Data Protection and Data Accessibility Policy

This editorial is based on **"An Open Data Policy Won't Work Without Earnest Implementation"** which was published in Livemint on 10/03/2022. It talks about the Draft India Data Accessibility and Use Policy 2022 and the privacy concerns associated.

For Prelims: Data Accessibility Policy, India Data Office (IDO), Data Protection Law, Supreme Court's Puttaswamy Judgement, Right to Privacy, Right to Information (RTI) Act

For Mains: Analysis of Draft India Data Accessibility and Use Policy 2022, Need for Data Protection Law, Data Accessibility Policy and the Right to Privacy.

Recently the **Ministry of Electronics and Information Technology (MeitY)** released its **Draft India Data Accessibility and Use Policy 2022** for public consultation. This is a continuation of earlier efforts to encourage better utilisation of large-scale data collected by the government machinery.

The draft policy is a step forward in **realising the potential of this large volume of data.** However, any data accessibility-and-use policy is incomplete without **adequate public safeguards** provided through a **comprehensive data protection framework.**

What are the Provisions of the Draft Policy?

- The policy aims to radically **transform India's ability to harness public sector data.**
  - It proposes the **establishment of an India Data Office (IDO)** to streamline and unify data access and sharing among government and other stakeholders.
- It **covers all data and information generated, created, collected, or stored** by the central government and authorised agencies.
  - The measures can also be adopted by state governments.
- All government data will be open and shareable unless it falls under a **negative list of data sets.**
  - Data categorised under the negative list of datasets will be shared only with trusted users under the controlled environment.
- **Data shall remain the property** of the agency/ department/ ministry/ entity which generated/collected it.
  - **Access to data under this policy shall not be in violation of any acts** and rules of the government of India in force.
- Despite the demands of academia and other stakeholders, large volumes of such data have remained unutilized.
  - The policy will take advantage of data generated through routine administrative processes for the **better delivery of public services.**

What are the Concerns Regarding the Policy?

- **Lack of Data Protection Law:** Any data accessibility-and-use policy is incomplete without adequate public safeguards provided through a comprehensive data protection framework. Unfortunately, the progress on that front has been slow.
    - The urgency of such a framework is all the more acute because the **proposed policy suggests licensing of public-sector data on citizens** to private entities.
- **Misuse of Data:** There are also issues of **conflict of interest and misuse of such data** for commercial or political purposes.
    - At a time when **data is "the new oil",** monetization of valuable public sector **data without adequate safeguards can be counter-productive,** with implications for governance of public services and the privacy of individuals.
- **Citizens' Attempts to Obtain Public Data:** Administrative control over data has also been **used to thwart attempts by users and citizens** to obtain data for public use.
    - A good example of this is the **Right to Information (RTI) Act**, which has been diluted to a large extent over the past decade. Citizens' attempts to obtain public data has even led to **many RTI activists losing their lives.**
- **Disregards Reliable Independent Surveys:** Public data has often been used to discredit independent credible surveys, rather than complement them. Such records are **often used to suit a political narrative.**
    - Data from the **Employee Provident Fund Organisation (EPFO)** and **E-Shram portal** have been used to argue that jobs are being generated, as against separate evidence from the **PLFS** of the **National Statistical Office (NSO).**
- **Impact of Commercial Interests in Data:** Given that **more data means more money,** commercial interests will prompt the government to collect granular personal details through greater capture and increased retention periods.
    - Tying government policy determinations with a fiscal potential **may also lead to distortion of the aims of data collection —** the welfare of farmers, healthcare, unorganised labourers or even schoolchildren.
    - Over time, the **original objectives for which databases are built will get diluted** in favour of commercial interests.
- **Federalism:** The policy, even though it notes that State governments will be, "free to adopt portions of the policy," **does not specify how such freedom will be achieved.**
    - It becomes relevant, if specific standards are prescribed by the Central government for data sharing, or as a precondition to financial assistance.
    - There is also the **absence of any comment on whether data gathered from States may be sold by the Central government** and whether the proceeds from it will be shared with the States.

What Steps Can Be Taken?

- **Maintaining Data Integrity:** While the policy proposes **greater openness and transparency in sharing public-sector data,** this can contribute to policy making only if data integrity is maintained and it can **independently be verified.**
    - As public data is a by-product of government administration, its quality is only as good as that of the administration.
    - To maintain the integrity of this data, it is **essential to open databases for public scrutiny** and **academic analysis.**
- **Role of Social Audit:** Social audits could **serve a purpose in maintaining data integrity.** Provisions for this are in-built in programmes such as the one that is run under the **Mahatma Gandhi National Rural Employment Guarantee Act.**
    - Its social audit has not only **raised the quality of data available** on this job programme's functioning, but also **helped improve the scheme itself.**
- **Independent Mechanism for Evaluation:** An essential part of our data policy should be to **protect it from the very institution that generates it** - the administrative machinery as well as the political leadership.
    - An independent mechanism of **evaluation and verification of public data is necessary** for it to prove meaningfully useful, **more so when such data is closely linked to people's access** to essential public services.
    - The policy will have little relevance unless safeguards are built in to protect privacy and the

data is reliable enough for the purpose of holding the government accountable.

- **Data Protection Law:** As per the **Supreme Court's Puttaswamy judgement** on the **fundamental right to privacy,** the first ingredient to satisfy constitutionality is the existence of a legal, more often a legislative, basis. **Without a law, there is absence of defined limits to data sharing** that are enforceable and contain remedies.
    - In this case, the promise of **privacy preservation through anonymization tools holds little promise** when it cannot be independently assessed by a body for data protection.
    - Such scenarios call for immediate and effective implementation of the **Data Protection Law.**

Drishti Mains Question

"Any data accessibility-and-use policy is incomplete without adequate public safeguards provided through a comprehensive data protection framework". Analyse this statement in the context of Draft India Data Accessibility and Use Policy 2022.

PYQ

Q. Which of the following adopted a law on data protection and privacy for its citizens known as 'General Data Protection Regulation' in April, 2016 and started implementation of it from 25th May, 2018? (2019)

(a) Australia
(b) Canada
(c) The European Union
(d) The United States of America

Ans: C

- With the objective to impose a uniform data security law on all EU members, General Data Protection Regulation (GDPR) was approved by the European Union (EU) in April 2016.
- GDPR standardised data protection law across all 28 EU countries and imposes new rules on controlling and processing personally identifiable information.
- It also extends the protection of personal data and data protection rights by giving control back to EU residents. GDPR replaces the 1995 EU Data Protection Directive, and came into force on May 25, 2018.
- **Therefore, option C is the correct answer.**

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)

- 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)

- 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.**