Mains Practice Question

Q. Recently, Home Ministry issued orders authorising 10 central government agencies to monitor, intercept and decrypt all data contained in any computer system. Do you think such powers are needed to address contemporary internal security challenges? Critically analyse. (250 words)

29 Dec, 2018 GS Paper 3 Internal Security

Approach:

- Explain the current framework related to surveillance in India.
- Analyse the need for such regulation.
- Discuss the concerns.
- State how it can help address contemporary internal security challenges.

Introduction

- At present, despite having the second highest number of Internet users in the world, India has little to show as a country in investigatory outcomes, measured regulatory responses or parliamentary processes which safeguard users.
- Currently, there are two main acts governing the legal provisions for surveillance in India:
    - **The Telegraph Act of 1885:** allows for the interception of calls and messages
    - **The Information Technology Act of 2000**: deals with provisions to intercept digital information including data stored on a computer, internet traffic and other data flows.
- Section 69 (1) of the IT Act, 2000 empowers the government to intercept, monitor or decrypt any information generated, transmitted, received or stored in any computer resource 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.

Body

Need for Data Interception

- The rising threat of terrorism, theft and homegrown criminals, and lack of institutional capacity to respond to such challenges.
- Increase in the cases of recruitment and indoctrination of youth by terrorist outfits like ISIS. Radicalisation through social media platforms is on the rise and youngsters are joining the ranks of militancy.
- Fake news and rumours have led to incidents of mob violence across the country.
- It is easier to hold the government accountable for the use of personal data than commercial platforms like Facebook.
- The state can regulate the commercialised surveillance and its effects on Indian society through these agencies.

Concerns

- A blanket approval to electronic surveillance can have direct effects on civil liberties and personal

freedom of citizens guaranteed by the constitution under Article 19 1(A). It may amount to the creation of a ‘surveillance state’.
- It is in contravention with the 2017 K.S. Puttaswamy (privacy) judgment of the Supreme Court, which directed the government to protect informational privacy of every individual under Article 21.
- The government can misuse information for its own benefit. Also, it does not address the failure of ground-level law and order.
- Grounds of surveillance like ‘sovereignty or integrity of India’ and ‘security of the state’ have not been defined clearly and leave more scope for misuse by the authorities. There remains a fear of decrypted data falling in wrong hands.

Conclusion

- National security should be protected by a smaller infringement upon fundamental rights by the government within the constitutional limits.
- A middle ground should be adopted that allows for reasonable surveillance subject to oversight by branches of government other than the executive. A balance should be maintained between the values of privacy and security based on constitutional principles and fundamental rights.
- All surveillance requests must necessarily go before a judicial authority, which can apply an independent legal mind to the merits of the request, in light of the citizens’ privacy- State’s surveillance proportionality standards.
- Interception request should be treated on its own merit and only authorised after due process, with adequate checks and balances, to aid the investigation.
- Grounds of surveillance should be more clearly defined for effective judicial review.
- Surveillance techniques and practices that are applied outside the rule of law must be brought under legislative control. A strong, rights-protecting, comprehensive privacy law that also regulates surveillance is the need of the hour.
- Digital interception should only aid law enforcement, not become a focus in itself.