Data Protection Bill — issues, debate

Writer - Karishma Mehrotra (Editor)

This article is related to General Studies-Paper-III (Internal Security Cyber Security)

Indian Express

6 Dec., 2019

"Cleared by the Cabinet, the Personal Data Protection Bill is due to be placed in Parliament. How does it propose to protect personal data, how is it different from previous draft, and why is it a subject of debate?"

Global negotiations today revolve around debates about the transfer of data. India's first attempt to domestically legislate on the topic, the Personal Data Protection (PDP) Bill, 2019, has been approved by the Cabinet and is slated to be placed in Parliament this winter session. The Bill has three key aspects that were not previously included in a draft version, prepared by a committee headed by retired Justice B N Srikrishna.

Why does data matter?

Data is any collection of information that is stored in a way so computers can easily read them (think 011010101010 format). Data usually refers to information about your messages, social media posts, online transactions, and browser searches.

The individual whose data is being stored and processed is called the data principal in the PDP Bill. This large collection of information about you and your online habits has become an important source of profits, but also a potential avenue for invasion of privacy because it can reveal extremely personal aspects. Companies, governments, and political parties find it valuable because they can use it to find the most convincing ways to advertise to you online. It is now clear that much of the future's economy and law enforcement will be predicated on the regulation of data, introducing issues of national sovereignty.

Who handles my data, and how?

Data is stored in a physical space similar to a file cabinet of documents, and transported across country borders in underwater cables that run as deep as Mount Everest and as long as four times the Indian Ocean. To be considered useful, data has to be processed, which means analysed by computers.

Data is collected and handled by entities called data fiduciaries. While the fiduciary controls how and why data is processed, the processing itself may be by a third party, the data processor. This distinction is important to delineate responsibility as data moves from entity to entity. For example, in the US, Facebook (the data controller) fell into controversy for the actions of the data processor — Cambridge Analytica.

The physical attributes of data — where data is stored, where it is sent, where it is turned into something useful — are called data flows. Data localisation arguments are premised on the idea that data flows determine who has access to the data, who profits off it, who taxes and who "owns" it. However, many contend that the physical location of the data is not relevant in the cyber world.

How does the PDP Bill propose to regulate data transfer?

To legislate on the topic, the Bill trifurcates personal data. The umbrella group is all personal data — data from which an individual can be identified. Some types of personal data are considered sensitive personal data (SPD), which the Bill defines as financial, health, sexual orientation, biometric, genetic, transgender status, caste, religious belief, and more. Another subset is critical personal data. The government at any time can deem something critical, and has given examples as military or national security data.

In the Bill approved by the Cabinet, there are three significant changes from the version drafted by a committee headed by the Justice B N Srikrishna Committee.

- The draft had said all fiduciaries must store a copy of all personal data in India — a provision that was criticised by foreign technology companies that store most of Indians' data abroad and even some domestic startups that were worried about a foreign backlash. The approved Bill removes this stipulation, only requiring individual consent for data transfer abroad. Similar to the draft, however, the Bill still requires sensitive personal data to be stored only in India. It can be processed abroad only under certain conditions including approval of a Data Protection Agency (DPA). The final category of critical personal data must be stored and processed in India.
- The Bill mandates fiduciaries to give the government any non-personal data when demanded. Non-personal data refers to anonymised data, such as traffic patterns or demographic data. The previous draft did not apply to this type of data, which many companies use to fund their business model.
- The Bill also requires social media companies, which are deemed significant data fiduciaries based on factors such as volume and sensitivity of data as well as their turnover, to develop their own user verification mechanism. While the process can be voluntary for users and can be completely designed by the company, it will decrease the anonymity of users and "prevent trolling", said official sources.

What are its other key features?

The Bill includes exemptions for processing data without an individual's consent for "reasonable purposes", including security of the state, detection of any unlawful activity or fraud, whistleblowing, medical emergencies, credit scoring, operation of search engines and processing of publicly available data, official sources said.

The Bill calls for the creation of an independent regulator DPA, which will oversee assessments and audits and definition making. Each company will have a Data Protection Officer (DPO) who will liaison with the DPA for auditing, grievance redressal, recording maintenance and more. The committee's draft had required the DPO to be based in India.

The committee's draft had several other significant keywords that are expected to be in the Bill. "Purpose limitation" and "collection limitation" limit the collection of data to what is needed for "clear, specific, and lawful" purposes or for reasons that the data principal would "reasonably expect". It also grants individuals the right to data portability, and the ability to access and transfer one's own data. Finally, it legislates on the the right to be forgotten. With historical roots in European Union law, this right allows an individual to remove consent for data collection and disclosure. After the Cabinet approval of the bill, an official source said this concept is still "evolving" and has not been "concretised" yet.

Government sources said they were open to the "widest debate on this Bill".

What are the two sides of the debate?

For data localisation-

A common argument from government officials has been that data localisation will help law-enforcement access data for investigations and enforcement. As of now, much of cross-border data transfer is governed by individual bilateral "mutual legal assistance treaties" — a process that almost all stakeholders agree is cumbersome. In addition, proponents highlight security against foreign attacks and surveillance, harkening notions of data sovereignty.

The government doubled down on this argument after news broke that 121 Indian citizens' WhatsApp accounts were hacked by an Israeli software called Pegasus. Even before that, the argument was used prominently against WhatsApp when a spate of lynchings across the country linked to rumours that spread on the platform in the summer of 2018. WhatsApp's firm stance on encrypted content have frustrated government officials around the world.

Many domestic-born technology companies, which store most of their data exclusively in India, support localisation. PayTM has consistently supported localisation (without mirroring), and Reliance Jio has strongly argued that data regulation for privacy and security will have little teeth without localisation, calling upon models in China and Russia. Many economy stakeholders say localisation will also increase the ability of the Indian government to tax Internet giants.

Against the Bill

Civil society groups have criticised the open-ended exceptions given to the government in the Bill, allowing for surveillance. Moreover, some lawyers contend that security and government access are not achieved by localisation. Even if the data is stored in the country, the encryption keys may still be out of reach of national agencies.

Technology giants like Facebook and Google and their industry bodies, especially those with significant ties to the US, have slung heavy backlash. Many are concerned with a fractured Internet (or a "splinternet"), where the domino effect of protectionist policy will lead to other countries following suit. Much of this sentiment harkens to the values of a globalised, competitive internet marketplace, where costs and speeds determine information flows rather than nationalistic borders. Opponents say protectionism may backfire on India's own young startups that are attempting global growth, or on larger firms that process foreign data in India, such as Tata Consulting Services and Wipro.

Expected Questions (Prelims Exams)

1. Consider the following statements in the context of Personal Data Protection Bill, 2019.

1. The Bill includes the right to store all types of sensitive data only in India in the Data Protection Report submitted by B.N. Krishna Committee.
2. There is a provision to constitute the Data Protection Agency (DPA) as an independent regulator for data assessment and audit
3. A data security officer in each company will consult the data protection agency regarding auditing, grievance redressal and record maintenance.

Which of the above statements is/are correct?

(a) 1 and 2 (b) 2 and 3

(c) 1 and 3 (d) 1, 2 and 3

Expected Questions (Mains Exams)

Q. Data will be the key to every diplomacy and every strategy of the future, so its protection and localization is very important for any country. Analyze this statement. (250 words)

Note: Answer of Prelims Expected Question given on 5 Dec., is 1 (c)