



Mains Practice Question

Q. Strong data protection and privacy laws are important for the digital well being of citizens in India. Examine. (250 words)

13 Nov, 2019 GS Paper 3 Economy

Introduction

- Recently, WhatsApp sued an Israeli firm, the NSO Group for using its platform to spy on journalists and human rights activists worldwide. The surveillance was carried out using a spyware tool called Pegasus, which has been developed by the NSO Group.
- This highlights the need for strong data protection laws and user privacy in India.

Need for strong data protection and privacy laws in India

- Right to privacy now being a **fundamental right (Puttaswamy judgment)**, framing guidelines for protection of digital data should be the responsibility of the government.
- Unregulated access to data can lead **to suppression of dissent and censorship**. Journalists, Human Rights activists etc. can be put under an invisible prison of surveillance.
- There is need to check **unauthorized leaks**, hacking, cyber crimes, and frauds. Monetary cost of data loss/theft is very high. For ex: there are numerous cases of Aadhaar data leaks by government websites themselves due to technical glitch.
- Data protection laws would **improve business processes**, and their compliance will eventually lead to securing digital payments, and improvement in banking operations as well.
- Restrict use of data by **data colonising** companies such as Facebook, Whatsapp, etc. User data is currently concentrated in the hands of few MNCs which can be misused against national interest. For ex: **Cambridge Analytica Scandal** which involved the collection of personally identifiable information of up to 87 million Facebook users. The data was allegedly used to attempt to influence voter opinion.

Steps taken to ensure user privacy

BN Srikrishna Committee (2017) report highlighted the need to have a Technology agnostic law- data protection law must be flexible to include changing technologies. It recommended to include:

- Informed and meaningful consent
- Minimal and necessary data processing
- Data controller must be accountable for any processing
- Establishing a high-powered statutory authority for enforcement, supported by a decentralised enforcement mechanism
- Penalties for wrongful data processing

Draft Digital Information Security in Healthcare Act (DISHA), 2018:

- It seeks to ensure the protection of data related to physical, physiological and mental health condition, sexual orientation, medical records and history and biometric information

Way forward

- **GDPR (General Data Protection Regulation) rules** framed by the EU has become a model for the world when it comes to privacy. Right to be forgotten is also in effect in the EU.
- There is an urgent need to pass the draft **Data Protection Bill, 2018** which seeks to regulate the processing of personal data of individuals (data principals) by government and private entities (data fiduciaries) incorporated in India and abroad.

PDF Refernece URL: <https://www.drishtiias.com/mains-practice-question/question-402/pnt>