Personal Data Protection Bill 2019

This article is based on **"The issues, debate around Data Protection Bill"** which was published in The Indian Express on 7/12/2019. It talks about the implications of new Personal Data Protection (PDP) Bill, 2019.

Global negotiations today revolve around debates about the transfer and security of data. In this context, the Personal Data Protection (PDP) Bill, 2019 is the India's first attempt to domestically legislate on the issue of data protection.

The Bill derives its inspiration from a previous draft version prepared by a committee headed by retired **Justice B N Srikrishna.** However, the present bill differs from what was recommended by Justice B N Srikrishna committee.

Significance of Data

- Data is the large collection of information that is stored in a computer or on a network.
- Data is collected and handled by entities called **data fiduciaries.**
- While the fiduciary controls how and why data is processed, the processing itself may be by a third party, the **data processor.**

  This distinction is important to delineate responsibility as data moves from entity to entity. For example, in the US, Facebook (the data controller) fell into controversy for the actions of the data processor — Cambridge Analytica.
- The processing of this data (based on one's online habits and preferences, but without prior knowledge of the data subject) has become an important source of profits for big corporations.

  Targeted advertising: Companies, governments, and political parties find it valuable because they can use it to find the most convincing ways to advertise online.
- Apart from it, this has become a potential avenue for invasion of privacy, as it can reveal extremely personal aspects.

- Also, it is now clear that much of the future's economy and issues of national sovereignty will be predicated on the regulation of data.
- The physical attributes of data — where data is stored, where it is sent, where it is turned into something useful — are called **data flows.** Data localisation arguments are premised on the idea that data flows determine who has access to the data, who profits off it, who taxes and who "owns" it.

Key Definitions

- **Data Principal:** The individual whose data is being stored and processed is called the data principal in the PDP Bill.
- **Data Fiduciary:** The 'data fiduciary' may be a service provider who collects, stores and uses data in the course of providing such goods and services.
- **Data Transfer:** Data is transported across country borders in underwater cables.
- **Data localisation:** It is the act of storing data on any device physically present within the borders of a country.

What does PDP Bill propose?

The B N Srikrishna committee draft had required all fiduciaries to store a copy of **all personal data in India,** which was criticised by foreign technology companies that store most of Indians' data abroad. The Bill, however, trifurcates the data into three categories and mandates the storage within India's boundaries depending upon the type of data.

- The Bill **trifurcates data** as follows:
    - **Personal data:** Data from which an individual can be identified like name, address etc..
    - **Sensitive personal data (SPD):** Some types of personal data like as financial, health, sexual orientation, biometric, genetic, transgender status, caste, religious belief, and more.
    - **Critical personal data:** Anything that the government at any time can deem critical, such as military or national security data.
- The Bill removes the requirement of **data mirroring** (in case of personal data). Only individual consent for data transfer abroad is required.

    Data mirroring: The act of copying data from one location to a storage device in real time.
- **Personal Data:** The Bill requires sensitive personal data to be stored only in India. It can be processed abroad only under certain conditions including approval of a **Data Protection Agency (DPA).**
- **Critical Personal Data:** Critical personal data must be stored and processed in India.

- **Non Personal Data:** The Bill mandates fiduciaries to provide the government any **non-personal data** when demanded.
    - Non-personal data refers to anonymised data, such as traffic patterns or demographic data.
    - The previous draft did not apply to this type of data, which many companies use to fund their business model.
- The Bill also requires **social media companies,** which are deemed significant data fiduciaries based on factors such as volume and sensitivity of data, to develop their own user verification mechanism.

    This intends to decrease the anonymity of users and prevent trolling.

Other key provisions of the bill

- The Bill includes exemptions for processing data without an individual's consent for **"reasonable purposes",** including security of the state, detection of any unlawful activity or fraud, whistleblowing, medical emergencies, credit scoring, operation of search engines and processing of publicly available data.
- The Bill calls for the creation of an **independent regulator Data Protection Authority,** which will oversee assessments and audits and definition making.
- Each company will have a **Data Protection Officer (DPO)** who will liaison with the DPA for auditing, grievance redressal, recording maintenance and more.
- The Bill proposes **"Purpose limitation"** and **"Collection limitation"** clause, which limit the collection of data to what is needed for "clear, specific, and lawful" purposes.
- It also grants individuals the **right to data portability** and the **ability to access and transfer one's own data.** It also grants individuals the right to data portability, and the ability to access and transfer one's own data.
- Finally, it legislates on the right to be forgotten. With historical roots in European Union law, **General Data Protection Regulation (GDPR)**, this right allows an individual to remove consent for data collection and disclosure.
- The Bill stated the **penalties** as: Rs 5 crore or 2 percent of worldwide turnover for minor violations and Rs 15 crore or 4 percent of total worldwide turnover for more serious violations.

    Also, the company's executive-in-charge can also face jail terms of up to three years.

Advantages

- Data localisation can **help law-enforcement agencies** access data for investigations and enforcement.
    - As of now, much of cross-border data transfer is governed by individual bilateral "mutual legal assistance treaties".
    - Accessing data through this route is a cumbersome process.

- Instances of cyber attacks and surveillance will be checked.
    Recently, many WhatsApp accounts were hacked by an Israeli software called **Pegasus.**
- Social media is being used to spread **fake news**, which has resulted in lynchings, national security threats, which can now be monitored, checked and prevented in time.
- Data localisation will also increase the ability of the Indian government to **tax** Internet giants.
- A strong data protection legislation will also help to enforce **data sovereignty.**

Disadvantages

- Many contend that the physical location of the data is not relevant in the cyber world. Even if the data is stored in the country, the encryption keys may still be out of reach of national agencies.
- National security **or reasonable purposes** are an open-ended terms, this may lead to intrusion of state into the private lives of citizens.
- Technology giants like Facebook and Google have criticised **protectionist policy on data protection (data localisation).**
    They fear that the **domino effect** of protectionist policy will lead to other countries following suit.
- Protectionist regime supress the values of a globalised, competitive internet marketplace, where costs and speeds determine information flows rather than nationalistic borders.
- Also, it may backfire on **India's own young startups** that are attempting global growth, or on larger firms that process foreign data in India.

Conclusion

- According to the Supreme Court in the **Puttaswamy judgement (2017)**, the **right to privacy** is a fundamental right and it is necessary to protect personal data as an essential facet of informational privacy, whereas the growth of the digital economy is also essential to open new vistas of socio-economic growth.
- In this context, the government policy on data protection must not deter framing any policy for the growth of the digital economy, to the extent that it doesn't impinge on personal data privacy.

Drishti Mains Question

Data localisation, despite its many advantages, may eventually do more harm than good. Comment. (250 words)