection to TSPs:** TSPs be provided legal safeguards and liabilities against arbitrary requests for interception.
- **Accountability:**
  - **Mandate a periodic audit of interception records** by an independent authority to prevent potential misuse.
  - Develop a mechanism for **periodic public reporting on the number and nature of interceptions,** while maintaining national security confidentiality.
  - **Competent authority needs to be held accountable through impartial review** for any wilful misuse of interception powers.
  -
    -
    - Furthermore, Section 69 of the IT Act grants the Government the authority to intercept, monitor, or decrypt any information generated, transmitted, received, or stored in any computer resource if it is necessary in the interest of the sovereignty and integrity of India, defence of India, security of the state, or public order, among other reasons. Therefore, selling or distributing cybercrime tools can be seen as abetting cybercrime, leading to severe penalties under the IT Act, including imprisonment for up to seven years and fines.