THE DRAFT DIGITAL PERSONAL DATA PROTECTION BILL, 2022: SOME KEY FEATURES AND CONCERNS

Written by ***Susmit Mukherjee***

2nd Year B.A., LL.B. (Hons.) Student, NALSAR University of Law, Hyderabad, India

DOI: 10.55662/JLSR.2023.9504

THE DRAFT DIGITAL PERSONAL DATA PROTECTION BILL, 2022 – AN INTRODUCTION

The Government of India, through the Ministry of Electronics and Information Technology or 'MeitY' officially released the Draft Digital Personal Data Protection Bill on 18th November 2022 and invited applications from the public concerning feedback and relevant suggestions to be submitted by 17th December 2022 (the deadline was later extended to 2nd January 2023 in light of requests from multiple stakeholders). This marks the fourth attempt by the Government of India to construct a specific set of laws aimed at Data Protection and individual privacy in online platforms.[i]

The attempts to draft such a Bill started with the Union Government creating an expert parliamentary committee under the leadership of Justice BN Srikrishna, which presented a Personal Data Protection Bill before the MeitY in July 2018, which was never enforced and was instead used by the MeitY to draft the Personal Data Protection Bill in December 2019. This Bill was then reviewed by a special Joint Parliamentary Committee, which released a report on the same, along with a draft Data Protection Bill 2021 to be presented in the Parliament. The present Bill arrived after the MeitY decided to withdraw the draft Data Protection Bill 2021 owing to certain unacceptable changes made to the original Data Protection Bill passed in 2019.

Till now, the issue of data privacy has been (and continues to be) addressed under the Information Technology Act of 2000 and the Information Technology Rules. Both of these legislations have so far proved inefficient in keeping up with the dizzying rate of technological

advancements and satisfying the growing need for data privacy, especially after the famous Justice K.S. Puttaswamy vs Union of India[ii] judgement in 2017, wherein the Supreme Court ruled that the right to privacy was a fundamental right. Furthermore, companies and organisations (with much greater bargaining power) that use data made accessible before them are often able to get away with using the same without as much as making the rightful owners of the same (referred to as 'Data Principals') aware of the fact that their right to privacy is being breached. Hence, properly drafted legislation in the form of the Draft Digital Personal Data Protection Bill, 2022, made to protect the interests of the Data Principals and balance the inequality of power between the Data Principals and Data Fiduciaries (individuals or institutions processing and using personal data) by placing them both on an equal footing was definitely the need of the hour.

THE DRAFT DIGITAL PERSONAL DATA PROTECTION BILL, 2022 AT A GLANCE – SOME KEY FEATURES

To begin with, the act aims to create a system of processing data in a way that recognises the rights of the Data Principal to safeguard their data along with the need for processing the data for lawful purposes and also "for matters connected therewith or incidental thereto".

The Scope: The provisions provided by this Act are applicable only to the act of processing personal data (in a digital form) within the territorial boundaries of India. However, persons operating outside India who engage in processing the digital personal data of Data Principles based in India shall also fall under its jurisdiction. Such personal data is restricted only to data collected in an online platform from Data Principals and digitalised versions of data collected in an offline medium.

Obligations of Data Fiduciaries along with the Rights and Duties of Data Principals: Chapter 2 (Sections 5 – 11) of the Act covers the Obligations of Data Fiduciaries, while Chapter 3 (Sections 12 – 16) deals with the rights, remedies and duties of Data Principals coming under the umbrella of the Act.

The Data Protection Board of India: Section 19 of the Act gives the Central government the responsibility to establish, as the guardians of this Act, the Data Protection Board of India, the functions (both internal and external) of which shall be carried out digitally.

Transparency: Section 6 of the Act clearly states that a Data Fiduciary must, before seeking consent from the concerned Data Principal, provide the Data Principal with "an itemised notice in clear and plain language" listing out the description of the data it seeks to collect along with the reason why such data needs to be processed. In cases wherein the Data Principal has already given/plans to give consent to the Data Fiduciary to process their personal data before the Act comes into power, the Data Fiduciary is compulsorily required to provide a similar notice providing a detailed description of the personal data collected from the Data Principal so far and the reason(s) why such data has been collected and processed once the Act comes into power.

Exemptions pertaining to the Central Government and its agencies: Section 18 (2) of the Act gives the Central Government the power to, by notification, exempt from this Act the acts of processing personal data by any State body to protect the sovereignty and integrity of the State, for maintaining good relations with other States, in the interests of maintaining public order and preventing the commission or incitement of any offences in relation to these grounds. The exemptions can also extend to the processing of data for "research, archiving or statistical purposes", provided the personal data being used would not be used to make any decisions concerning a specific Data Principal and such processing of data is conducted strictly according to the standards and guidelines set by the Data Protection Board of India.

Section 18 (4) clearly states that the provisions of Section 9 (6) are not applicable to the State or any State agency. Section 9 (6) instructs Data Fiduciaries to stop retaining personal data from Data Principals or ensure that the personal data cannot be, in any way, associated with the respective Data Principals once it can be reasonably inferred that the retaining of such personal data is no longer serving the originally intended purpose and continuing the act of retention of personal data is not required for any business or legal purpose.

Transfer of data under the ownership of Data Principal(s) to places outside the Indian territory: Transfer of such data by Data Fiduciaries only to foreign countries notified by the

Central Government after assessing as many factors "as it may consider necessary" is allowed under this Act in conformity with certain terms and conditions (if applicable).

***Prescribed penalties for non-compliance with the provisions of the Act*:** The Draft Digital Personal Data Protection Bill, 2022 imposes penalties, ranging from up to Rs 10 thousand to up to Rs 250 crore for certain violations (non-compliance with specific provisions of the Act) which have been defined in the Act itself (under Schedule 1). That being said, it is the Board that ultimately exercises the power to impose financial penalties for non-compliance with the provisions given in the Act. The Bill also clearly mentions the factors to be considered by the Board while determining the amount of financial penalty (under Section 25 (2)).

Provision for Data localization: Laws on Data localization mandatorily require data about (and belonging to) the people of a particular country to either be collected and processed or stored inside the country or in territories within its jurisdiction. Data localization helps combat the uncontrolled free flow of valuable data and ensures security by preventing crime (law enforcement authorities get speedier access to personal data) and protecting the country from foreign surveillance. Data localization also makes it much easier for the government to secure local data in the event of foreign conflict and geopolitical instability. The Bill does not contain any specific provisions regarding data localization.[iii]

Post-Mortem privacy: Section 15 of the Act gives the Data Principal the right to nominate an individual to take the place of the Data Principal "in the event of death or incapacity" and exercise the rights associated with such a position according to the provisions given in the Act.[iv]

CONCERNS REGARDING SOME OF THE DRAWBACKS OF THE BILL

There is a high possibility of the Bill facilitating unsupervised data processing by the State authorities which can, in turn, violate the Data Principal's fundamental right to privacy[v]: As mentioned earlier, the Bill grants the State the power to exempt the acts of processing of data by its agencies from the purview of some or all the provisions of the Act for the purpose of State security, public order etc.. Hence, the rights of Data Principals together with the obligations of

Data Fiduciaries would cease to remain valid (with the exception of Data Security) in such cases. The State also has the power to continue retaining data and not delete previously collected data even when the purpose of collecting such data from the Data Principal has already been served. Misuse of these powers by the State can lead to government bodies monitoring and profiling the people of India on any of the abovementioned grounds of exemption (For example - State security) without any regard to individual privacy.

The provisions of the Bill are unfairly biased towards Government bodies as the rights and privileges enjoyed by them are not made available to their private counterparts performing the exact same function(s)[vi]: Section 8 (2) of the Act clearly specifies that a Data Principal "is deemed to have given consent" to the State for the processing of personal data if such data is required by the State or any of its respective agencies for issuing a license, certificate or permit allowing the Data Principle to freely perform "any action or activity" (For example – Agriculture Income Support). As mentioned above, the State can also keep such data for an unlimited period of time. At the same time, the equivalents of State-run services in the private sector have to go great lengths to follow proper procedure for obtaining consent and unlike State-run services, are also bound by Section 9 (6) of the Act. This differential treatment goes against Article 14 of the Indian Constitution (Equality before law).

The provisions of the Bill do not guarantee the independent functioning of the Data Protection Board of India[vii]: Section 19 (1) of the Act gives the Central Government the responsibility of creating the Board. According to Section 19 (2), the composition, selection procedure, terms and conditions of service and dismissal of the Chairperson (or any other member) shall be prescribed by the Central Government itself. Section 19 (3) also clearly states that the Central Government shall appoint the Chief Executive of the Board (who is in charge of managing all its affairs) whose terms and conditions of service shall be determined by the Central Government. Given the large amounts of personal data processed by the Central Government on a daily basis, there would be times when the Board would have no choice but to investigate State agencies. Taking into consideration the enormous amount of power and authority the Government of India has over the Board, a very fundamental question arises as to how 'independently' the Board would be able to function in such situations.

***The process of verification of age to check if the person using a particular online platform is a child or not would be problematic for users who wish to remain anonymous*:** Section 10 (1) of the Act mandatorily requires Data Fiduciaries to get "verifiable parental consent" before processing the personal data belonging to a child. However, where the Data Fiduciary is an online platform, it would have no choice but to verify the age (For example – by asking to upload the birth certificate or other identifying information) of every single user who submits data in that platform in order to verify if that particular user is a child (under the age of 18 according to Section 2 (3) of the Act) or not. This would lead to an issue of privacy for users of a particular online platform who would prefer to remain anonymous.

The Bill associates the requirement for a notice with only obtaining 'consent' from the Data Principal: As mentioned earlier, Section 6 of the Act makes it very clear that a notice is to be sent by the Data Fiduciary solely for the purpose of seeking consent from the Data Principal to process their personal data. This narrows down the scope of usage of notices to only personal data obtained through consent and not personal data being processed without consent. Notices can also be used by Data Fiduciaries to keep Data Principals notified about what aspects of their personal data are being processed (and most importantly, by whom), if the previously collected data needs to be updated, if certain personal data previously listed in the original notice (the one seeking consent for processing of data) is not required anymore and the Data Principal has the right to delete the same if they wish etc.. Reducing the use of notices to only obtaining consent prevents the Data Principal from enjoying such services.

CONCLUSION

In this day and age, there is no doubt that the need for a properly drafted legal framework on data protection is more than ever before. As India continues to make massive strides in the field of Information Technology, more and more people are slowly realising the need for 'going digital' and embracing the internet, not as a luxury but as a necessity. Hence, the Digital Personal Data Protection Bill, 2022 is certainly a step in the right direction and is symbolic of the changing times and a need to reflect on how far we have come and how much we have overcome to get where we are right now.

There have been numerous attempts to enact such a legislation in the past and there is no doubt that that there would be attempts to replace the same with much better and up-to-date legislations in the future. It remains to be seen if the Digital Personal Data Protection Bill, 2022 would actually come into power after being put up before the Monsoon Session of the Parliament in July.[viii] Even if it does, the Bill is far from perfect and would require numerous modifications down the road to ensure that it caters to the needs of all concerned stakeholders. This can only be achieved through rigorous in-depth discussions among the stakeholders (who should all be on an equal footing) in a common platform.

ENDNOTES

[i] Saransh Jauhari and Chitrakshi Kapgate, The Digital Data Protection Bill, 2022 and the concerns associated, 14 December 2022 6:05 PM, The Digital Data Protection Bill, 2022 And The Concerns Associated (knimbus.com) (accessed on 12th May 2023)
[ii] K.S. Puttaswamy and Another v. Union of India and Others, SCC Online, 2017 SC 3
[iii] Sanjay Notani, Vinay Butani, Naghm Ghei, Divyashree Suri, Overview of the Digital Personal Data Protection (DPDP) Bill, 2022, Overview of the Digital Personal Data Protection (DPDP) Bill, 2022 | ELPLAW, (accessed on 12th May 2023)
[iv] Trishee Goyal, A first look at the new data protection Bill, November 20, 2022 10:52 PM, A first look at the new data protection Bill - The Hindu (accessed on 12th May 2023)
[v] Ministry: Electronics and Information Technology, Draft Digital Personal Data Protection Bill, 2022, Draft Digital Personal Data Protection Bill, 2022 (prsindia.org) (accessed on 12th May 2023)
[vi] Id.
[vii] Id.
[viii] Krishnadas Rajagopal, New Digital Personal Data Protection Bill in Monsoon Session, April 11, 2023 12:56, New Digital Personal Data Protection Bill in Monsoon Session - The Hindu (accessed on 12th May 2023)