Withdrawal of Personal Data Protection Bill

For Prelims: Data Protection, Personal Data, Privacy, Personal Data Protection Bill, Data Localisation, Other Related Laws

For Mains: Significance of Personal Data Protection, Challenges in safeguarding data, Measures for implementation of data protection bill

Why in News?

The government of India has withdrawn the **Personal Data Protection Bill** from **Parliament** as it considers a **"comprehensive legal framework"** to regulate the online space to boost innovation in the country **through a new bill.**

What was the Personal Data Protection Bill & Its Major Challenges?

- **About:**
  - **The Personal Data Protection Bill, 2019** was introduced in **Lok Sabha** by the Minister of Electronics and Information Technology, on December 11, 2019.
  - Commonly referred to as the **"Privacy Bill",** it intended to **protect individual rights** by regulating the collection, movement, and processing of data that is personal, or which can identify the individual.
- **Challenges:**
  - 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.
    - It had been **opposed by social media firms**, experts and even ministers, who said that it had **too many loopholes to be effective** and beneficial for both users and companies.
    - 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.

Why has the Bill been withdrawn?

- **Too Many Amendments:**
  - **The Joint Committee of Parliament** analyzed the Personal Data Protection Bill, 2019 in detail.
    - **81 amendments were proposed and 12 recommendations were made** towards a comprehensive legal framework on the **digital ecosystem.**
    - Considering the report of the JCP, **a comprehensive legal framework is being worked upon.**

        - Hence, it is proposed to withdraw.
- **Compliance Intensive:**
    - The Bill was also seen as **being too "compliance intensive"** by startups of the country.
        - The revamped bill will be much **easier to comply with**, especially for startups.
- **Issues with Data Localisation:**
    - The tech companies questioned a proposed provision in the Bill called **Data Localisation.**
        - Under data localisation, it would have been **mandatory for companies** to store a copy of certain sensitive personal data **within India**, and the **export of undefined "critical" personal data** from the country would be **prohibited.**
        - The activists had criticised that it **would allow the central government** and its agencies blanket exemptions from adhering to any and all provisions of the Bill.
- **Pushback from Stakeholders:**
    - The bill had faced **major push back from a range of stakeholders** including big tech companies such as Facebook and Google, and privacy and civil society activists.
- **Delay in Implementation:**
    - The delays in the Bill had been criticised by several stakeholders pointing out that it was a matter of grave concern that India did not have a basic framework to protect people's privacy.

What did the Joint Committee of Parliament Recommend?

- It proposed **81 amendments to the Bill** finalized by the Srikrishna panel, and **12 recommendations** including **expanding the scope of the proposed law to cover discussions on** non-personal data**,** thereby changing the mandate of the Bill from personal data protection to broader data protection.
    - **Non-personal data** is any set of data that **does not contain personally identifiable information.**
- The JCP's report also recommended changes on issues such as **regulation of social media companies,** and on using only **"trusted hardware"** in smartphones, etc.
- It proposed that social media companies that do not act as intermediaries should be treated as **content publishers, making them liable for the content they host.**

Way Forward

- **Data Localisation:**
    - The data should be stored in a region that is trusted by the Indian government, and that data should be accessible in the event of a crime.
    - The government may also consider allowing **cross-border data flows only to "trusted geographies".**
- **Classification of Data:**
    - The new Bill could also **do away with classification of personal data** from the perspective of data localisation, and only use classification for awarding damages to people whose personal data may have been compromised by an entity.

UPSC Civil Services Examination, Previous Year Questions (PYQs)

Prelims

Q. 'Right to Privacy' is protected under which Article of the Constitution of India?

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

Ans: (c)

Explanation:

- 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.**

Q. 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