The Elephant in the Room: The Government & Regulator under PDP Bill, 2019

1. Introduction

As India evolved to become a global services hub combined with an increased reliance on web-based applications for day-to-day activities, sharing personal data has increased beyond anticipation. Conglomerates have consistently articulated concerns about the lack of or minimal data protection in India and devised their own best practices. In recent years privacy debates have been taking center-stage, particularly since 2017 when a nine-judge bench of the Supreme Court affirmed the right to privacy as a fundamental right in *K.S. Puttaswamy vs. Union of India*. A new data protection law has been on the anvil for a while now. After the aforesaid judgment was pronounced, the government set up an expert committee led by Justice B.N. Srikrishna to devise a statutory framework on data protection. In 2018, the committee submitted its report along with a proposed draft Data Protection Bill which remained open for public comments for about 3 months. At the time, Justice Srikrishna stated data privacy is a burning issue and there are three parts to the triangle. *"The citizen's rights have to be protected, the responsibilities of the states have to be defined but the data protection can't be at the cost of trade and industry."* Eventually in December 2019, the Personal Data Protection Bill (**"PDP Bill 2019"**) was introduced in the Parliament, which provides for protection of personal data and seeks to regulate cross-border flow of data. In the last three-four months, much has been written about this intended law, how it will impact every business entity doing business in India, particularly tech companies.

This newsletter analyses provisions relating to the proposed regulator – Data Protection Authority or DPA – and its role and the intervention of the state.

2. DPA and its (unfettered) powers

The proposed law contains 98 sections, divided across 14 chapters. The statement of objects and reasons identifies 13 salient features which include, amongst others to **(a)** promote concepts like consent, purpose and storage limitation(s), data minimization; **(b)** prescribe obligations on data fiduciaries (i.e. data collectors) who must collect data for a precise purpose with express consent of an individual i.e. data principal; **(c)** confer various rights on individuals who give their data including rights to restrict or prevent disclosure of that data; and the highly controversial provision **(d)** empower the Central Government to exempt any government agency from the purview of the law!

Sections 41 through 56 in chapter 9 of PDP Bill 2019 contains 16 provisions covering the DPA which will be created through a government notification. The statutory objective of the DPA, as described in section 49, is to protect interests of individuals, prevent misuse of personal data, ensure compliance and promote awareness about data protection.

2.1 *Constitution*: The DPA shall consist of maximum 7 members, including a chairperson and one member with experience and qualification in law. The government shall create a selection committee who will make recommendations about who should be appointed. This selection committee shall consist of 3 officers, headed by the Cabinet Secretary along with Law Secretary and Secretary of Ministry or Department of Electronics and Information Technology. The procedure for selection is not provided and all 3 members of the selection committee will be bureaucrats who may or may not possess subject matter expertise. The draft bill does stipulate that the DPA members

should be capable and experienced with at least a decade in the areas of data protection, data security, cyber laws and national security, amongst others. The term of the 7 members shall be for 5 years or until they attain 65 years, whichever is earlier. Given the involvement of the government in its constitution and funding, one wonders whether the DPA can truly be independent and protect data privacy. In view of the vastness of the powers and the potential repercussions for individuals, the business and the technology space generally it is absolutely imperative that the selection committee identifies and picks seasoned and credible ones from industry with the necessary subject-matter expertise.

2.2 *Powers:* Section 45 states the powers of the chairperson, while 49 provides those of the DPA generally. The chairperson has been given wide powers of general superintendence and direction of the DPA, and, additionally, can exercise any power or do anything which can be done by the DPA as a whole. This appears to be quite unfettered and without necessary checks and balances.

While section 49 imposes a rather wide duty on the DPA, the functions are categorized in 15 sub-points, but that are wide enough to cover every facet. In fact, DPA has been given extensive powers to enforce its obligations. It is empowered to regulate significant data fiduciaries, monitor cross-border transfers of data, specify codes of practice, develop mechanisms for creating data trust scores, and an all-inclusive provision which allows it to "*perform such other functions as may be prescribed.*" Furthermore, section 50 authorizes the DPA to make regulations in order to issue codes of practice spanning 18 different aspects, including notice requirements, quality of personal data, manner of obtaining consent, portability, transparency and security requirements plus cross-border transfers. Additionally, the 19th one is an omnibus provision which stipulates *"any other matter which, in the view of the Authority, may be necessary to be provided in the code."* It can also approve codes submitted by others i.e., industry organizations, statutory or government agencies. However, a code shall be issued following discussions with relevant stakeholders, including sectoral regulators and after following the prescribed procedure. Who will prescribe the process? Clearly, the government. What will be the checks and balances? There is complete silence. Absent an express provision that unequivocally sets out the framework of a consultative process, chances are both the DPA and the government may not follow a transparently consultative process.

Section 53(8), a non-obstante provision which overrides anything to the contrary, stipulates that the DPA or an inquiry officer shall have powers analogous to a civil court under the Civil Procedure Code for five types of matters. These include discovery and production of documents; summoning and enforcing presence of persons and examining them on oath; inspection of documents, records of data fiduciary; issuing commissions to examine witnesses or documents; and, again, "*any other matter which may be prescribed.*" Further, in its endeavor to enforce the statutory provisions, once made into law, the proposed authority shall be vested with powers to seek information and conduct inquiries[1] into any activity "*detrimental to the interest of data principals*," conduct search and seizure of locations where it reasonably believes that some data or document(s) can be either compromised or destroyed.

Section 94 provides that the DPA would make regulations, rules, safeguards for protection of privacy and restrictions on continuous or systematic collection of "*sensitive*" personal data etc. It will even define what is critical personal data, currently undefined in the draft. Yet, at this stage, there is no visibility on the (currently non-existent) processes to be followed by the DPA, while the government has the ability to access anything it feels would fit within the stated exemptions.

[1] Section 53(1) allows the DPA to do this, either on its own volition or on the basis of a complaint received

2.3 *Meetings:* The DPA will have to follow rules governing meetings once they are prescribed, but the current scheme of the sections merely provide that if the chairperson is unavailable, another member will be chosen to preside and voting shall be by majority of votes, with a casting vote of the chairperson in case of a tie. Further, if any member has any pecuniary interest in a matter to be discussed, then such person shall disclose the interest and abstain from voting. This is broadly similar to principles of company law. What is troubling is that section 47 currently provides that vacancies or defects in the constitution of the DPA or irregularity in the procedure shall not impact the merits of any case. The scale of data intended to be collected is mammoth, particularly in view of the ambitious digital transformation of India's national ecosystem. And, if exceptions will exist in the functioning of the DPA, the risk of erosion of the right to privacy may become a reality.

3. Powers of Central Government

Chapter XIV, titled "Miscellaneous" contains some more controversial provisions. Under section 86, the Central Government has the ability to issue periodic directions in the "*interest of sovereignty and integrity of India, security of the State, friendly relations with foreign states or public order*" and such policy directions shall be binding on the DPA. While the DPA shall have an opportunity to express its views on the directions, yet the Central Government shall have the final say on whether a question is one of policy or not. While orders to protect national security are not unusual, but it would not be incorrect to assume that possibility of potential abuse of this provision is real.

Section 91 clarifies that the that Central Government reserves the right to interpret any policies for the benefit of India's digital economy, provided it does not involve the use of personal data that can be directly used to identify an individual. Section 91(2) states further that the government, in consultation with the DPA, can direct data collectors to hand over anonymized personal information or other "*non-personal data*" for the purpose of "*evidence-based policy-making*." The current form of the draft bill contains no insights on what this involves.

The vast powers given to the Central Government appear to be virtually enshrined in every other provision. The one that has concerned all, be it individuals, industry or even the activists, relate to the exemptions granted to the government for data collection. Section 35 allows the Central Government to exempt any of its agencies from the purview of this law, provided it feels that such action is "*necessary or expedient*[2]" in the "*interests of sovereignty and integrity of India, national security, friendly relations with foreign states, public order*" or for preventing offences related to the above against India. How this will happen is not articulated at all. The only safeguards are a written order from the Central Government specifying the reasons for breaching privacy and in a manner as may be specified in future. If exemptions are to be given, the process for government agencies ought to have been stated explicitly. Effectively, this means that exceptions can be made to collection rules, reporting and other requirements whenever the government takes a position that it is necessary. There are no unambiguous provisions which govern the use of the data by the government. Rather, for the moment at least, it seems that its surveillance powers are omnipresent in the draft, at virtually every place and at every turn of the page. This leaves innumerable questions on how the citizens' privacy, a fundamental right mandated by the Supreme Court, shall be protected.

[2] Previously, the language was necessary and proportionate for government data processing. *K.S. Puttaswamy* judgment had provided that that right to privacy could be intruded upon only if was legally authorized, done in accordance with due process and imposed an obligation to ensure it was necessary and proportionate to the objective sought

4. Conclusion

"Power tends to corrupt; absolute power corrupts absolutely."[3] With broad carve-outs on various accounts, including national security, sovereignty and fiscal interests, it appears there is minimal levels of protection for personal data and very high degree of potential for intervention by the government. This seems to be contrary to the spirit of the judgment in *K.S. Puttaswamy* case which was issued after extensive hearings and exhaustive deliberations of a nine-judge Bench of the Supreme Court. Rather than actualizing and upholding the fundamental right of individual privacy, PDP Bill 2019 has the potential of taking retrograde steps in India's privacy debate. Further, the Central Government intervention definitely casts a shadow on the working of the DPA. The processes are unstated or unclear and a lot is left to the rule-making power. While a regulator cannot anticipate everything, even what could have been inserted in the provisions, has not been done so. The control of the government in every aspect of the DPA combined with the authority's discretionary powers and insufficient accountability are a grave cause of concern. The elephant in the room needs to be addressed, effectively by all the stakeholders and the Joint Parliamentary Committee[4] else such unbridled power is a threat to and will dilute individual privacy.

Author
Priti Suri

[3] A statement made by Lord Atkin, a 19th century British historian

[4] This was formed two days after the bill was introduced in the Parliament and consists of 30 members, from various political parties. While the consultative process is over, but the JPC sought an extension to submit its report in the monsoon session of the Parliament