Draft Personal Data Protection Bill, 2019

Why in News

Recently, **Facebook India's policy head has appeared** before the **30-member Joint Committee of Parliament** which is examining the **draft** Personal Data Protection Bill, 2019.

- However, **Amazon has declined to appear** on the ground of risky travel amidst the **pandemic.**

Key Points

- Amazon, Twitter, Facebook, Google and Paytm are among the companies from whom the committee has **sought views on data security and protection** amid concerns that the **privacy of users is being "compromised" for commercial interest.**
    - Facebook was interrogated on how it targets audiences, their data storage model and transfer of data, etc.
    - **Amazon's refusal** amounts to a **breach of parliamentary privilege** and the panel is **unanimous about taking coercive action** if no one from the company appears on the next date.
- **Personal Data Protection Bill, 2019:**
    - It is commonly referred to as the **"Privacy Bill"** and intends to **protect individual rights by regulating the collection, movement, and processing of data** that is personal, or which can identify the individual.
        - The Bill derives its inspiration from a **previous draft version prepared by** a committee headed by retired **Justice B N Srikrishna.**
    - In **December 2019, Parliament approved sending it to the joint committee.**
    - The Bill gives the government **powers to authorise the transfer of certain types of personal data overseas** and has given **exceptions allowing government agencies to collect personal data** of citizens.
    - The Bill **divides the data into three categories and mandates their storage** depending upon the type.
        - **Personal Data:** Data from which an individual can be identified like name, address, etc.
        - **Sensitive Personal Data:** Some types of personal data like financial, health-related, sexual orientation, biometric, genetic, transgender status, caste, religious belief, and more.
            - It needs to be **stored only in India and can be processed abroad only under certain conditions** including **approval of the Data Protection Agency** (DPA).
        - **Critical Personal Data:** Anything that the government at any time can deem critical, such as military or national security data.
            - It **must be stored and processed in India only.**

- It **removes the requirement of data mirroring** (in case of personal data). **Only individual consent for data transfer abroad is required.**
    - **Data mirroring** is the act of copying data from one location to a storage device in real-time.
    - In the earlier version, the Bill **enabled the transfer of personal data outside India,** with a subcategory of **SPD having to be mirrored** in the country (i.e. a **copy will have to be kept in the country)**.
- It **mandates data fiduciaries to provide the government with 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.**
    - **Data Fiduciary:** It may be a **service provider who collects, stores and uses data** in the course of providing such goods and services.
- The Bill **requires companies and social media intermediaries,** which are "significant data fiduciaries", to **enable users in India to voluntarily verify their accounts.**
    - It would be visible in a **"demonstrable and visible mark of verification,** which shall be visible to all users of the service".
    - This intends to **decrease the anonymity** of users and **prevent trolling.**

- **Advantages:**
    - **Data localisation** can help law-enforcement agencies access data for investigations and enforcement and also **increase the ability** of the government to **tax internet giants.**
    - Instances of cyber-attacks (for example, **Spyware Pegasus**) and surveillance can be checked.
    - **Social media,** which is sometimes used to spread fake news, can be **monitored and checked,** preventing emerging national threats in time.
    - 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 as the **encryption keys may still be out of reach** of national agencies.
    - **National security or reasonable purposes** are **open-ended and subjective terms,** which may lead to intrusion of the state into the private lives of citizens.
    - **Technology giants like Facebook and Google are against it and have criticised** the protectionist policy of data localisation as they are afraid it would have a **domino effect in other countries** as well.
    - 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.**

Source: TH