Falling Short on Data Protection Provisions

What is the issue?

The Joint Parliamentary Committee (JPC) on Personal Data Protection Bill, 2019 has recently met and the agenda is to adopt the draft report that deals with privacy and security of the personal data of citizens.

What is the draft personal data protection bill 2018?

- The draft personal data protection bill 2018 was submitted by the Justice B.N. Srikrishna-headed expert panel.
- The Justice Srikrishna Committee has set the standards to build a legal framework based on the landmark judgment, ***Justice K.S. Puttaswamy vs Union of India***, on privacy.
- The draft takes into account three aspects in terms of data - the citizens, the state and the industry and notes that "**the right to privacy** is a fundamental right".
- To know more about the draft personal data protection bill 2018, click here

What is the Personal Data Protection Bill, 2019?

- The PDPB seeks to provide for protection of personal data of individuals, and establishes a Data Protection Authority for the same.
- **Applicability -** The Bill governs the processing of personal data by government, companies incorporated in India and foreign companies dealing with personal data of individuals in India.
- **Categorisation of personal data** - The Bill categorises certain personal data as sensitive personal data which includes financial data, biometric data, caste, religious or political beliefs, or any other category of data specified by the government.
- **Obligations of data fiduciary -** A data fiduciary is an entity or individual who decides the means and purpose of processing personal data.
- All data fiduciaries must undertake certain measures such as
    - implement security safeguards (data encryption and preventing misuse of data),
    - institute grievance redressal mechanisms to address complaints of

individuals.
    - institute mechanisms for age verification and parental consent
- **Rights of the individual -** The Bill includes the right to
    - Obtain confirmation from the fiduciary on whether their personal data has been processed
    - Seek correction of inaccurate, incomplete or out-of-date personal data
    - Have personal data transferred to any other data fiduciary
    - Restrict continuing disclosure of their personal data by a fiduciary, if it is no longer necessary or consent is withdrawn
- **Grounds for processing personal data -** The processing of data by fiduciaries is allowed only if consent is provided by the individual.
- But it can be processed without consent if it is required by the State for providing benefits to the individual or for legal proceedings or to respond to a medical emergency.
- **Social media intermediaries:** The Bill proposes to include intermediaries with certain obligations to enable online interaction between users and allow for sharing of information.
- **Data Protection Authority -** The Bill sets up a Data Protection Authority consisting of a chairperson and 6 members with at least 10 years' expertise in the field of data protection and information technology.
- Orders of the Authority can be appealed to an Appellate Tribunal which in turn can be appealed in the Supreme Court.
- **Transfer of data outside India -** Sensitive personal data may be transferred outside India for processing if explicitly consented and subject to certain additional conditions but critical personal data can only be processed in India**.**
- Such sensitive personal data should continue to be stored in India.
- **Sharing of non-personal data with government -** The central government may direct data fiduciaries to provide it with any non-personal data and anonymised personal data for better targeting of services.

What are the divergences of the 2019 bill from the Justice Srikrishna Committee's draft Bill?

- The JPC was set up in 2019 to take up the personal data protection bill after parliamentarians were divided over several provisions of the law.
- The dissent notes submitted by some panel members from the Opposition point out that the draft falls short of the standards set by the Justice Srikrishna Committee.

- The key divergences from the Justice Srikrishna Committee's draft Bill is in the selection of the chairperson and members of the Data Protection Authority (DPA).
- While the 2018 draft Bill allowed for judicial oversight, the 2019 Bill relies entirely on members of the executive government in the selection process for the DPA.
- The 2018 Bill allowed for exemptions to be granted to state institutions from acquiring informed consent from data principals only to the "security of the state" but the 2019 Bill adds "public order" as a reason.

What has the panel suggested to build additional compliance?

- Companies will need to report a data breach within 72 hours
- Mandatorily disclose if information relating to a data principal (person or entity that owns the data) is passed on to someone else
- Appoint senior management personnel as data protection officers
- Ensure that copies of sensitive and critical personal data already in possession of foreign entities be brought back by the government in a timebound manner.
- Called for a mechanism in which social media companies can be treated as publishers in some circumstances.
- A change in the contentious portion of the law - Clause 35, which deals with conditions under which the government can access personal data without consent.

What relaxations were suggested for the government?

- Rule about mandatory disclosure of third party sharing need to the data principal need not be made in case it is for State functions or to comply with a court order.
- Quantifying the penalties for companies violating the provisions of the law
- An in-house inquiry by government departments to fix responsibility in the event of a leak.

How can the rules be made more stringent?

- The dangers of exemption on the grounds of public order is susceptible to misuse and "security of the state' criteria is recognised by other data regulations such as Europe's General Data Protection Regulation as a viable reason for exemption.
- The Global Privacy Assembly, featuring Privacy Commissioners from over

19 countries came up with a clear resolution on principles for government access to personal data.

- It has asked for a set of principles on legal basis, the need for clear and precise rules, proportionality and transparency, data subject rights, independent oversight, and effective remedies and redress to the individuals affected.
- The JPC's adoption of the draft Bill and the dissent notes suggest that it has fallen short of standards protecting privacy rights of individuals against blanket misuse by the state.
- The Parliament has to tighten the provisions further and bring them in conformance with the 2018 Bill.

References

1. https://www.thehindu.com/opinion/editorial/falling-short-on-data-protection-provisos/article37633990.ece
2. https://www.hindustantimes.com/india-news/data-protection-bill-report-panel-calls-for-strict-rules-for-firms-leeways-for-govt-101637606267855.html

