Regulatory governance under the PDP Bill: A powerful ship with an unchecked captain?

As the Joint Parliamentary Committee considers the Personal Data Protection Bill, 2019, MediaNama will publish a series of articles from legal experts focussing on the key aspects of the Bill and how they will affect users and companies. This is the second article in the series. Read our extensive coverage of the Bill here.

By Smriti Parsheera

"I prefer to sail in a bad ship with a good captain rather than sail in a good ship with a bad captain."
— Mehmet Murat ildan

If the ship here is a metaphor for the rights and obligations offered by the draft Personal Data Protection Bill (PDP Bill) and the Data Protection Authority of India (DPA) as its captain, where does the current draft of the Bill leave us? Is it a good ship with a good captain or does it place the wheels of a powerful untested machine into the hands of an untrained and unchecked captain?

The preamble to the PDP Bill offers a precursor to the ambitious task that the Bill sets out for itself. It lists the various objectives of the law, which include specifying the usage and flow of personal data, creating organisational and technical measures for data processing, monitoring cross border data transfers and providing remedies against harmful processing. It then speaks of the role of the DPA as the agency responsible for giving effect to all of those purposes.

As per Section 41 of the PDP Bill, the DPA is to be set up as a body corporate, consisting of a Chairperson and up to six whole-time members. In adopting this structure, the Bill deliberately opts out of allowing any part-time members on the DPA's board. This is not in line with the practice that has been followed in the composition of many other statutory agencies. For instance, the Telecom Regulatory Authority of India can have up to two whole-time and two part-time members in addition to the Chair. By closing the possibility of having such part-time members, the Bill denies the DPA the opportunity to gain from the expertise of academics, researchers, practitioners and technical experts who could otherwise have injected independent ideas and critiques into its functioning.

While the draft does allow the DPA to engage consultants and experts to help it in the discharge of its functions (Section 48), this is very different from having independent voices in the management of the DPA itself. Further, the experience of other regulators shows that provisions of this nature are generally used for hiring entry-level researchers and consultants rather than those who might be in a position to drive policies at the top level.

A new concept that has been introduced in this Bill is that one of the members of the DPA has to be a person qualified in law. This is perhaps an attempt

to ensure the legitimacy and effectiveness of the DPA's adjudicatory functions, assuming that the legal member would be the one overseeing those activities.

Moving on to the DPA's selection process, all of the members are to be appointed based on the recommendations of an executive-led selection committee consisting of the Cabinet Secretary and the Secretaries in-charge of Legal Affairs and Electronics and Information Technology. This is a troubling departure from the draft that was proposed by the Justice Srikrishna Committee, which required that the selection committee should be headed by the Chief Justice of India or another judge of the Supreme Court. In addition, it was also to have another independent expert nominated by the judicial member.

Why is the constitution of the selection committee so relevant?

The success of the DPA, especially in the initial years when the foundational regulations and practices will be put in place, will depend to a large extent on the quality of its leadership. With an exclusively executive controlled selection process the chances are that the DPA will fall prey to the standard Indian practice of appointing former bureaucrats as the heads of regulatory agencies. This is already the case with the present banking, securities, insurance and telecom regulators in the country. While the persons selected in this manner may no doubt be competent individuals, the inherent flaw in such a system is that it perpetuates the hierarchies of the government set up into the functioning of what is supposed to be an independent regulatory body.

The DPA's independence from the government becomes particularly important given that it will not only regulate the private sector but also supervise the personal data processing of all government agencies. Bonhomie between the DPA's leadership and other government bodies could therefore result in weaker enforcement of the law. Let us examine this using an example.

Suppose an individual manages to discover an unencrypted database containing the personal details of all the beneficiaries of a public subsidies scheme. They report it to the concerned government department and the DPA. What is the DPA expected to do in such a situation?

The PDP Bill requires that every data fiduciary should implement necessary security safeguards like encryption, de-identification and measures to prevent unauthorised access (Section 24). Presumably, one of the likely reasons why the data could be accessed by a third party in this case was due to the department's failure to adopt appropriate security checks. The fact that the data was kept unencrypted makes it all the more vulnerable to being misused.

If such a situation of unauthorised or accidental disclosure of data leads to a compromise of its confidentiality, it amounts to a "data breach" (Section 2(29)). The department would therefore have to assess if the breach is likely to cause

any harm to the affected individuals. If so, it should immediately inform the DPA about the breach, its possible implications and any action taken to control the damage arising from it (Section 25). The DPA will then have to take a call on the best way to deal with the data breach, including determining whether the department should be compelled to inform the concerned beneficiaries of the scheme or the public at large about the breach.

In addition, the DPA will have to decide on what action it should take against the department for failing to secure the data in the first place. The range of orders that the DPA may pass for any such contravention of the law includes the issuance of a warning, directions to discontinue a violation of the law or temporary suspension of the fiduciary's activities (Section 54). In addition, the DPA can also impose a penalty of up to fifteen crores on the department for its failure to ensure appropriate security standards (Section 57(2)). The factors to be considered by the DPA while deciding on the levy of any penalty or payment of compensation to affected individuals include the nature and gravity of the violation, level of harm suffered and whether the violation was intentional or negligent in character (Sections 63(4) and 64(4)).

In the scenario described above, how might the DPA's actions be affected by the fact that the violator in question is a government agency? Would the risk of reputational damage to the department or its officials or any sort of political risks influence the DPA's decision on whether to go public about the breach? Further, since the department is performing a legitimate state function of delivering subsidies, is it practically possible for the DPA to place any restrictions on its data processing activities? A warning, reprimand or suggested remedial measures are perhaps the more likely interventions that we can expect in such cases.

Finally, when it comes to the potential imposition of a penalty, this decision is completely dependent on the initiation of a complaint by the DPA (Section 63(1)) followed by an adjudication process to be conducted by its officers. Given the composition and structure of the DPA one can expect that any penal action against the government would be reserved only for the most egregious of circumstances.

Suppose in the above example, the government entity had taken appropriate measures to de-identify the data that was leaked but the individual who found it intentionally used it to re-identify the beneficiaries of the scheme. What action may be taken by the DPA in such a case?

The individual's actions in the above scenario amount to the commission of an offence under Section 82 of the draft Bill, which is punishable with an imprisonment of up to three years and/or a fine of up to two lakh rupees. However, the PDP Bill bars courts from taking cognizance of any such offence, except in case of a complaint made by the DPA (Section 83(2)). The DPA will therefore have the discretion to decide whether to initiate any criminal action against the

individual.

It is curious to find that the PDP Bill chose to opt for this formulation despite its explicit rejection by the Supreme Court in the context of the Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits and Services) Act, 2016 (Aadhaar Act).

The original text under Section 47 of the Aadhaar Act contained a provision similar to the PDP Bill, which allowed only the Unique Identification Authority of India to initiate a complaint for any offence committed under that law. The Supreme Court, however, declared this to be unconstitutional, with the majority decision in the *Puttaswamy* case noting that:

> "*By restricting the initiation of the criminal process, the Aadhaar Act renders the penal machinery ineffective and sterile … Such bar is unconstitutional as it forecloses legal remedy to affected individuals.*"

This led to an amendment of the Aadhaar Act in 2019 to clarify that a complaint could also be initiated by an Aadhaar number holder or individual. It is necessary that a similar provision should also be included in the PDP Bill.

Transparency in DPA's regulation-making process

The example above refers to the monitoring and enforcement functions of the DPA, in essence, its duties to ensure compliance with the provisions of the law. In addition to this, the DPA also has the power to frame subordinate legislation on many important aspects. Here, it is curious to find that the PDP Bill draws an unexplained distinction between the process to be followed in case of the framing the codes of practice for data fiduciaries and all other types of regulations. Examples of the codes of practice listed under the PDP Bill include the process for obtaining valid consent, data portability standards, anonymisation methods, etc. In all such cases the PDP Bill requires that the adoption of the codes has to be done in a transparent and consultative manner (Section 50(4)). There is, however, scope to further improve this provision by codifying the details of the process to be followed by the DPA to ensure careful deliberation by the DPA and effective participation from stakeholders.

On the other hand, when it comes to the framing of all other regulations (other than the codes of practice), the PDP Bill is completely silent in terms of requiring the DPA to follow a transparent and deliberative process. The reason for the inferior treatment for this category of regulations, which have the effect of law and can therefore bear significant consequences for data principles and fiduciaries, is not clear.

For instance, the Bill allows the manual processing of data by "small entities" to be exempted from certain requirements under the law (Section 39). While it does provide the suggested criteria for designating such entities, for instance based on their turnover and number of users, the actual classification is left to be done by the DPA through regulations. Another requirement under the Bill

is that significant data fiduciaries should undertake a data protection impact assessment under certain circumstances, and the DPA can specify the cases in which this exercise would be mandatory (Section 27). This decision also has to be made through regulations to be framed by the DPA.

In both these cases, the regulation-making process will not have to be subject to any consultation, debate or cost-benefit analysis. This sort of an opaque decision-making processes vests a tremendous amount of discretion in the hands of the DPA.

The same observations also hold true for the various situations where the law empowers the Central Government to take decisions "in consultation with the Authority". Examples of this include the notification of additional categories of sensitive personal data under Section 51(1); declaration of certain social media intermediaries as significant data fiduciaries under Section 26(4); and issuance of directions for the provision of any anonymised personal data or non-personal data under Section 91(2). Unless such a requirement is built into the law, the DPA would not be required to follow a transparent, consultative process while rendering its advice to the government on these important aspects.

DPA's control over the innovation sandbox

The 2019 version of the Bill also introduces a new concept of a "sandbox". It gives the DPA the authority to modify the application of certain provisions of the law for eligible entities that are engaged in "innovation in artificial intelligence, machine-learning or any other emerging technology in public interest". The relaxations that may be provided in the sandbox include exclusions from the need for having a clear and specific purpose for data processing, collection only for a specific purpose and limited period of retention of the data (Section 40).

In order to be eligible for the sandbox an entity should have in place a suitable privacy by design policy that has been certified by the DPA (Section 22). This is an odd provision in that it requires the DPA to verify and certify the fiduciary's managerial and business practices, the technology being used by it and the transparency of its data processing. All of these are matters which would ordinarily have to be verified by the DPA only in ex-post facto circumstances, in case of an inquiry or adjudication proceedings.

The present formulation of the sandbox and privacy by design provisions gives rise to several concerns:

1. **Burden on DPA:** The requirement to certify the privacy by design policy of each entity that makes such a submission would cast a huge burden on the DPA. Given the large number of fiduciaries in the ecosystem this sort of prior certification does not seem to be the best use of the DPA's time and resources.
2. **Lack of clarity around the certification:** The implications and purpose of the certification are also unclear. If the objective is mainly to

make sure that any entity that seeks to enter into a sandbox has the basic processes in place, that could have been achieved through other mechanisms. For instance, the DPA could follow a case-by-case analysis only for those entities that seek to apply for the sandbox. Alternate requirements like self-certification or third-party audit of the relevant entities could also have been considered, along with suitable checks and balances.

3. **Ambiguous conditions:** The factors to be considered by the DPA while allowing entry into the sandbox include judging whether the activity being pursued by the fiduciary is in "public interest" and if it amounts to an "innovative use of technology". The undefined nature of these terms vests ample discretion in the hands of the DPA in deciding which entities would be included or excluded from the sandbox.
4. **Lack of transparency in the regulation-making process:** The detailed process and additional criteria for applying for the sandbox as well as the privacy by design certification is left to be determined by the DPA through regulations. This circles back to the issue of lack of transparency and accountability requirements in the DPA's regulation-making processes.

In summary, the PDP Bill grants many far reaching powers to the DPA. Most of the principles laid down in the draft law are to be supplemented by regulations and codes of practice to be adopted by the DPA. In addition, the DPA is also responsible for monitoring compliance with the law, providing redress to aggrieved individuals, monitoring technological developments and promoting awareness among stakeholders. While casting all of these diverse functions on the DPA, the Bill, however, fails to go far enough in terms of ensuring the independence and the accountability of the agency.

The lack of procedural safeguards in the draft Bill coupled with weak state capacity leaves us in a situation where even a well-intentioned captain might not be able to successfully steer this ship, let alone the havoc that may be caused by a rogue one.

*

Smriti Parsheera *is a fellow with the technology policy team at the National Institute of Public Finance and Policy, New Delhi.*

Edited by Aditi Agrawal