NEXT IAS

EDITORIAL ANALYSIS

Time: 10 min **Date: 20-10-2023**

Implementing the Data Protection Act

Syllabus: GS2/ Government Policies & Interventions

In Context

- The Government of India recently notified the Digital Personal Data Protection Act 2023 (DPDPA).

Key Provisions of the Act

- **Applicability:** The law applies to the processing of digital personal data within India where such data is: (i) collected online, or (ii) collected offline and is digitized. It will also apply to the processing of personal data outside India if it is for offering goods or services in India.
- **Consent:** Personal data may be processed only for a lawful purpose after obtaining the consent of the individual. A notice must be given before seeking consent.
    - The notice should contain details about the personal data to be collected and the purpose of processing.
- **Lower age of consent:** The Law **gives powers to the central government** to prescribe a **lower age of consent than 18 years** for accessing Internet services without parental consent if the platform they are using can process their data in a “verifiably safe manner”.
    - This would essentially mean a white-listing approach for companies in the edtech sector, and for medical purposes, among other things.
- **Ease of cross-border data flows:** The Centre has proposed to significantly ease cross-border data flows to international jurisdictions – by **moving away from a whitelisting approach** to a **blacklisting mechanism**.
    - Earlier, the government had said that it would issue a list of countries where data flows would be allowed.
- **Impact on Social Media Companies:** Significant Data Fiduciaries (**the fiduciaries with huge volume and processing sensitive data**) have to develop their **own user verification mechanism**.
    - It will **reduce the anonymity of users** and decrease trolling, fake news and cyberbullying.
- **Exemptions:** Rights of the data principal and obligations of data fiduciaries (except data security) will not apply in specified cases.
    - **These include:** (i) prevention and investigation of offences, and (ii) enforcement of legal rights or claims.

        - The central government may, by notification, exempt certain activities from the application of the Act.
        - **These include:** (i) processing by government entities in the interest of the security of the state and public order, and (ii) research, archiving, or statistical purposes.
    - **Data Protection Board of India:** The central government will establish the Data Protection Board of India. Key functions of the Board include: (i) monitoring compliance and imposing penalties, (ii) directing data fiduciaries to take necessary measures in the event of a data breach, and (iii) hearing grievances made by affected persons.
        - Board members will be appointed for two years and will be eligible for re-appointment.
    - **Penalties:** The schedule to the Act specifies penalties for various offences such as up to: **(i) Rs 200 crore for non-fulfilment of obligations for children, and (ii) Rs 250 crore for failure to take security measures to prevent data breaches**.
        - Penalties will be imposed by the Board after conducting an inquiry.

Significance

- This enactment is a step in the right direction and **aims to empower citizens** with the **right to know** and **hold authority** over their data.
- It **limits** possibilities of **corporate and government surveillance** and citizen profiling with exceptions built in for **national security and interests**.
- While there can be debate over whether these exceptions run too far in allowing the government to use and/or misuse personal data for its purposes, the overall intention and enforcement law is expected to serve the people of India well.

Challenges of implementation

- **Data held by State governments:**
    - The law covers in its ambit, all data presently held and managed by state governments and its agencies as well.
    - States hold **massive data sets** under various **schemes, programmes and surveys** implemented.
    - This area poses **unfavourable challenges** in terms of capacity, infrastructure, knowledge and implementation.
- **Issues of standardisation & updation:**
    - These data sets are scattered across departments and agencies, and sometimes districts, with minimal standardisation, interoperability, or integration between them.
    - Very few data managers hold and update metadata (explanatory details about the underlying data sets) for data sets in their purview.
- **Prone to errors:**
    - Lack of capacity and standardised infrastructure often lead to inconsistencies, duplicity, and errors in data making it much more difficult than imagined for any useful analysis and use at higher levels of hierarchy.
- **Manual work behind online dashboards:**
    - While dashboards with performance indicators are often prepared and presented with glamour, the backend processes are mostly manual, riddled with ad hoc checks for consistency, accuracy and quality.

- **Inability to implement pre existing data policies:**
    - Many states have adopted data policies or strategies over the last couple of decades. Examples include Karnataka, Odisha, Punjab, Sikkim, Tamil Nadu, Telangana, among others.
    - While some fall short of important themes such as data retention, continuity, cybersecurity, standardisation, capacity, etc., some lack a strong implementation framework that sets milestones and accountability, while building a clearly structured plan for the timely, successful and effective execution of the policy.
- **Complexity of operation:**
    - Unlike most policies and laws where the enforcement is the responsibility of a particular department, the DPDPA 2023 and data policies need to be **enforced across every department** and **agency** wherever there is public data.
    - This makes the effort much more complex and cumbersome in the convoluted and hierarchical bureaucracies our governments operate with.

<u>Suggestions</u>

- **Revising policy guidelines:**
    - With the DPDPA now passed, it has become urgent for states to act.
    - The existing policies or strategies need to be revised in alignment with the DPDPA or a new one designed to serve as an action plan for the entire state government.
    - The policy now needs to put down guidelines for data collection, standardisation, anonymisation, integration, infrastructure, security, retention, continuity, processing, and use.
- **Capacity building:**
    - They need to elaborately build a plan for the capacity development of all government officials involved at any stage of the data lifecycle to understand the DPDPA, other relevant laws in India (such as the Aadhaar Act 2016, the Right to Information Act 2005, the IT Act 2000 and others), and their personal roles and responsibilities.
- **Cybersecurity:**
    - The importance of cybersecurity needs to be explained and reflected in measures and investments at all levels of the bureaucracy to ensure public data is safe and cyber threats can be minimised.
- **Grievance redressal:**
    - Since the DPDPA sets in a detailed process for registering and addressing public grievances, states need to establish their processes for citizens and institutions to raise grievances, queries, requests, and suggestions related to personal and non-personal data.
- **Holistic approach:**
    - There is a need for a commitment to a prolonged allocation of resources, a rigorous process to monitor and track policy implementation, and a culture where data is understood as an asset, a responsibility, and the key to an inclusive and secure future.

<u>Way ahead</u>

- The DPDPA is an opportunity for governments to improve their data ecosystem and enable evidence-driven decision-making, transparency, and renewed accountability.
- With the advent of modern technologies such as artificial intelligence (AI) making its way as an ally and a threat, it is now that the states need to hold the reins of their data ecosystem and drive change.

Daily Mains Question

[Q] What is the significance of enactment of the Digital Personal Data Protection Act 2023. Examine the implementation hurdles for the Act.