CRITICAL ANALYSIS OF THE PERSONAL DATA PROTECTION BILL, 2018 & 2019

-RICHA GUPTA[1]

The Data Protection Bill was drafted in the year 2018 by a nine-member expert committee, headed by *Justice B N Srikrishna*. The said Committee with its purpose to formulate an extremely efficient and operative data protection law for India, post its deliberations and ruminations submitted its report along with draft bill, christened as "***The Personal Data Protection Bill, 2018"***.[2] The Bill was capitulated to the *Ministry of Electronic and Information Technology* on July 27, 2018. It is an exceedingly noteworthy progression in the advancement of over-all Indian data protecting laws. The Bill acknowledges privacy as a fundamental right and embodies a transformative alteration in the prevailing legislative framework with regards to Data Protection in India.[3] The Data Protection Bill derives its provisions from the GDPR which stands for *General Data Protection Regulations of the European Union*.[4] The Bill has been ushered in at an exceptionally paramount time and finds its premise in the recent judicial judgment of the Supreme Court case of Justice *K. S. Puttaswamy (Retd.) & Anr. v. Union of India & Ors*[5] which concedes Right to Privacy as Fundamental Right.

Cyber Crime cases in India and globally have been unbridled. They not only encompass the grave crime of stealing the data but also cover the sale of the stolen data which transverses across continents barring any constraint with regards to boundaries. This era of technology progression can be classified as *Hi-tech*, which is coupled with plentiful resources and unfathomed expertise of technology.[6] India's state of Data Security has not always been very sound, and being one of

[1] 4th YEAR, BBA LL. B (HONS), SYMBIOSIS LAW SCHOOL, PUNE
[2]Committee of Experts under the Chairmanship of Justice B N Srikrishna, "Report of the Committee of Experts under the Chairmanship of Justice B N Srikrishna," Committee Report (India: Ministry of Electronics & Information Technology, Government of India, July 27, 2018).
[3] "The Information Technology Act, 2000," Government of India, June 9, 2000.
[4](EU) 2016/679 (General Data Protection Regulation).
[5] K. S. Puttaswamy (Retd.) & Anr. v. Union of India & Ors, W.P. (Civil) No. 494 of 2012.
[6] Philip E. Agre, "*Marc Rotenberg bTechnology and privacy: The new landscape*", July 3, 1998.

the major players in outsourced data processing in the world, India could very well be targeted with the epidemic of cyber-crime due to the truancy of a suitable solid data protection framework. There is a perceptible absence of provisions on Digital/Cyber security in India and the same has to be supported by strong cyber securing mechanisms.[7]

Indian *BPO Companies and Information Technology Centre* possess confidential information in abundance as they have unconstrained access to personal data of individuals spanning through various continents and nations. These companies handle the minutest of details such as that of credit cards, medical history, personal history, family backgrounds etc. This clearly demarcates that the companies and its officials or employees possess sensitive and vulnerable details profusely about an individual. The collection of information can be misappropriated by a number of people at whose behest the same is stored. There can be undue usage of the information, breaches, leakage of confidential date etc.

The *Personal Data Bill*, was initially introduced in the parliament in the year 2006, with deriving its formulations post extensive deliberations from framework of GDPR.[8] The proposed Bill follows a very all-inclusive model, it targets to explain the collection, processing and distribution of personal data.[9] The Bill at large, is a step towards the construction of a secure cyber space for all the citizens, but it stands pending for its due approval, due to the lacunae present in the bill. The bill not only smears on government enterprises but is equally applicable on private enterprises, engaged in the business of data functions.[10] The bill also covers the appointment of personnel such as Data Controllers who have adjudicatory powers and authority to govern over the wide range of subjects incapsulated in the bill. The Bill also lays down stringent application of punishment in terms of providing adequate compensation for damages to the affected victims.[11]

The Data Protection Bill, regulates the personal data of citizens that is processed by government companies and foreign companies. With the advent of the bill, the Government through a solid

[7] Data Protection Law in India-Needs and Position, Adv. Swati Sinha, 2018.
[8] European Commission, "2018 Reform of EU Data Protection Rules," Text, European Commission, accessed March 7, 2019.
[9] Section 3(32), Bill.
[10] *Ibid.*
[11] Section 75, Bill.

legislation in place is aiming to formulate a framework to authorize data of certain classes to be stored within Indian borders. In this way, the framers are by and large aiming at data sovereignty.[12] The Bill also, enables the processing of data by fiduciaries with the prior consent of the individual the concerned data belongs to and has to go through due processing. Data Fiduciaries comprises of entities or individuals which decide the purpose of personal data processing.[13]

ANALYSIS

The report of the nine-member expert committee along with the draft bill, must be considered as a jump start point in the long process of data protection. At one end, the positives of the bill can be looked at but from the other end it is imperative to understand the imperfections of the draft bill. India is the world's largest democracy and it holds the burden to set high standards and expectations in terms of protections of its civil rights and liberties. The Bill, in its form provides the reforms of transparency, security safe guards, privacy, collection limit, storage limit etc.[14] However, the bill lacks in various aspects, such as it does not postulate the concepts of notification breach, cross border data transfer, interception of communication etc. Unfortunately, these are some of the issues that weren't addressed in the draft bill apart from the pool of other issues that are of high importance. The bills, aims at an enactment of a law that will protect the privacy rights of the citizens and therefore, it is important that a public consultation with a draft of proper modifications must be entertained in order to improve the standing of the Bill.

The Bill is to be applied to activities that were connected to processing the personal data available within the territory or boundaries of India, by an Indian company incorporated in India, Indian state or any citizen, who is in link with a business carried on in India, which incorporates offering goods and services to people in India. The Bill also aimed at creating two new bodies, that are the DPAI, *Data Protection Authority of India* and the *Appellate Tribunal*.[15]

[12] Section 12(1), Bill.
[13] Paragraph B (1), Chapter 4, Page 51 of the Report.
[14] Section 29&30, Bill.
[15] Section 22, Bill.

Central Government as per the Bill,[16] has been empowered with excessive power, where it can also command and issue directions to the DPAI.

The Bills undertakes the task of enumerating a few terms extensively. Like, a "*Data Fiduciary*" decides what necessarily has to be done with the data, a "*Data Processor*" assumes the duty to process the data of a natural principal, who is coined as the "*Data principal*".[17] The Government (State) is incapsulated in the ambit of the terms data fiduciary and data processors, but the State enjoys various exemptions and bypass the procedure if the requirement be. Another important distinction the bill embarks upon is between the meaning of the terms, *de-identification* and *anonymisation.*[18] The term De-identifications, derives its meaning from the EU GDPR.[19] It primarily, assigns a unique non-personal identifier for a certain data and removes the personal identification from that particular data. Nonexistence of attachment of an identifier with the data leads to it being categorized as anonymised, as it lacks a method of re-identification.

Currently in India, the *Information Technology Act, 2000*, provided the protection of personal sensitive data under its Section 43A.[20]This Bill, aims to amend the existing provision of laws and seeks to exceedingly expand the scope of *Right to Information Act, 2005* as well.[21] The Bill also lays down certain requirements for a consent to be valid, provided that it must be informed, specific, clear, free and capable of being withdrawn.[22] The requirement of notice is laid down in the Bill in detail. Additionally, it implies to provide the data principal with the required and necessary minute details in the notice, which eventually comes out to be a long read which sometimes leads to the dearth of consent. The data principal has been empowered with the ability to withdraw consent, but this comes at the price of bearing the legal consequences of the same, which might not be favourable at all times.

As mentioned in the aforementioned paragraph, the concept of consent was introduced but at the same time it was highly thinned in the Bill. A wide exception was provided, in case if sensitive personal information was to be processed for disseminating an important function of the

[16] Section 66, Bill.
[17] Section 3(14), Bill.
[18] Section 61(6)(m), Bill.
[19] Supra 7.
[20] Section 43A, Information Technology Act, 2000.
[21] Rule 3 of the Information Technology (Reasonable security practices and procedures and sensitive personal data or information) Rules, 2011.
[22] Section 12(2), Bill.

parliament or state, which was duly authorized by law. With the advent of the Bill, the DPAI was also empowered to allow the processing of personal data for some purposes without consent. Some of them included the detection of unlawful and deceitful activities such as fraud, whistleblowing etc.[23]

The key features of the bill have been explained in the aforementioned paragraphs, the author will now be *analyzing the key issues in the draft bill*.

The Bill in its draft does define terms such as, *the date principal and the data fiduciary*. While the data is processed by the fiduciary, they have to corroborate, that the same is processed in manner that is *reasonable and fair* [24]and at the same time it respects the privacy and dignity of the individual. The fiduciary in its duty to process the data must be able to demonstrate the same to the DPA, i.e. the Data Protection Authority, with the data being processed in a righteous manner. Fiduciary's failure to comply to this provision can also attract monetary penalty. As per the author's observation the Bill puts an active obligation on the fiduciary, but fails to itemize or design a set guideline as to what would rightly constitute "*fair and reasonable*" under the said bill. Truancy of the meaning of the same leads to a wide interpretation of the connotation "*fair and reasonable*",[25] and leads to various fiduciaries devising different standards to measure the same. As per the author, a basic guideline of the same would enable better compliance of the provision.

Secondly, the bill states that the DPA must be duly informed if an unfortunate mishap of a data breach takes place, since the DPA is a body that ensures due compliance and undertakes effective enforcement of action and implication of penalty.[26] The DPA must be informed primarily if the data breached leads it any sort of harm to any data principal. The grey area in this provision was with regards to the discretion to be exercised by the fiduciary on the selective reporting of data breaches to the DPA. There also exited the conflict of interest during the reporting of low impact data breach and also making the reporting of breach an onerous duty on the fiduciary.

[23] Section 17(2), Bill.
[24] Paragraph B (1), Chapter 4, Page 51 of the Report.
[25] Section 4, Bill.
[26] Section 32, Bill.

In further analysis, it was noted that the fiduciary is mandatorily required to provide notice to the principal and obtain their consent before the data processing begins. [27]The data can be utilized for a specified purpose only and has to be stored with adequate security safeguards. Also, the data principal exercises the right to obtain summary of their personal data held with the fiduciary and if required they can seek the correction of inaccurate and incomplete data that is stored with the fiduciary.[28] However, these provisions do not apply on the fiduciary, in a scenario where the data is processed for purposes such as national security, legal proceedings, personal purposes etc.[29] The grey area that arises here is with regards to whether the exemptions are warranted in the bill clearly. This leads to the problem of questioning of certain kinds of exemptions under data processing.

Another issue arising at large was not acquiring consent for the processing of data for functions of the state, as the bill allowed the processing of an individual's personal data for dissemination of any function of the state without their prior consent if necessary, but it did not lay down as to what functions of the legislature or parliament would necessarily enable this provision to follow, where the absence of consent would not be an issue.[30]

The Bill required every fiduciary to retain a "*serving copy"* of all the sensitive personal data in a server.[31]The Government may also notify a certain "*critical personal data*" which would allow the processing of data in servers located in India.[32] The grey area, in this provision was unclarity on the meaning of serving copy and critical personal data. Clear specifications with regards to the same were required as the implications of same would vary for different fiduciaries as per their nature. The Bill has specifically recognized various benefits of local storage of data as it would enable better access for investigation to enforcement agencies and would also prevent the unrequited surveillance of Indian citizens. However, this was not very efficient as it played a deterrent for other fiduciaries to invest in India and also had an adverse impact on others who had resorted to cheaper mechanisms of data storage.

[27] Section 8(1), Bill.
[28] Section 8(2), Bill.
[29] Section 8, Bill.
[30] Section 13, Bill.
[31] 8 Section 40, Bill.
[32] 9 Section 40(2), Bill.

Additionally, it was observed that the Bill provided certain rights to the data principal in terms of taking control of their data. However, it was also observed that a complaint could only be raised by the data principal if there was possibility of harm. This somehow led to the issues of a question being raised with regards to, if the mere violation of principal's right wasn't enough to raise a complaint.[33]

Lastly, the Bill required the DPA to ensure that the penalties were imposed in case there were violations in law. Recovery Officers were also appointed for the same for the enforcement of actions against fiduciaries and to ensure the victims got their compensations and the criminals were arrested, detained, had their properties attached.[34] However, the grey area with regards to this proviso did not specify the requirement of a court order for the aforementioned enforcement orders.

SUGGESTIONS & CONCLUSION

In conclusion, it is noted by the Author that the draft bill proposed is a good step towards framing a solid legislative framework for Data Protection security laws in India. However, it is not very comprehensive and consists of lacunae that can be rectified by amendments in the draft bill by expert committees. India, has created the Draft bill in in a comparatively shorter time period than its inspiration source, i.e., the GDPR (General Data Protection Regulation) of Europe. This certainly, means that the shortcoming in the formulation of same are inevitable and there can be fair amount of implementation and enforcement challenges faced in the evolution process. As discussed in the aforementioned paragraphs, the author has discussed depth the serious flaws in the current Bill and has identified the grey areas and has made suggestions that cab be implemented for the Bill to function better.

[33] Section 24, Bill ; Section 25, Bill; Section 26, Bill ;Section 27, Bill.
[34] Section 78(2), Bill.

As per the author's analysis of the current situation, some changes in the bill can prove to be fruitful and largely business friendly, such as provision of increased certainty, but at the same time, some other changes such as the requirement to share the non-personal data with the government, can lead to concerns that might hamper data security in the long run. Therefore, the draft bill with its advent has to be a balance of both, good and bad. The report of the nine-member expert committee along with the draft bill, must be considered as a jump start point in the long process of data protection and not a conclusive step. The bills, aims at an enactment of a law that will protect the privacy rights of the citizens and therefore, it is important that a public consultation with a draft of proper modifications must be entertained in order to improve the standing of the Bill.

REFERENCES

- **BOOKS:**

- "Information Technology Law and Practice- Cyber Laws and Laws Relating to E-Commerce" by Vakul Sharma.
- "Cyber Crimes and Real-World Society" by Lalitha Sridhar.

- **LAWS:**

- Information Technology Act, 2000.

- **CASES:**

- *Justice K.S. Puttaswamy and Ors. Vs. Respondent: Union of India (UOI) and Ors., (2019) 1 SCC 1.*

- **ARTICLES:**

- International Journal of Scientific & Engineering Research, Volume 4, Issue 5, May-2013 789 ISSN 2229-5518
- A Free and Fair Digital Economy Protecting Privacy, Empowering Indians" dated July 27, 2018.
- Committee of Experts under the Chairmanship of Justice B N Srikrishna, "Report of the Committee of Experts under the Chairmanship of Justice B N Srikrishna," Committee Report (India: Ministry of Electronics & Information Technology, Government of India, July 27, 2018).
- European Commission, "2018 Reform of EU Data Protection Rules," Text, European Commission, accessed March 7, 2019.
- Philip E. Agre, "Marc Rotenberg Technology and privacy: The new landscape", July 3, 1998.
- Data Protection Law in India-Needs and Position, Adv. Swati Sinha, 2018.
- Committee of Experts under the Chairmanship of Justice B N Srikrishna, "Draft Personal Data Protection Bill, 2018," July 27, 2018.
- Paragraph 185 of the judgement by the plurality of judges authored by J. Chandrachud in "Justice KS Puttaswamy and Another Vs. Union of India and Ors," 10 SCC.
- European Centre for International Political Economy, "The Economic Importance of Getting Data Protection Right: Protecting Privacy, Transmitting Data, Moving Commerce" March 2013.