Shaping the Data Governance Regime

This editorial is based on **"A chance for India to shape a data governance regime"** which was published in the Hindu on 14/02/2023. It discusses the issue with Governance of Data and ways to address the same.

For Prelims: G-20, Personal Data Protection Bill, 2019, Justice K. S. Puttaswamy (Retd) Vs Union of India, Article 21, Right to be forgotten, Data Localisation, India Stack

For Mains: Data Governance and related Issues in India, Government Policies & Interventions

In recent years, **India has made great strides in its digital strategies and data governance.** India has **embraced technology and digitalisation to drive economic growth** and to improve the lives of its citizens.

India's G-20 presidency **has provided an opportunity for the country to showcase its advancements in the digital arena,** particularly with regards to data infrastructures and data governance. As the world becomes increasingly digital, **the G-20 has recognised the need for international cooperation and collaboration in addressing the challenges,** opportunities and risks posed by the rapid growth of data and digital technologies.

The government has been trying to pass a data protection law with multiple attempts in 2019 and another attempt in 2022. The 2022 bill (the Digital Personal Data Protection Bill) differs in many ways from its 2019 counterpart (the Personal Data Protection Bill) such as its classifications of personal data, its consent frameworks and data localisation requirements. However, there are **still some challenges that need to be addressed.**

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 Challenges with Data Protection in India?

- **Lack of Awareness:**
  - One of the biggest challenges with data protection in India is the lack of awareness among individuals and organizations about the importance of data protection and the risks associated with data breaches.
    - This makes it difficult for individuals to take necessary precautions to protect their personal data.
- **Weak Enforcement Mechanisms:**
  - The existing legal framework for data protection in India lacks strong enforcement mechanisms, making it difficult to hold organizations accountable for data breaches and non-compliance.
- **Limited Scope:**
  - The **Personal Data Protection Bill, 2019 applies only to the processing of personal data by entities within India.**
  - It does not cover data processing by entities located outside India, which can make it difficult to protect the personal data of Indian citizens in such cases.
- **Lack of Standardization:**
  - There is a **lack of standardization in data protection practices among organizations in India,** which makes it difficult to implement and enforce data protection regulations.
- **Inadequate Safeguards for Sensitive Data:**
  - The current data protection framework in India **does not provide adequate safeguards for sensitive data such as health data and biometric data,** which are increasingly being collected by organizations.

What Steps has India taken to Strengthen its 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.
- **Other Initiatives taken:**
  - India’s Data Empowerment and Protection Architecture (DEPA)

What should be the Way Forward?

- **Develop a Comprehensive Data Protection Law:**
  - India needs a **robust data protection law that protects citizens' privacy rights** while also facilitating the use of data for legitimate purposes. The law should be in line with global best practices and should provide for strong enforcement mechanisms.
- **Build Digital Infrastructure and Skills:**
  - India needs to invest in **building digital infrastructure and developing digital skills to ensure that data is collected,** stored, and used in a responsible and accountable manner.

- **Develop Clear and Accountable Data Governance Policies and Regulations:**
  - India needs to **establish clear policies and regulations that govern the collection, storage, and use of data by governments,** businesses, and citizens. These policies and regulations should be transparent, accountable, and enforceable.
- **Balance the Interests of all Stakeholders:**
  - India needs to **balance the interests of governments, businesses, and citizens to ensure that data governance supports sustainable development** and benefits all stakeholders.
- **Promote Open-Source Solutions:**
  - India can **promote the development and implementation of open-source solutions** to ensure that underlying data architectures are a social public good, and to promote digital technologies to become accessible and affordable for all.
- **Ensure Alignment with Broader Development Strategies:**
  - India needs to **ensure that its data governance regime is aligned with its broader development strategies** and values, and that it supports the development of a secure, more egalitarian, and trustworthy digital future for all.
    - India Stack can be **designed and implemented in a way that is consistent with India's broader development strategies.**
      - India Stack is a **unified software platform that provides digital public goods,** application interfaces and facilitates digital inclusion.

Drishti Mains Question

What measures has the Indian government implemented to ensure effective data governance and protection of personal data in the country?

UPSC Civil Services Examination Previous Year Question (PYQ)

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