IAS GS World PCS
Committed To Excellence

EXCLUSIVE Editorial Simplified

21 November 2022

The Hindu

Paper - II
(Indian Polity)

Data privacy:

A first look at the New Data Protection Bill

❖ **The latest draft of the data protection law — the Digital Personal Data Protection Bill, 2022 (DPDP Bill, 2022) — has now been made open for public comments and the government is expected to introduce the Bill in Parliament in the budget session of 2023.**

Is this the first draft?

This is the fourth iteration of a data protection law in India. The first draft of the law — the Personal Data Protection Bill, 2018, was proposed by the Justice Srikrishna Committee set up by the Ministry of Electronics and Information Technology (MeitY) with the mandate of setting out a data protection law for India. The government made revisions to this draft and introduced it as the Personal Data Protection Bill, 2019 (PDP Bill, 2019) in the Lok Sabha in 2019. On the same day, the Lok Sabha passed a motion to refer the PDP Bill, 2019 to a joint committee of both the Houses of Parliament. Due to delays caused by the pandemic, the Joint Committee on the PDP Bill, 2019 (JPC) submitted its report on the Bill after two years in December, 2021. The report was accompanied by a new draft bill, namely, the Data Protection Bill, 2021 that incorporated the recommendations of the JPC. However, in August 2022, citing the report of the JPC and the "extensive changes" that the JPC had made to the 2019 Bill, the government withdrew the PDP Bill.

Why have there been so many revisions and changes?

Constant interactions with digital devices have led to unprecedented amounts of personal data being generated round the clock by users (data principals). When coupled with the computational power available today with companies (data fiduciaries), this data can be processed in ways that increasingly impair the autonomy, self-determination, freedom of choice and privacy of the data principal.

The current legal framework for privacy enshrined in the Information Technology Rules, 2011 (IT Rules, 2011) is wholly inadequate to combat such harms to data principals, especially since the right to informational privacy has been upheld as a fundamental right by the Supreme Court (K.S. Puttaswamy vs Union of India [2017]). It is inadequate on four levels; first, the extant framework is premised on privacy being a statutory right rather than a fundamental right and does not apply to processing of personal data by the government; second, it has a limited understanding of the kinds of data to be protected; third, it places scant obligations on the data fiduciaries which, moreover, can be overridden by contract and fourth, there are only minimal consequences for the data fiduciaries for the breach of these obligations.

While the need to have an effective personal data protection regime is undisputed, India like other jurisdictions has struggled to come up with an optimum formulation for several reasons. First, while protecting the rights of the data principal, data protection laws need to ensure that the compliances for data fiduciaries are not so onerous as to make even legitimate processing impractical. Second, the challenge lies in finding an adequate balance between the right to privacy of data principals and reasonable exceptions, especially where government processing of personal data is concerned. Third, given the rate at which technology evolves, an optimum data protection law design needs to be future proof — it should not be unduly detailed and centred on providing solutions to contemporary concerns while ignoring problems that may emerge going forward. Fourth, the law needs to be designed for a framework of rights and remedies that is readily exercisable by data principals given their unequal bargaining power with respect to data fiduciaries.

What is the scope of the present formulation of the Bill?

The DPDP Bill, 2022 applies to all processing of personal data that is carried out digitally. This would include both personal data collected online and personal data collected offline but is digitised for processing. In effect, by being completely inapplicable to data processed manually, this provides for a somewhat lower degree of protection as the earlier drafts only excluded data processed manually specifically by "small entities" and not generally.

Data protection laws in other geographies

- An estimated 137 out of 194 countries have put in place legislation to secure the protection of data and privacy, with Africa and Asia showing 61% (33 countries out of 54) and 57% adoption respectively, according to data from the United Nations Conference on Trade and Development (UNCTAD), an intergovernmental organisation within the United Nations Secretariat. Only 48% of Least Developed Countries (22 out of 46) have data protection and privacy laws.
- **Europion Modal:** the EU's landmark General Data Protection Regulation or GDPR in force since May 2018, is clearly focused on privacy and requires individuals to give explicit consent before their data can be processed. A pair of sub-legislation — the Digital Services Act (DSA) and the Digital Markets Act (DMA) — take off from the GDPR's overarching focus on the individual's right over her data. The DSA focuses on issues such as regulating hate speech, counterfeit goods etc. while the DMA defines a new category of "dominant gatekeeper" platforms, and is focused on uncompetitive practices and the abuse of dominance by these players.
- US Modal: There is no comprehensive set of privacy rights or principles in the US that, like the EU's GDPR, addresses the use, collection, and disclosure of data. Instead, there is limited sector-specific regulation. The approach towards data protection is different for the public and private sectors. The activities and powers of the government vis-a-vis personal information are, however, sufficiently well-defined and addressed by broad legislation such as the Privacy Act, the Electronic Communications Privacy Act, etc. For the private sector, there are some sector-specific norms.
- CHINA MODEL: New Chinese laws on data privacy and security issued over the last 12 months include the Personal Information Protection Law (PIPL), which came into effect in November 2021. It gives Chinese data principals new rights as it seeks to prevent the misuse of personal data. The Data Security Law (DSL), which came into force in September 2021, requires business data to be categorized by levels of importance, and puts new restrictions on cross-border transfers.

Furthermore, as far as the territorial application of the law is concerned, the Bill covers processing of personal data which is collected by data fiduciaries within the territory of India and which is processed to offer goods and services within India. The current phrasing, inadvertently, seems to exclude data processing

by Indian data fiduciaries that collect and process personal data outside India, of data principals who are not located in India. This would impact statutory protections available for clients of Indian start-ups operating overseas, thereby impacting their competitiveness. This position further seems to be emphasised with the DPDP Bill, 2022 exempting application of most of its protections to personal data processing of non-residents of India by data fiduciaries in India.

How well does the DPDP Bill, 2022 protect data principals?

The bulwark of most data protection legislations consists of allowing maximum control to the data principal over their personal data. This happens by mandating a comprehensive notice to the data principal on different aspects of data processing based on which the data principal can provide explicit consent to such processing. While limited circumstances for non-consent based processing of personal data exists, it still gives the data principal the right to access, correct, delete etc their data. Concomitantly, the data fiduciary is placed, inter alia, with the obligation of data minimisation, which is to collect only such personal data as is required to fulfil the purpose of processing (collection limitation); process it only for the purposes stated and no more (purpose limitation) and to retain it in its servers only for so long as is required to fulfil the stated purpose (storage limitation).

What is the arrangement in this bill at present?

The current draft removes explicit reference to certain data protection principles such as collection limitation. This would allow a data fiduciary to collect any personal data consented to by the data principal. Making collection solely contingent on consent, ignores the fact that data principals often do not have the requisite know-how of what kind of personal data is relevant for a particular purpose. For example, a photo filter app may process data related to your location or information on your contacts even though it may not require such information to carry on its primary task of applying the filter. It also does away with the concept of "sensitive personal data". Depending on the increased potential of harm that can result from unlawful processing of certain categories of personal data, most data protection legislations classify these categories as "sensitive personal data". Illustratively, this includes biometric data, health data, genetic data etc. This personal data is afforded a higher degree of protection in terms of requiring explicit consent before processing and mandatory data protection impact assessments. By doing away with this distinction, the DPDP Bill, 2022 does away with these additional protections.

Additionally, the Bill also reduces the information that a data fiduciary is required to provide to the data principal. While the previous iterations required considerable information in terms of the rights of the data principals, grievance redressal mechanism, retention period of information, source of information collected etc to be provided for the data principal, the current draft reduces the scope of this information to the personal data sought to be collected and the purpose of processing the data. While this may have been done in an attempt to simplify the notice and avoid information overload, there are other ways such as infographics, just-in-time notices etc that are being recommended by data protection authorities to ensure a comprehensive yet comprehensible notice.

Moreover, the DPDP Bill, 2022 seems to suppose that a notice is only to be provided to take consent of the data principal. This is a limited understanding of the purpose of notice. A notice is also important for the data principal to exercise data protection rights such as the right to know what personal data is being processed by whom, whether that data needs correction or updation and also to request deletion of data that may not be relevant for the purpose of processing. These rights exist even in cases of non-consent based processing of data. As such, limiting notice to only consent based personal data processing would limit the scope for the exercise of these rights.

What else in this bill?

The DPDP Bill, 2022 also introduces the concept of "deemed consent". In effect, it bundles purposes of processing which were either exempt from consent based processing or were considered "reasonable purposes" for which personal data processing could be undertaken under the ground of "deemed consent". However, there exist some concerns around this due to the vaguely worded grounds for processing such as "public interest" and the removal of additional safeguards for protection of data principals' interests. An important addition to the right of data principals is that it recognises the right to post mortem privacy which was missing from the PDP Bill, 2019 but had been recommended by the JPC. The right to post mortem privacy would allow the data principal to nominate another individual in case of death or incapacity.

Expected Question

Que. Consider the following statements-

1. In KS Puttaswamy v. Union of India, the right to informational privacy has been upheld as a fundamental right by the Supreme Court.
2. This data protection law has been introduced in India for the fourth time.

Which of the above statements is/are true?

(a) 1 only (b) only 2

(c) all of the above (d) None of the above

Answer : C

Mains Expected Question & Format

Que.: Recently the latest draft of data protection law has been introduced, while discussing its various aspects, what is its relevance at present?

Answer Format :

- **Introduction (40-50 words)**

  Briefly describe the latest draft of the data protection law that has been introduced.

- **Main Body (140-160 words)**

  State what and for what data protection law has been introduced and state its positive and negative aspects.

- **Conclusion (30-40 words)**

  State its relevance at present.

Note: - The question of the main examination given for practice is designed keeping in mind the upcoming UPSC mains examination. Therefore, to get an answer to this question, you can take the help of this source as well as other sources related to this topic.