Syllabus subtopic: Government policies and interventions for development in various sectors and issues arising out of their design and implementation.

Prelims and Mains focus: key features of the bill, its merits and demerits,

News: The Personal Data Protection Bill, which is to be tabled in Parliament, seeks to allow processing of personal data without the consent of the owner for several “reasonable purposes” ranging from the operation of search engines to whistle-blowing, according to an official with knowledge of the matter.

Key highlights of the bill:

- The bill categorizes data into three categories—critical, sensitive and general.

- Sensitive data—financial, health, sexual orientation, biometrics, transgender status, religious or political beliefs and affiliation—can be stored only in India. However, data can be processed outside India with explicit consent.

- Critical data will be defined by the government from time to time and has to be stored and processed in India. Any personal non-critical and non-sensitive data will be categorized as general data with no restriction on where it is stored or processed.

- The bill also proposes setting up of a “regulatory sandbox” for entities engaged in developing new technologies in the nature of artificial intelligence and machine learning. These entities, for instance, startups, can avail of certain exemptions from purpose, storage and consent requirements of data.

- In a first, the data protection bill wants social media platforms to create a mechanism that will enable registered users to voluntarily verify their accounts. The provision is largely aimed at checking social media trolling.

- The bill, while seeking to preserve the sanctity of individual consent, allows for several exemptions for prevention and detection of any unlawful activity including fraud; whistle blowing; mergers and acquisitions; network and information security, credit scoring; recovery of debt; processing of publicly available personal data; and operation of search engines.

- According to the draft, personal data may be processed without obtaining consent if such processing is necessary for the purposes specified by regulations after taking into
consideration certain factors such as public interest.

- Personal data may be “processed” if this is necessary for the performance of “any function of the state authorized by the law” for any public service and for compliance with any order of a court or tribunal.

- Under the proposed law, the government is also entitled to direct a fiduciary—any person or entity that processes data—to get access to non-personal data to provide better services to citizens. For instance, the government can use non-personal or anonymous data for research or any other purpose.

- While the (changes in the bill) would arguably help enable certain types of businesses, other changes such as lack of a clear implementation road map, transition provisions and the requirement to share anonymized and non-personal data under certain circumstances may be of concern to businesses.

- The bill empowers users with the “right to be forgotten”. This will allow users, termed “data principal” under the proposed bill, to erase their personal data published online and give them the freedom to ask entities such as Facebook and Twitter to delete any data they do not want in the public domain.

- People can ask for restricting or preventing continued disclosure of data once the purpose for which it was collected has been served, or is no longer necessary. Such data will also need to be withdrawn if the data principal has withdrawn consent for the purpose it was given for, said the official cited earlier.

Responsibilities imposed

- The bill places a few responsibilities on data principals.

- They will have to file an application with an adjudicating officer in case they wish to withdraw consent or want to limit the use of data, according to the official.

- Data principals will have to convince the officer that their right or interest in preventing or restricting the continued disclosure of their personal data overrides the right to freedom of speech and expression and the right to information of any other citizen.