Data Protection Regime

This article is based on **"Why the Personal Data Protection Bill matters"** which was published in The Hindu on 12/04/2021. It talks about how the personal data protection bill, 2019 can help in establishing a strong data protection regime.

The pandemic has increased people's participation in the digital economy. Unfortunately, the number of personal data breaches from major digital service providers has increased worryingly in the same period.

The recent alleged data breach at MobiKwik could stand to be India's biggest breach with the data of 9.9 crore users at risk. Given the significance of data in this age, robust data protection regimes are necessary to prevent such events and protect users' interests.

Presently, how different entities collect and process users' personal data in India is mainly governed by the Information Technology Act, 2000, but this data protection regime falls short of providing effective protection to users and their personal data.

However, the **Personal Data Protection Bill, 2019** (which is now under scrutiny by a Joint Parliamentary Committee) could play a big role in providing robust protections to users and their personal data.

Associated Issues With IT Act

- **Issue of Consent:** Data aggregator entities could override the protections in the regime by taking users' consent to process personal data under broad terms and conditions.
    - This is problematic given that users might not understand the terms and conditions or the implications of giving consent.
- **Neglecting Data Privacy:** The frameworks under IT Act emphasize data security but do not place enough emphasis on data privacy.
    - In essence, while entities must employ technical measures to protect personal data, they have weaker obligations to respect users' preferences in how personal data can be processed.
- **Large Vacuum for Data Protection:** The data protection provisions under the IT Act also do not apply to government agencies. This creates a large vacuum for data protection when governments are collecting and processing large amounts of personal data.
- **Becoming Obsolete:** IT Act was enacted in 2000 and further amended in 2008. However, technology and cross-platform integration have increased exponentially.
    - Therefore, the current data protection regime seems to have become inadequate in addressing risks emerging from new developments in data processing technology.

How the Personal Data Protection Bill, 2019 can help?

The Bill seeks to bring a massive and meaningful change to personal data protection in India through this regime. The proposed regime under the Bill seeks to be different from the existing regime in some prominent ways.

- **Defining the Roles:** The Bill envisages codifying the relationship between individuals and firms/state institutions as one between “data principals” (whose information is collected) and “data fiduciaries” (those processing the data) so that privacy is safeguarded by design.
    - Also, the Bill seeks to apply the data protection regime to both government and private entities across all sectors.
- **Ensuring Data Privacy:** The Bill seeks to emphasize that data principals will have to maintain security safeguards to protect personal data and also have to fulfill a set of data protection obligations and transparency and accountability measures.
    - In nutshell, the provides scrutiny on these entities govern and process personal data to uphold users’ privacy and interests.

Note:

- The need for a more robust data protection legislation came to the fore in 2017 post the Supreme Court’s landmark judgment in Justice K.S. Puttaswamy (Retd) v. Union of India established the right to privacy as a fundamental right.
- In the judgment, the Court called for a data protection law that can effectively protect users’ privacy over their personal data.
- Consequently, the Ministry of Electronics and Information Technology formed a Committee of Experts under the Chairmanship of Justice (Retd) B.N. Srikrishna to suggest a draft data protection law.

- **Rights of the Citizens:** The Bill seeks to give users a set of rights over their personal data and means to exercise those rights.
    - For instance, a user will be able to obtain information about the different kinds of personal data that an entity has about them and how the entity is processing that data.
- **Establishing a Regulator:** The Bill seeks to create an independent and powerful regulator known as the Data Protection Authority (DPA).
    - The DPA will monitor and regulate data processing activities to ensure their compliance with the regime.
    - More importantly, the DPA will give users a channel to seek redress when entities do not comply with their obligations under the regime.

Associated Issues With The Bill

Several provisions in the Bill create cause for concern about the regime’s effectiveness. These provisions could contradict the objectives of the Bill by giving wide exemptions to government agencies and diluting user protection safeguards.

- **Scope for Loopholes:** For instance, under clause 35, the Central government can exempt any government agency from complying with the Bill.
    - Government agencies will then be able to process personal data without following any safeguard under the Bill.
    - This could create severe privacy risks for users.
- **Compromised Concept of Consent:** Similarly, users could find it difficult to enforce various user protection safeguards (such as rights and remedies) in the Bill.
    - For instance, the Bill threatens legal consequences for users who withdraw their consent for a data processing activity.

    - In practice, this could discourage users from withdrawing consent for processing activities they want to opt-out of.
- **Sweeping Mandate of DPA:** DPA will be tasked with regulating the provisions of the bill to frame regulations on issues such as mechanisms for taking consent, limitations on the use of data, and cross-border transfer of data.
    - The supervisory mandate of the DPA is sweeping, given the fact that it has to regulate a wide array of preventive obligations, such as security safeguards and transparency requirements.

Conclusion

In this digital age, data is a valuable resource that should not be left unregulated. In this context, the time is ripe for India to have a robust data protection regime.

The Joint Parliamentary Committee that is scrutinizing the Bill, is expected to submit its final report in the Monsoon Session of Parliament in 2021. This interim period shall be utilized to make some changes in the Bill targeted towards addressing various concerns in it could make a stronger and more effective data protection regime.

Drishti Mains Question

In this digital age, data is a valuable resource that should not be left unregulated. In this context, the time is ripe for India to have a robust data protection regime. Discuss.