Digital Personal Data Protection Bill 2022

For Prelims: Digital Personal Data Protection Bill, Right to Privacy, Puttaswamy Judgement, Data Protection Laws of Other Nations

For Mains: Provisions of Digital Personal Data Protection Bill 2022, Puttaswamy Judgement, Data Protection Laws of Other Nations

Why in News?

The Union Government has released a revised personal data protection bill, now called **the Digital Personal Data Protection Bill, 2022.**

- The Bill has been introduced after 3 months of the withdrawal of the **Personal Data Protection Bill, 2019.**

What are the Seven Principles of the 2022 Bill?

- **Firstly,** usage of **personal data** by organisations must be done in a manner that is **lawful, fair to the individuals concerned and transparent to individuals.**
- **Secondly**, personal data must **only be used for the purposes** for which it was collected.
- **The third principle** talks of **data minimisation.**
- **The fourth principle** puts an emphasis on **data accuracy** when it comes to collection.
- **The fifth principle** talks of how personal data that is collected **cannot be "stored perpetually by default"** and storage should be **limited to a fixed duration.**
- **The sixth principle** says that there should be **reasonable safeguards to ensure** there is "no **unauthorized collection or processing** of personal data".
- **Seventh principle** states that "the person who decides the purpose and means of the processing of personal data **should be accountable for such processing".**

What are the Key Features of the Digital Personal Data Protection Bill?

- **Data Principal and Data Fiduciary:**
  - **Data Principal** refers to the individual whose **data is being collected.**
    - In the case of children (**<18 years**), their parents/lawful guardians will be considered their **"Data Principals".**
  - **Data Fiduciary** is the entity (individual, company, firm, state etc), which decides the **"purpose and means of the processing of an individual's personal data".**
    - **Personal Data** is "any data by which an individual can be identified".
    - **Processing** means "the entire cycle of operations that can be carried out in respect of personal data".
  - **Significant Data Fiduciary:**
    - **Significant Data Fiduciaries** are those who deal with a high volume of personal data. The **Central government** will define who is designated under this category based on a number of factors.

        - Such entities will have to appoint a **'Data protection officer'** and an independent **Data Auditor.**
- **Rights of Individuals:**
    - **Access to Information:**
        - The bill ensures that individuals should be able to **"access basic information"** in languages specified in the **eighth schedule of the Indian Constitution.**
    - **Right to Consent:**
        - Individuals need to **give consent before their data is processed** and "every individual should know **what items of personal data** a Data Fiduciary wants to collect and the **purpose of such collection** and further processing".
        - Individuals also have the **right to withdraw consent** from a Data Fiduciary.
    - **Right to Erase:**
        - Data principals will have the right to **demand the erasure and correction** of data collected by the data fiduciary.
    - **Right to Nominate:**
        - Data principals will also have the **right to nominate an individual** who will exercise these rights in the event of their death or incapacity.
- **Data Protection Board:**
    - The Bill also proposes to set up a **Data Protection Board** to ensure compliance with the Bill.
    - In case of an unsatisfactory response from the Data Fiduciary, the consumers can file a complaint to the **Data Protection Board.**
- **Cross-border Data Transfer:**
    - The bill allows for **cross-border storage and transfer of data** to "certain notified countries and territories" provided they have a **suitable data security landscape**, and the **Government can access data** of Indians from there.
- **Financial Penalties:**
    - **For Data Fiduciary:**
        - The bill proposes to **impose significant penalties** on businesses that undergo data breaches or fail to notify users when breaches happen.
        - The penalties will be imposed ranging from Rs. 50 crores to Rs. 500 crores.
    - **For Data Principal:**
        - If a **user submits false documents while signing up for an online service,** or files frivolous grievance complaints, the user could be fined up to Rs 10,000.
- **Exemptions:**
    - The government can **exempt certain businesses from adhering to provisions of the bill** on the basis of the **number of users and the volume of personal data** processed by the entity.
        - This has been done keeping in mind **startups** of the country who had complained that the Personal Data Protection Bill, 2019 **was too "compliance intensive".**
    - **National security-related exemptions,** similar to the previous 2019 version, **have been kept intact.**
        - The **Centre has been empowered** to exempt its agencies from adhering to provisions of the Bill in the interest of **sovereignty and integrity of India, security of the state, friendly relations with foreign states, maintenance of public order** or **preventing incitement** to any cognisable offence.

Why is Digital Personal Data Protection Bill Significant?

- The new Bill offers significant **concessions on cross-border data flows**, in a departure from the previous Bill's contentious requirement of local storage of data within India's geography.
- It offers a relatively **soft stand on data localisation requirements** and permits **data transfer** to select global destinations which is likely to **foster country-to-country trade agreements.**
- The bill recognises the data principal's **right to postmortem privacy (Withdraw Consent)** which was missing from the PDP Bill, 2019 but had been recommended by the **Joint Parliamentary Committee (JPC).**

How has India Strengthened Data Protection Regime?

- **Justice K. S. Puttaswamy (Retd) vs Union of India 2017:**
  - In August 2017, a nine-judge bench of the Supreme Court in **Justice K. S. Puttaswamy (Retd) Vs Union of India** unanimously held that Indians have a constitutionally protected **fundamental right to privacy** that is an intrinsic part of life and liberty under **Article 21.**
- **B.N. Srikrishna Committee 2017:**
  - Government appointed a **committee of experts for Data protection** under the chairmanship of **Justice B N Srikrishna** in August 2017, that submitted its report in July 2018 along with a draft Data Protection Bill.
    - The Report has a wide range of recommendations to **strengthen privacy law in India** including **restrictions on processing and collection** of data, Data Protection Authority, **right to be forgotten**, **data localisation** etc.
- **Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules 2021:**
  - **IT Rules (2021)** mandate social media platforms to exercise greater diligence with respect to the content on their platforms.

What Data Protection Laws are there in Other Nations?

- **European Union Model:**
  - **The** General Data Protection Regulation focuses on a **comprehensive data protection** law for processing of personal data.
  - In the EU, the right to privacy is enshrined as a **fundamental right** that seeks to protect an **individual's dignity and her right** over the data she generates.
- **US Model:**
  - There is **no comprehensive set of privacy rights or principles in the US** that, like the EU's GDPR, addresses the use, collection, and disclosure of data.
  - Instead, there is **limited sector-specific regulation.** The approach towards data protection is different for the public and private sectors.
    - The activities and powers of the government vis-a-vis personal information are well-defined and addressed by broad legislation such as the **Privacy Act,** the **Electronic Communications Privacy Act,** etc.
    - For the private sector, there are **some sector-specific norms.**
- **China Model:**
  - New Chinese laws on **data privacy and security** issued over the last 12 months include the **Personal Information Protection Law (PIPL),** which came into effect in November 2021.
    - It gives **Chinese data principals new rights** as it seeks to prevent the misuse of personal data.
  - **The Data Security Law (DSL),** which came into force in September 2021, requires business data to be **categorized by levels of importance,** and puts new restrictions on cross-border transfers.

UPSC Civil Services Examination, Previous Year Questions (PYQs)

Prelims

Q1. 'Right to Privacy' is protected under which Article of the Constitution of India? (2021)

(a) Article 15
(b) Article 19
(c) Article 21
(d) Article 29

Ans: (c)

Exp:

- In Puttaswamy v. Union of India case, 2017, the Right to Privacy was declared a fundamental right by the Supreme Court.
- Right to Privacy is protected as an intrinsic part of the Right to Life and Personal Liberty under Article 21 and as a part of the freedoms guaranteed by Part III of the Indian Constitution.
- Privacy safeguards individual autonomy and recognizes one's ability to control vital aspects of his/her life. Privacy is not an absolute right, but any invasion must be based on legality, need and proportionality.
- **Therefore, option (c) is the correct answer.**

Q2. Right to Privacy is protected as an intrinsic part of Right to Life and Personal Liberty. Which of the following in the Constitution of India correctly and appropriately imply the above statement? (2018)

(a) Article 14 and the provisions under the 42nd Amendment to the Constitution.
(b) Article 17 and the Directive Principles of State Policy in Part IV.
(c) Article 21 and the freedoms guaranteed in Part III.
(d) Article 24 and the provisions under the 44th Amendment to the Constitution.

Ans: (c)

Explanation:

- In 2017, a nine-judge bench of the Supreme Court (SC) in its verdict in Justice K.S. Puttaswamy v. Union of India case unanimously affirmed that the Right to Privacy is a Fundamental Right under the Indian Constitution.
- The SC bench held that the privacy is a Fundamental Right as it is intrinsic to guarantee of life and personal liberty as provided under Article 21 of the Constitution.
- The bench also stated that the elements of privacy also arise in varying contexts from the other facets of freedom and dignity recognised and guaranteed by the Fundamental Rights contained in Part III of the Constitution.
- Therefore, option (c) is the correct answer.

Mains

Q. Examine the scope of Fundamental Rights in the light of the latest judgement of the Supreme Court on Right to Privacy. **(2017)**

Source: IE