JCP prescription for Data Bill

Why in news?

The Joint Committee of Parliament (JCP) on the Personal Data Protection Bill has tabled its report.

Why the JCP was formed?

- With the growth of the Internet, consumers have been generating a lot of data, which has allowed companies to show them personalised advertisements based on their online behaviour.
- Companies began to store a lot of these datasets without taking the users' consent
- They also fail to take any responsibility when the data leaked.
- To hold such companies accountable, the government in 2019 tabled the Personal Data Protection Bill for the first time.
- The JCP was formed to deliberate on issues surrounding personal data protection.
- It expanded its mandate to include discussions on non-personal data, thereby changing the mandate of the Bill from personal data protection to broader data protection.
- In all, the committee has made 99 recommendations, of which 12 are in connection with the provisions made in the Bill, and the rest are in the form of modifications.
- In its report, the committee stressed a need to set up new processes to unify such data present across spectrums and organisations such as public and private sector companies, research organisations and academic institutions.

What are the major recommendations?

- **Non-Personal Data Too** - The key recommendation that changes the nature of the Bill itself is for inclusion of non-personal data within the larger umbrella.
- The reason, the committee said, was that it was impossible "to distinguish between personal data and non-personal data, when mass data is collected or transported".
- This means that all issues under the new legislation will be dealt with by a single Data Protection Authority (DPA) instead of separate ones for personal and non-personal.
- **Transition Period** - As technology has become an inseparable part of everyone's life, companies, firms and even government organisations deal with various kinds of data.
- For data aggregators to comply with the rules under the new Bill, the JCP suggested that up to 24 months be given from the date of notification of the Act.
- All data fiduciaries that deal exclusively in children's data have to register themselves with the DPA.
- For this, a period of 9 months from the notification of the Act has been suggested.
- **Social Media Liability -** Social media platforms that do not act as intermediaries should be treated as publishers.
- They will be held liable for the content they host.

- Confusion among stakeholders entails regarding these recommendation.
- As most social media companies are treated as intermediaries, a general consensus is that this would strip these companies of protections they are accorded under Section 79 of the Information Technology Act.

Section 79 in The Information Technology Act, 2000

- It provides for exemption from liability of intermediary in certain cases.
- An intermediary shall not be liable if
  - The function of the intermediary is limited to providing access to a communication system over which information made available by third parties is transmitted or temporarily stored or hosted.
  - the intermediary does not-
    - Initiate the transmission.
    - Select the receiver of the transmission, and
    - Select or modify the information contained in the transmission.
- However an intermediary shall be liable if
  - The intermediary has conspired or abetted or aided or induced, whether by threats or promise or authorise in the commission of the unlawful act.
  - or on being notified by the appropriate Government if the intermediary fails to expeditiously remove or disable access to that material.

- **Penalty** - The committee has recommended
  - A fine of up to Rs 15 crore or 4% of the total global turnover of the firm for data breaches.
  - A jail term of up to 3 years if de-identified data is re-identified.
- **Timely Alert** - In case of any data breach, the data aggregator or fiduciary must notify the DPA **within 72 hours** of becoming aware of it.
- The DPA shall then decide the quantum of severity of the data breach and accordingly ask the company to report it and "take appropriate remedial measures".

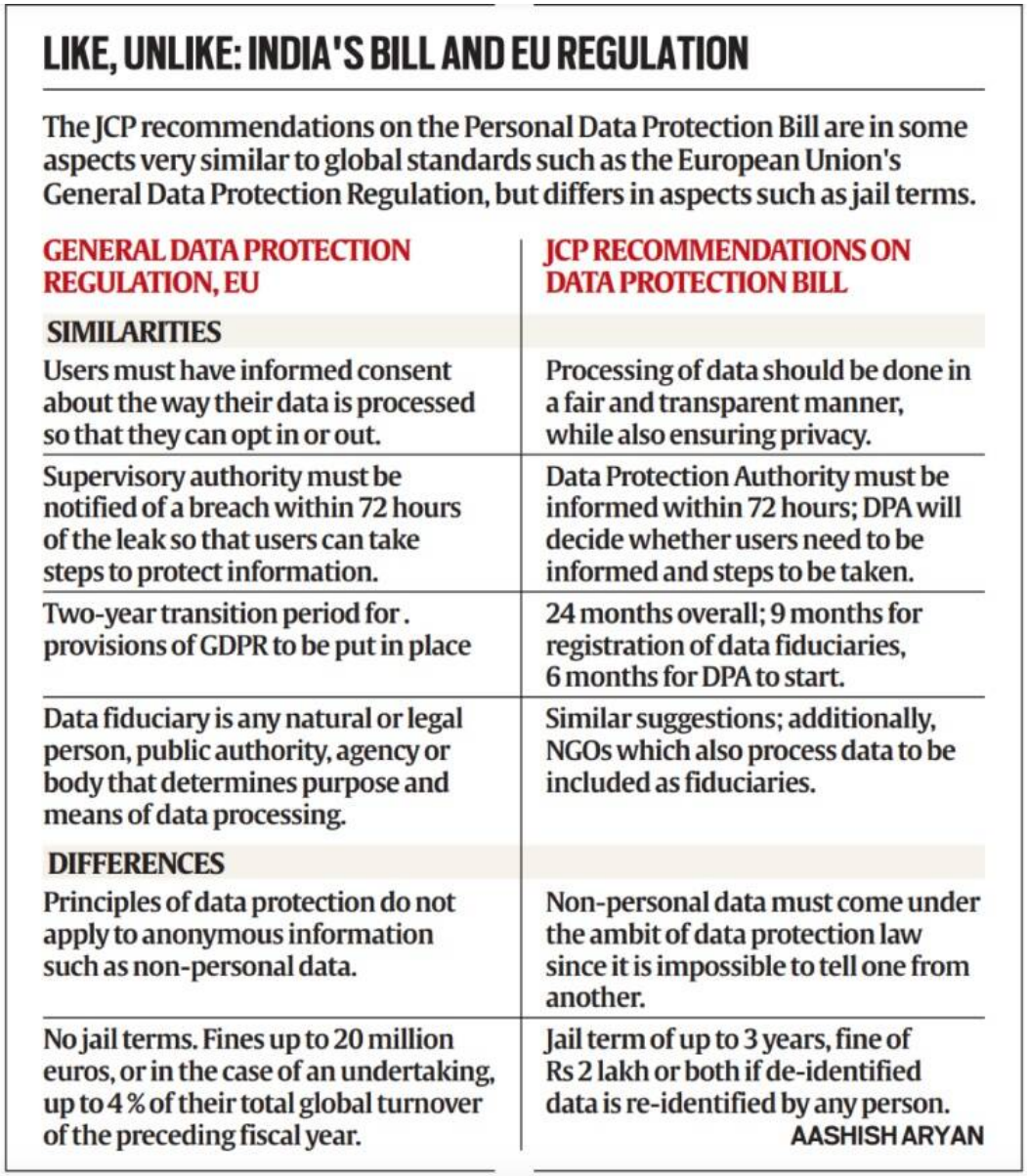
What factors did the JCP take into consideration?

- Among the major concerns that the JCP recommendations sought to address are
  - Data protection,
  - Minimal user trust in companies handling data,
  - Impact of data breaches on health and well-being of individuals,
  - Proliferation of bots
  - Fake accounts
  - Data localisation.

What are the other findings?

- The JCP said there was a sense of unease in the general public about what companies handling their data knew about them.
- This has resulted in undermining the end user trust and confidence.
- Concerns and tensions about misuse of sensitive and critical personal data are rising exponentially.
- To deal with such situations it was important to build a "legal, cultural, technological and economic infrastructure" for a secure and user-friendly data ecosystem.

- The JCP report also discusses the impact on mental health and emotional well-being that a user experiences due to a data breach.
- As much as 86% felt worried, angry and frustrated, while 85% experienced disturbed sleeping habits.



LIKE, UNLIKE: INDIA'S BILL AND EU REGULATION

The JCP recommendations on the Personal Data Protection Bill are in some aspects very similar to global standards such as the European Union's General Data Protection Regulation, but differs in aspects such as jail terms.

GENERAL DATA PROTECTION REGULATION, EU	JCP RECOMMENDATIONS ON DATA PROTECTION BILL
SIMILARITIES	
Users must have informed consent about the way their data is processed so that they can opt in or out.	Processing of data should be done in a fair and transparent manner, while also ensuring privacy.
Supervisory authority must be notified of a breach within 72 hours of the leak so that users can take steps to protect information.	Data Protection Authority must be informed within 72 hours; DPA will decide whether users need to be informed and steps to be taken.
Two-year transition period for . provisions of GDPR to be put in place	24 months overall; 9 months for registration of data fiduciaries, 6 months for DPA to start.
Data fiduciary is any natural or legal person, public authority, agency or body that determines purpose and means of data processing.	Similar suggestions; additionally, NGOs which also process data to be included as fiduciaries.
DIFFERENCES	
Principles of data protection do not apply to anonymous information such as non-personal data.	Non-personal data must come under the ambit of data protection law since it is impossible to tell one from another.
No jail terms. Fines up to 20 million euros, or in the case of an undertaking, up to 4 % of their total global turnover of the preceding fiscal year.	Jail term of up to 3 years, fine of Rs 2 lakh or both if de-identified data is re-identified by any person.

AASHISH ARYAN

Reference

1. https://indianexpress.com/article/explained/parliament-joint-committee-personal-data-protection-bill-explained-7678434/



IAS PARLIAMENT

Information is Empowering

A Shankar IAS Academy Initiative