"ONE STEP FORWARD, TWO STEPS BACK: A CRITICAL ANALYSIS OF THE NEW PERSONAL DATA PROTECTION BILL, 2019"

AAKASH BHAMBRI & PARTH MISHRA

INTRODUCTION

With the growing advancement in the field of technology and more specifically computers, there is also an observable growth in the human dependency on this new technology with more and more tasks being done via the help of this new technology due to the ease and efficiency these machines have to offer. This now includes the storage of several terabytes' worth of personal data of individuals as well. This becomes extremely useful and problematic at the same time. This is because while it is efficient to store data on these machines, it is also prone to leaks and being accessed by any unauthorized source. Furthermore, this data can also be used illegally by these organizations for targeted advertisement. Targeted advertisements are essentially ads which are specifically shown to an individual based on the information that the company has on that individual. All this information is made available to such organizations with help from companies that possess the personal data of such individuals.[1] It is extremely essential to have certain data protection laws in place, as without any laws in place there would be no restriction placed on these companies from exploiting the personal data of the individuals that have provided them with such data. Keeping this view in mind, one of the first data protection Bills was introduced by the United Kingdom in 1984[2]. The aptly named Data Protection Bill of 1984 was very basic in its extent of protection offered to the personal data as the Bill itself was made at a time when the government was not aware of how the personal data can be used. In present times, however, stronger Bills need to be in place in order to ensure the security and safety to the personal data that has been given with consent to these companies. One of the strongest data protection Bills in present times has been enacted by the European Union, which is the General Data Protection Regulation of the European Union[3] (hereinafter referred to as GDPR). GDPR offers the provider of personal data or the data principal an array of rights to exercise their power over those that they offer their data to. This includes some rights which are yet to even be recognized

[1] Johnson, J. *Targeted advertising and advertising avoidance* 128-144 The Rand Journal of Economics, 44(1). (2013).
[2] Data Protection Bill, 1984, c. 35
[3] General Data Protection Regulation of the European Union, 2016, L119, p. 1-88

by other countries, such as the Right to be Forgotten. This Right was first recognized by the European Court of Justice (ECJ), the highest court of the European Union and was further asserted into power by the provisions of the GDPR[4]. Inspired by this wave of new legislation being implemented worldwide, even India attempted to make its mark by creating legislation to ensure the protection of the data of its citizens. To do so, a bill was tabled in the Parliament that is currently being viewed by a Joint Committee before being affirmed. This is the Personal Data Protection Bill[5] which aims to, *"to provide for protection of the privacy of individuals relating to their personal data, specify the flow and usage of personal data, create a relationship of trust between persons and entities processing the personal data, protect the rights of individuals whose personal data are processed, to create a framework for organizational and technical measures in processing of data, laying down norms for social media intermediary, cross-border transfer, accountability of entities processing personal data, remedies for unauthorized and harmful processing, and to establish a Data Protection Authority of India for the said purposes and for matters connected therewith or incidental thereto."*[6] In this article, the authors will attempt to analyse whether or not the provisions of the Bill in question are congruent with what it seemingly aims to achieve through its provisions. The authors will attempt to disseminate the provisions of the Bill attempting to highlight all that the article ensures, including the provision of Right to be Forgotten. Furthermore, the authors will also try and understand the need for such a provision in India and if there was the existence of any previous framework established to deal with data breaches. Lastly, the article will also attempt to analyse the efficiency of the Bill in question and attempt to understand the positives as well as the shortcomings and problems that the Bill can cause. To do this, the authors will contrast the Bill with other foreign legislations that have been passed to ensure data protection. This will help the authors in attempting to understand the problems of the Bill more clearly, when it has been compared with some of the stronger legislation, such as the GDPR.

TERMINOLOGIES

Section 3 of the Protection of Data Bill, 2019 (hereinafter referred to as *the Bill*), defines certain key terms which are necessary to understand the applicability of the regulation. The Section distinguishes between personal data and sensitive personal data and allocates different obligations to both individual categories. Personal data is defined as data about or relating to a natural person who is directly or indirectly identifiable through a certain feature or a combination of features (whether virtual or physical) and also includes inferences drawn from such data for

[4] Joshi, A. *Leave Me Alone! Europe's "Right To Be Forgotten"* 15-17 Litigation, 41(2), (2015).
[5] The Personal Data Protection Bill, 2019, Bill No. 373 of 2019
[6] Id. at p. 2.

the purpose of profiling.[7] Sensitive personal data is data that reveals, is related to, or constitutes financial data, health data, official identifiers, sex life and sexual orientation, biometric data, genetic data, transgender status, intersex status, and caste or tribe, religious, political belief or affiliation, and any other category as may be notified.[8] In a departure from the construct under the previous version of this Bill, passwords are no longer classified as sensitive personal data, similar to the position under the European Union's General Data Protection Regulation, 2016 (GDPR). The Natural person whose data is to be collected is called 'data principal'[9] and the body that collects or processes this data for any specific purpose is the 'data fiduciary'.[10] Because of the horizontal application of the bill, data fiduciaries can include State, corporate entities and individuals. Authority means the Data Protection Authority of India established under sub-Section (1) of Section 41.[11] Section 3(19) of the Bill defines 'financial Data' as financial data as any number or other personal data that is used to identify (i) an account opened by a data fiduciary, or (ii) a card or payment instrument issued by a financial institution. It is also defined to include personal data regarding the relationship between a financial institution and a data principal including financial status and credit status. 'Processing' as defined under Section 3(32) of the bill, means an operation or set of on personal data, and may include operations such as collection, recording, organisation, structuring, storage, adaptation, alteration, retrieval, use, alignment or combination, indexing, disclosure by transmission, dissemination or otherwise making available, restriction, erasure or destruction.[12] Anonymisation which is a key part of the bill as it lays the foundation for the 'right to be forgotten' is defined as an irreversible process of transforming or converting personal data to a form in which the data principal cannot be identified as per the standards of irreversibility laid down by the Data Protection Authority (DPA).

POSITIVES

The need for the legislation regarding data protection was identified as there was no regulating statute or body that governed the processing of the same in our country. The Data Security Council of India (DSCI) which was setup by NASSCOM in India contributes in policy making matters and ensuring a safe Cyberspace with the government. But the organization being a private entity had no authoritative function and could not regulate data protection and could

[7] Section 3 (29), Personal Data Protection Bill, 2019, Bills of Parliament, 2019.
[8] Trilegal, *Analysis of Personal Data Protection Bill, 2019*, (12th Dec. 2019)
https://www.trilegal.com/index.php/publications/analysis/the-personal-data-protection-bill-2019
[9]Section 3 (14), Personal Data Protection Bill, 2019, Bills of Parliament, 2019
[10] Section 3 (13), Personal Data Protection Bill, 2019, Bills of Parliament, 2019.
[11] Section 3(5), Personal Data Protection Bill, 2019, Bills of Parliament, 2019.
[12] Section 3 (32), Personal Data Protection Bill, 2019, Bills of Parliament, 2019.

only advise the government. Keeping the same in mind, the Protection of Data Bill, 2019 was introduced comprising of 98 Sections to ensure a proper legislative framework, we shall explore some of major Sections and how they have a positive impact on data processing. Clause 2 (A) (b) of the bill talks about the application to both government and private entities. It ensures that the bill covers every ambit of what shall constitute 'data fiduciaries.' Right to be forgotten is probably the most key aspect of this bill which derives its basis from the provision of anonymisation. Right to be forgotten can be defined as the right to have negative private information about a person to be removed from Internet searches and other records under some specific conditions. The right to be forgotten also appears in Recitals 65 and 66 and in Article 17 of the GDPR. It states, "The data subject shall have the right to obtain from the controller the erasure of personal data concerning him or her without undue delay and the controller shall have the obligation to erase personal data without undue delay" and the principle in our country was adopted from the same. Section 18[13] of the Bill along with the correction, completion and updating of data, provides for erasure of the data which is no longer necessary for the purpose for which it was processed. This Section hence, deals with the right to be forgotten in our country. Section 17[14] of the Bill entails the rights provided to the data principal against the data fiduciary. The basic essence of the provision being that the data principal can obtain information about what's being done with the data that they possess. On one hand the draft sets out detailed provisions for consent and explicit consent. On the other, there are provisions which dilute the right of data principals (individuals) completely such as Section 17 and 22. These allow for wide discretion to be exercised by the Data Protection Authority under the Bill. Tighter provisions including timelines for retention of and deletion of data, process, audit and compliance therefore would have been welcome additions. Section 22 and 23 of the Bill deals with transparency with reference to data processing. Section 22 specifically talks about the obligation on the part of data fiduciary to prepare a privacy by design policy which shall contain all the technicalities and relevant information pertaining to the data processing that the fiduciaries would perform. This includes the technology involved in doing so, the managerial, organisational, technical prices to identify and avoid harm to the data principle along with the privacy policy of the fiduciary. This is a form of e-contract between the party, whilst ensuring the principal that no harm shall be accrued to them. Section 23 explicitly talks about transparency in processing of personal data. It entails that the data fiduciary shall take necessary steps to maintain transparency in processing personal data and shall make a number of information available to the principal.[15] Section 25

[13] Section 18, Personal Data Protection Bill, 2019, Bills of Parliament, 2019.
[14] Section 17, Personal Data Protection Bill, 2019, Bills of Parliament, 2019.
[15] Section 23, Personal Data Protection Bill, 2019, Bills of Parliament, 2019.

talks about the security safeguards with reference to the nature, scope and processing of personal data. It states that the fiduciary shall implement necessary safeguards in order to avoid any likelihood of harm to the data. It also places an obligation on the fiduciaries to review its security safeguard measures periodically, and take measures accordingly if they're able to find a fault in the system.

THE PROBLEMS WITH THE PROPOSED BILL

While the new proposed legislation has many positive steps taken by the Parliament to ensure the protection of the data of the data principal in terms of the rights it provides, there are many shortcomings in this Bill that also seemingly negate the protection that it seeks to provide. These shortcomings in certain cases are so grave that it cannot be ignored as it can damage all the rights that it provides the data principal by providing the Central Government with certain extraordinary powers over the data of the data principle and over the data fiduciaries as well. Chapter III of the Bill lays down the grounds by which the data of the data principal can be processed without obtaining the consent for the same. The provision that establishes the consent of the data principle was a very strong provision that has seemingly been negated by even the existence of Chapter III. If one is to delve deeper into the phrasing of the Article 12, more specifically the provision (f) of Article 12, it can be observed that the State can seemingly process the personal data of any individual in case of breakdown of public order. Here, the Bill establishes certain ambiguity as to what can be defined as a breakdown of public order. There are many instances such as mass protest, that may be peaceful and legal in terms of the definition provided by Article 19(1)(b) of the Indian Constitution[16], but it may enable the Central Government to classify that as a breakdown of public order and to further infringe upon the personal data of those involved. Such ambiguity rests too much on the shoulders of the Judiciary in order to interpret the scope of the provision. Furthermore, Section 25 of the Bill puts power in the hands of the data principal to be informed of any data breach that occurs to the personal data that has been provided to any data fiduciary. However, the same Section also puts a limitation on this power in the clause (5) of the same, by stating that the final power of reporting this breach to the data principle will rest on the Data Protection Authority of India. The breach shall only be reported if the Authority wishes so, and if the Authority believes that reporting the breach can cause harm, it may refrain from reporting the breach itself to data principal. This is another instance of the Bill providing the data principal with a certain power and mitigating that power in the subsequent provision.

[16] India Const. art 19. cl 1. sub-cl f.

EXEMPTION OF STATE FROM THE PROVISIONS OF THE BILL

The next set of problems that are created by the bill in question are pertaining to the creation of a new post under the Authority. This is the post of the Inquiry Officer that has been created to Bill as a sort of gatekeeper to the data that is being provided to the data fiduciaries. The Inquiry Officer has been created under the text of Section 53 of the Bill. The purpose for which the Inquiry Officer has been created seem reasonable enough and are justified as the role of the Inquiry Officer is to look into the workings of the data fiduciaries and to check whether the data being kept by the fiduciaries is safe and protected. In doing so, however, the Bill has provided the Officer with tremendous amounts of power of the data fiduciaries. Under the clause (7) of Section 53, the Inquiry Officer has the power to look into every piece of information that the data fiduciary has been collecting. This also included the information regarding the employees of the data fiduciary as well. What makes this provision even more problematic is that when the Section in question is read with the Section 86 of the Bill, which creates a relationship between the Authority and the Central Government, the position of the Inquiry Officer can seem even more damaging. This is because according to the Section 86 of the Bill, the Central Government, because of its supremacy over the Authority, can gain access to all the amounts of data that the Authority has collected. This would mean that the Central Government can essentially use the data collected by the Inquiry Officer from the data fiduciaries for its own purposes as well. It would seem that the Central Government is establishing a sort of gateway that only it can use for the access of certain personal data of the data principal that has been provided with consent to the data fiduciaries. The consent over this data was only for the fiduciaries, and this consent is now being exploited by the Central Government for the advancement of its own purposes.

CONCLUSION

The Bill in some ways appears to defeat the very purpose for which it was created. Privacy policy in terms of data in our country wasn't ever regulated well enough, the objective behind the concerned bill was to rectify that, and to some extent succeeds to do so but lacks on the front of providing what shall be the correct interpretation of privacy, or at least the privacy that is expected by the citizens of this nation in context of digital privacy. When private entities have a free hand in processing data, they might use it to benefit them while they harm the principal involved. The bill introduces detailed provisions with reference to data processing and all the aspects that help to govern them. It also aims to regulate the privacy policies of the data fiduciaries but provides no concrete guidelines with reference to what actions would be under the ambit of breach of privacy, rather directs the fiduciaries to keep updating their policies and

provide the principal with transparency. The subject matter of the bill being data protection, but the bill only regulates the data and doesn't protect it. It establishes a new statute to protect the privacy of an individual but at the same time, it allows players to breach the same in a legitimate way, and hence, when it appears that the bill takes one-step further towards data privacy, it actually takes two steps back.