NEXT IAS

DAILY EDITORIAL ANALYSIS

TOPIC

INDIA'S DATA PROTECTION RULES NEED SOME FINE TUNING

INDIA'S DATA PROTECTION RULES NEED SOME FINE TUNING

Context

- India's journey towards robust data protection has seen significant milestones, especially with the introduction of the **Draft Digital Personal Data Protection (DPDP) Rules, 2025**.
- While these rules mark a progressive step, there are areas that require fine-tuning to ensure they effectively balance user privacy and business interests.

About

- India's digital ecosystem is undergoing rapid transformation. With a booming tech industry and an ever-increasing reliance on digital platforms, safeguarding user data has become critical.
- The recently introduced **Digital Personal Data Protection Act, 2023 (DPDP Act)** marks a significant step toward ensuring data privacy and security.
- **Timeline of the DPDP Act, 2023:**
  - **2017:** Supreme Court recognizes the right to privacy as a fundamental right in **Justice KS Puttaswamy vs GOI**. **Justice BN Srikrishna Committee** is formed to draft data protection laws.
  - **2018-2021:** Multiple drafts of the Personal Data Protection (PDP) Bill are introduced and revised, with the Joint Parliamentary Committee submitting a report in December 2021.
  - **2023:** The DPDP Act is enacted to ensure data protection through rights-based governance.

Key Provisions of the DPDP Act, 2023

- **Data Fiduciary Obligations:** Entities handling personal data, termed 'Data Fiduciaries,' are mandated to process data transparently, ensuring accuracy and security.
  - They must obtain explicit consent from individuals before data collection and processing.
- **Data Principal Rights: Individuals** (referred to as 'Data Principals') are granted rights to access, correct, and erase their personal data.
  - They can also nominate representatives to exercise these rights on their behalf.
- **Data Protection Board of India:** The Act establishes this board to oversee compliance, address grievances, and impose penalties for violations.
  - The board functions as a digital office, streamlining its operations.
- **Data Localization:** Certain categories of personal data are required to be stored within India, ensuring data sovereignty and security.
  - The specifics of these categories are determined by the government.
- **Processing of Children's Data:** Processing personal data of **children (individuals under 18)** necessitates parental consent.
  - Data Fiduciaries must undertake due diligence to verify parental consent and are prohibited from tracking or targeting advertisements at children.
- **Penalties for Non-Compliance:** The Act stipulates penalties for significant data breaches, emphasizing the importance of adhering to data protection norms.
  - Up to ₹250 crore for not implementing security safeguards.
  - Up to ₹500 crore for breaches of the Act.

Challenges in the Current Framework

- **Ambiguity in Cross-Border Data Transfers:** The Act provides vague guidelines on transferring data to other countries, leaving room for inconsistent enforcement.
  - A lack of clarity on 'trusted' nations could disrupt global operations of multinational corporations.
- **Broad Exemptions for the Government:** The government is exempted from several provisions under national security and public interest clauses.

  - Critics argue that this could lead to potential misuse and undermine the principle of data privacy for citizens.
- **Weak Data Breach Notification Timelines:** While organizations are required to notify breaches, the absence of strict timelines leaves room for delayed reporting, which could hinder containment efforts and public awareness.
- **Limited Focus on Non-Personal Data:** The Act primarily focuses on personal data, potentially overlooking the privacy implications of non-personal data, which can be re-identified and pose privacy risks.
- **Lack of Strong Independent Oversight:** The Data Protection Board, responsible for enforcement, is appointed by the government, raising concerns about its autonomy.
  - A truly independent regulatory body is crucial for impartial enforcement.
- **Insufficient Provisions for SMEs:** While the Act seeks to ease compliance for smaller businesses, many argue that the complexity of obligations could still burden startups and MSMEs, stifling innovation.

Global Lessons

- India can draw inspiration from global frameworks like the EU's GDPR and California's CCPA:
  - **Informed Consent:** GDPR mandates explicit, unambiguous user consent for data processing.
  - **Proportional Penalties:** GDPR bases penalties on company turnover, ensuring compliance.
  - **Transparency:** CCPA emphasizes clear communication of data usage to users.

Recommendations for Fine-Tuning

- **Enhance Clarity on Cross-Border Transfers:** Clearly define 'trusted nations' and establish transparent procedures for international data sharing.
- **Strengthen Government Accountability:** Limit exemptions for government agencies by introducing oversight mechanisms to ensure proportionality and necessity.
- **Mandate Timely Breach Notifications:** Impose strict timelines for reporting data breaches to both regulators and affected individuals.
- **Expand Scope to Non-Personal Data:** Address data-driven risks by including anonymized and non-personal data under the law.
- **Empower an Independent Regulator:** Establish an autonomous Data Protection Authority to enforce the law impartially and address grievances effectively.
- **Support MSMEs and Startups:** Simplify compliance requirements for smaller organizations to foster innovation while ensuring security.

Road Ahead

- The DPDP Act is undoubtedly a landmark step in India's legislative journey toward protecting data privacy.
- However, as technology evolves and data becomes the cornerstone of the digital economy, laws must adapt dynamically. By addressing existing shortcomings, India can build a robust data protection framework that not only safeguards citizens' rights but also fosters innovation and global trust in its digital economy.
- Fine-tuning these rules will position India as a global leader in privacy protection, ensuring a harmonious balance between individual rights and economic growth.

Source: TH

■■■■

Mains Practice Question

Critically examine the Digital Personal Data Protection Act, 2023 considering the balance between privacy rights and the requirements of a digital economy. What specific challenges and improvements can be identified in the current data protection framework?