The JPC Report and the Data Protection Bill, 2021

Why in news?

After two years of deliberation, the Parliamentary Joint Committee on the Personal Data Protection Bill, 2019 (JPC) tabled its report which contains a new version of the law, "The Data Protection Bill, 2021."

How did the Data Protection Law evolve in India?

- The proposal for a data protection law came after the Supreme Court declared in **Puttuswamy Judgement (2017)** that privacy is a fundamental right and directed the government to come up with the data protection regime.
- The Draft Personal Data Protection Bill 2018 was submitted by the Justice B.N. Srikrishna-headed expert panel.
- Later, The Personal Data Protection Bill, 2019 was introduced in Lok Sabha that focused on the protection of data of individuals.
- It was referred to a Joint Parliamentary Committee for further scrutiny on the demand of opposition members.
- After two years of deliberation, the Parliamentary Joint Committee on the Personal Data Protection Bill, 2019 (JPC) tabled its report this week.
- The recommendations are included with a redrafted version of the law, named The Data Protection Bill, 2021.

What are the key takeaways from the report?

- **Change in Name and Scope of the Bill**- The JPC report has changed the name of the draft law from the 'Personal Data Protection Bill' to the 'Data Protection Bill'.
- **Inclusion of non-personal data-** The committee has said that the PDP Bill should cover both sets of data till an additional framework is established to distinguish between personal and non-personal data.
- **Exemptions for government bodies**- The JPC report retains the controversial clause providing that central government will have the authority to exempt any agency of the government from the provisions of the act.
- However, this is subjected to just, fair, reasonable and proportionate

procedure.

- **Data Breaches**- The committee has recommended that clause 25(3) include a 72-hour reporting period for data breaches.
- **Children's Data-** Section 3(8) of the Bill defines a "child" as a person who has not completed eighteen years of age.
- Data fiduciaries processing children's data have a different set of obligations to follow including getting consent from a parent or guardian before processing the child's data.
- **Data protection in the financial sector**- The committee has recommended a homegrown alternative to the SWIFT payment system to ensure privacy and to boost the domestic economy.
- **Regulation of social media-** It says all social media platforms that do not act as intermediaries should be treated as publishers and be held accountable for the content they host.
- It has also said no social media platform should be allowed to operate in India unless the parent company sets up an office in the country to regulate them in lines with Press Council of India.
- **Data localization-** The committee has asked the government to ensure that a mirror copy of sensitive and critical personal data, which may be already stored by foreign entities outside the country, should mandatorily be brought back within a specified time frame.
- It has also asked for data localization provisions to be followed in letter and spirit.

What is the reason for dissent on the provisions of the bill?

- **Evasion of surveillance reforms**- The bill does not regulate mass surveillance projects like Crime and Criminal Tracking Network and Systems (CCTNS), Central Monitoring System (CMS) or the National Intelligence Grid (NatGrid)
- The bill inserts the phrase, “to ensure the interest and security of the state”, in its title.
- A data protection law that is sought to be legislated to protect individual privacy now has state security as one of its primary objectives.
- **Non-consensual processing of personal data-** As per Clause 12, the state does not need to conform to the consent principle, if processing of personal data is necessary for the state to provide any service or benefit or issuance of any certificate, license or permit.
- The Bill has expanded the entities which can process personal data without consent by including the conditions of proportionality and legitimate state aim for non-consensual processing of personal data.

- The Bill continues to use the terms ‘employer’ and ‘employee’, and there has been a great increase in the use of gig workers where several instances of the workers privacy being comprised are noted.
- **Exemptions**- Clause 35, first proposed by the Srikrishna committee has witnessed considerable dilution by providing primacy to this provision over any other laws
- It deals with the power of the central government to exempt departments from the application of the Data Protection Bill, 2021
- In India, the reasons for providing the exemption are not required to be tabled in Parliament and the order invoking the exemption is not a gazetted notification and will likely be exempt from RTI proceedings.
- Hence, the government can exempt its own departments or ministries from the application of the Data Protection law.
- Such exceptions need to be limited and precise as in case of the United Kingdom’s Data Protection Act, 2018 in which the national security exemption does not extend to the entire Act.
- **Dilution of the powers of the Data Protection Authority-** The Justice B N Srikrishna panel had proposed an appointment committee consisting of judicial members, with the Chief Justice of India as chairperson, to choose members of the Data Protection Authority.
- This was diluted in 2019 and the panel included the Cabinet Secretary, Law Secretary and the IT Secretary.
- This was heavily criticised for compromising the independence of the appointment process.
- Changes have been made in Clause 42(2) of the draft Data Protection Bill, 2021 by which the Attorney General, an expert, a director of an IIT, and a director of an IIM are included in the selection panel.
- This provides choice to the government in picking any one director from the multiple IITs and IIMs across India.
- **Expansion of the powers of the central government-** The JPC has said that the authority should be bound by the directions of the central government under all cases and not just on questions of policy.
- The JPC and the Bill recognise the importance of privacy and the need to protect all facets of data only for the private actors.
- The expansion of the scope of the encroachment of privacy by government actors continues and the accountability of the state in protecting our privacy continues.

References

- https://economictimes.indiatimes.com/tech/technology/decoding-data-protection-bill/articleshow/87952722.cms
- https://www.livelaw.in/top-stories/data-protection-bill-report-joint-parliamentary-committee-exemptions-non-personal-data-childrens-data-right-to-privacy-188048

