CENTRE FOR POLICY RESEARCH

Submissions by the Technology and Society Initiative, Centre for Policy Research, New Delhi in response to the Personal Data Protection Bill, 2019[1]

The Personal Data Protection Bill, 2019 ("PDP Bill" or "the Bill"), the first of its kind in India to propose an overarching protective framework for personal data is apparently the outcome of deliberations by the Justice BN Srikrishna Committee, which was constituted in 2017 to come up with a draft bill.

But there are certain important features in the Bill that depart from the earlier draft bill ("draft") proposed by the Srikrishna Committee. Some of these, and other important features of the PDP Bill, are highlighted here. The purpose of these submissions before the Joint Parliamentary Committee is to present for its consideration, certain fundamental issues with some of the policy choices and specific provisions in the Bill.

These are classified under three broad types of implications: rights and fairness; trade and innovation; and lack of regulatory vision. These are not watertight buckets simply because what may be harmful for privacy and rights may also be detrimental for digital innovation in certain cases. An excessive regulatory burden may carry implications for trade and innovation as well. Mindful of this, we have chosen to place provisions and choices made in the Bill under their respective implication category after evaluating where among the three heads of implications, the predominant impact of such provisions or choices would be felt.

I. Rights and Fairness Implications

1) *Prospect of a Surveillance State*

A clear point of departure from the draft is the power vested in the State to acquire and process personal data of citizens without informed consent.

Clause 35 of this bill vests the Central government with power to exempt any agency of the Government from the application/purview of this Bill (all or select provisions) in respect of "processing of such personal data". As compared with clause 42 of the draft, which allowed access to personal data to the Government as long as it complied with necessity and proportionality requirements and on the basis of authorisation by specific laws (all of which were insisted upon by the Hon'ble Supreme Court in *Justice KS Puttaswamy v. Union of India* (2017), clause 35 vests an umbrella power of designating agencies as the Government may

[1] These submissions have been prepared by Dr. Ananth Padmanabhan, visiting fellow, CPR, with assistance rendered by Ms. Kanksshi Agarwal, Senior Researcher, CPR and Ms. Simrin Mediratta, Researcher, Governance and Public Policy Initiative, CPR.

deem fit and without stipulating the need for necessity or proportionality, thereby widening the scope of this exemption.

This clause facilitates amplifying the government's existing surveillance powers. It will make it far easier to validate surveillance projects like CMS and NATGRID, nationwide facial recognition, and new mass interception projects, effectively making way for the government to collect and process any category of personal data on a whim. Because the purposes stipulated in Clause 35 for this authority to kick in – interests of sovereignty and integrity of India, the security of the State, friendly relations with foreign States, public order – are not easily amenable to judicial review, the only real safeguard is to reintroduce necessity and proportionality and limit the agencies that may wield authority under this clause.

2) *Verification and the Erosion of Privacy*

The Statement of Objects and Reasons to this Bill, in para 4(vi), adds that one of its salient features is to specify a provision relating to "social media intermediary" whose actions have significant impact on electoral democracy, security of the State, public order or the sovereignty and integrity of India, and to empower the Central Government, in consultation with the Authority, to notify the said intermediary as a significant data fiduciary (SDF). This is an addition to the concept of SDFs, which was introduced in the earlier draft. Reference to "laying down norms for social media intermediary" also forms part of the preamble to the Bill. Therefore, the provisions that operationalise this objective, clauses 26(4) and 28(3) of the Bill, merit closer attention and analysis.

Broadly, clause 26(4) brings SMIs that exceed a certain threshold of users, and which have the potential to impact the grounds mentioned above, within the fold of SDFs. It also defines such intermediaries to be those that primarily or solely enable online interaction between two or more users and allow them to create, upload, share, disseminate, modify or access information using their services. Internet access providers, search-engines, on-line encyclopaedias, e-mail services and online storage services have been expressly excluded.

In addition to the already cumbersome compliances that SDFs must fulfil under the PDP Bill, clause 28(3) places additional responsibility on SMIs to provide an option for voluntary verification of user accounts. Such verification, if carried out by users, will be demonstrated by a visible mark that can be seen by all users of the SMI in question. On first glance, this is a benign provision. However, it can result in creating an architecture that potentially mandates, with time, the linking of social media identities with citizenship or other real-world identities. Any measure of this kind that can result over time in eroding the privacy of individuals must be kept out of the PDP Bill. If anything, the linking of social media accounts with Aadhaar is already the subject matter of separate judicial enquiry and the resolution of this issue should be left to courts of law.

There is an added reason why clause 28(3) could very well bring down the curtains on anonymity and privacy: the need for verification introduced by clause 16(2), wherein every data fiduciary shall, before processing the personal data of any child, verify his age. The impact of this latter provision is clear – be it a child or an adult, verification now becomes imperative only because the prospect of a user being a child cannot be ruled out unless and until such verification is carried out. Thus, by demanding compulsory verification for all child users and mandating a process for voluntary verification of adult users in the case of SMIs, clause 16(2) read with clause 28(3) makes verification the norm rather than exception. To avoid this result, we recommend that the verification requirements in clause 16(2) as well as 28(3) may be removed.

3) *Weak Regulatory Safeguards*

The Data Protection Authority (DPA), seemingly created to protect the rights of citizens, is incapable of doing so when it comes to data processing by the State. The DPA is claimed to be an independent regulatory body in its structure and design, but the government's shadow is apparent in its selection committee composition and structural organisation. The selection committee[2] for the DPA comprises of – a) the Cabinet Secretary (who is also the Chairperson); b) Secretary, Department of Legal Affairs; and c) Secretary, Ministry of Electronics and Information Technology. This selection committee, devoid of civil society, members from the judiciary and external experts, then becomes a 'Government committee' that has the potential to politicise data protection. This is a troubling departure from the earlier draft, which required that the selection committee be headed by the Chief Justice of India or another judge of the Supreme Court. In addition, it was to also have another independent expert nominated by the judicial member.

Far from retaining these minimal safeguards, clause 86(1) of the Bill makes it clear that the Central Government can issue necessary directions to the DPA in the interest of the sovereignty and integrity of India, the security of the State, friendly relations with foreign States or public order. The DPA is also bound by directions issued by the Central Government on "questions of policy", an expression wide enough to literally cover any point of ambiguity on rights and obligations under the Bill.[3] The fact that the Central Government's decision is final in this regard, ie. on whether a question is one of policy or not,[4] makes it abundantly clear that there is no independence whatsoever envisaged for the DPA under this Bill.

The absence of these checks is particularly worrisome because clause 63(1) of the Bill makes it clear that penalties – a major deterrent envisaged under the Bill – can only be imposed pursuant to an inquiry conducted on the basis of a complaint preferred by the DPA. Even

[2] Clause 42, Bill
[3] Clause 86(2), Bill
[4] Clause 86(3), Bill

courts can take cognizance of offences under the Bill only upon a similar complaint by the DPA.[5] By divesting data principals of their autonomy to initiate these forms of remedial actions through a private complaint, and vesting this authority in a DPA that does not inspire confidence in its independent functioning, regulatory safeguards have been weakened considerably in the Bill.

A primary function of the DPA is to regulate personal data processing by government agencies. Therefore, its dependence on the government is a threat to the privacy of data principals and can lead to authoritarian behaviour from the government. Moreover, the government has been vested with wide powers to frame regulations on various aspects of the PDP Bill, with the authority to override regulations on similar subjects that the DPA may frame. In sum, the nature of the DPA, its interactions with other regulatory bodies and its powers as an independent regulator itself are extremely suspect.

In the light of these issues, we recommend that clause 86, 83(2) and proviso to 63(1) are deleted, and that the guidelines framed by the Constitution Bench of the Hon'ble Supreme Court in *Union of India v. R. Gandhi*, (2010) 11 SCC 1 when constituting an independent tribunal be incorporated into the PDP Bill as well. With an exclusively executive led selection process, the DPA will likely replicate the practice of appointing former bureaucrats as the head of the regulatory body. Such a format perpetuates the hierarchies of the government into the functioning of what is expected to be an independent regulatory body. Accordingly, all provisions pertaining to the constitution and functioning of the DPA merit serious relook and complete overhaul in order to ensure that they comply with independence of quasi-judicial tribunals – a basic feature of the Constitution of India.

4) *Excessive reliance on Criminal Penalties*

The Bill seeks to penalise any person who knowingly or intentionally re-identifies any de-identified personal data without the consent of the data principal. Clause 82 provides for imprisonment of up to 3 years or a fine, which may extend to INR 2,00,000, or both. There is no necessity at present to show that harm was caused, in order for this criminal liability to stand attracted. This renders the provision excessive, unfair and harsh. It should be removed from the final version. Moreover, the JPC may insist upon all criminal liability under the Bill being subject to the threshold of 'intentional' and 'wilful' misconduct by the perpetrator.

5) *The Bill must make clear that the data principal qualifies as an aggrieved person for purposes of appeal to the Appellate Tribunal, in all cases where such appeal has been provided for and the expression "person aggrieved" has been used.*

[5] Clause 83(2)

II. Trade and Innovation Implications

1) *Data localisation and cross-border data transfers*

Data localisation can be defined in myriad ways but the Bill focusses on two commonly used models. The first is a hard localisation model where data is stored only in a domestic server and cannot under any circumstance be transferred or parallelly stored in a server outside the domestic jurisdiction. The second is a soft localisation model, otherwise known as data mirroring, where data can be stored in a server outside the domestic jurisdiction but a copy of the same has to be retained in a local server.

The reasons advanced for data localisation are also myriad, of which two stand out:

a) To push back against exploitative data practices, duly called data colonialism, an extractive economic model practised by US-based technology companies to make use of data tapped from India to consolidate their global monopoly;

b) To avoid the tiresome process of criminal investigations that the Indian law enforcement agencies have to parse in order to access data stored in the United States.

India's data localisation policies so far, most notably the RBI directive on localising payments data, have not been received positively in the international arena. Indo-US trade relationships have been adversely impacted owing to this stance. The United States has consistently emphasised the need for a liberal cross-border data flow regime between the two countries as a precondition for a free trade agreement.

Consequently, the PDP bill has narrowed the scope of the 'data mirroring'[6] provision by requiring only sensitive personal data to be stored in parallel within India's borders, a softer approach to the apparently rigid positioning taken by the Srikrishna Committee. This committee had earlier insisted that *all* personal data be stored in parallel in India.

However, the PDP Bill has not tempered the stance by the Srikrishna Committee on the hard localisation mandate. In much the same way as the Committee did, the PDP bill too creates a category of "critical personal data"[7] that should be stored and processed only in India. The legislation does not define "critical personal data" except by way of leaving it to the government to classify data types as falling within this category as and when it deems fit. This category of "critical personal data" is permitted to leave Indian shores only under extremely narrow circumstances that relate to health crises, or where the government decides that such transfer is not antithetical to India's strategic and security interests.

Cross-border data transfers is another area where the PDP Bill introduces a restrictive approach. This is ironic considering the Indian IT and IT-enabled services sector had grown on the strength of liberal cross-border data transfer arrangements. The PDP Bill insists that all

[6] Clause 34, Bill
[7] Clause 33(2), Bill

"sensitive personal data" can be transferred outside the country only upon meeting certain stringent conditions.[8] This includes a requirement which, upon first glance, appears to mimic the adequacy requirement in the European Union's General Data Protection Regulation (GDPR). In other words, for data from India to be transferred to another country, the destination country must have an adequate protective framework for privacy in place.

However, the Bill goes on to include, as a condition of adequacy, the implicit requirement that the destination country should not impede Indian law enforcement agencies from accessing the data or blocking the transfer of such data in appropriate situations. The adequacy framework under the GDPR only envisaged rights adequacy, not any other kind including the adequacy to enforce muscular authority of the State.

Apart from its huge potential for heavy-handedness in governmental action, this provision on data transfer also suffers from lack of clarity. It could mean one of three possibilities: a) the data must continue to be stored in India even when transferred abroad; b) the data can be deleted forever, so long as it is validly transferred abroad; c) the data need not remain stored in India for the period of such transfer, but upon successful completion of the processing activity for which it was transferred in the first place, the data must be transferred back to India. The PDP Bill provides no guidance on which of these would satisfactorily comply with its requirements.

These extreme positions in the Bill on localisation and cross-border data transfers, besides their impact on trade relations, could curtail a platform's ability to invest in India, lead to loss of market openings for start-ups and reduce access to international cloud service businesses. India's National AI Strategy is focussed on developing an innovation ecosystem for AI technologies. These and other innovation friendly strategies will only work when businesses and start-ups are protected from the adverse effects of data localisation and restrictions on cross-border data flows. It is imperative therefore that the JPC take a relook at these provisions to a) identify the kind of data ecosystem the country wants to build for the future, b) understand if keeping data within Indian shores will be crucial to that vision, and c) align policy measures in accordance with it. These are policy choices that demand a data-intensive enquiry, one that has not been carried out either by the Srikrishna Committee or the Ministry of Electronics and IT (or any other government department or ministry for that matter). Therefore, we recommend that Chapter VII be deleted for the present and re-introduced as an amendment if, and to the extent, localisation, mirroring and cross-border transfer restrictions are demonstrated by any data-backed study to advance any legitimate governmental purpose.

2) Non-personal data

Non-personal data is data that does not identify individuals but can be used to generate aggregate patterns. For example, an analysis of e-commerce data can be used to determine

[8] Clause 34(1), Bill

users' purchasing patterns or data on public transport systems. India's important policy documents from the last three years, such as NITI Aayog's National AI Strategy, Ministry of Commerce's Artificial Intelligence Task Force Report[9]and the Economic Survey of India 2018–19, highlight a national vision where data is at the heart of policy.

In order to leverage data for social welfare and innovation policy, a clear demarcation between personal and non-personal data is crucial. The state clearly sees the value of large data sets held by the private sector, but questions on the legal and economic complexities of such arrangements remain unexplored. In 2017, TRAI's consultation paper on privacy and ownership of data[10] sought inputs on creating data sandboxes - silos where entities can contribute anonymised data for others to develop new products. The Economic Survey of India 2018-19 also highlighted the "data explosion of recent years" and compared the data of Indians to "a collective resource, a national asset, that the government holds in trust, but rights to which can be permitted." These debates and concerns led the Ministry of Electronics and Information Technology (MEITY) to constitute a Committee to arrive at a framework for Non-Personal Data.[11] The Committee, headed by Infosys co-founder Kris Gopalakrishnan, is likely to look into the economic and social value of data, property rights for data, data taxonomy and the building of public databases for data democratisation.

The Srikrishna Committee did not define non-personal data, possibly because its mandate was restricted to a protective framework for personal data. The committee simply vested powers in the government to formulate separate policies for non-personal data. The PDP Bill, on the other hand, defines non-personal data as data that falls outside the purview of personal data. Yet, clause 91 of the Bill empowers the Government to direct any data fiduciary to provide any anonymised personal data or non-personal data "...to enable better targeting of delivery of services or formulation of evidence-based policies by the Central Government, in such manner as may be prescribed."

There are five problems here. First, the State is wielding paternal authority over citizens, exercising an unspoken trusteeship over their data and actions to do with the same. Second, there are no safeguards to protect the privacy of data principals against the State once they acquire such converted data from private actors. Even anonymised data can be used to profile, target and identify an individual or a group of people through reidentification methods.

Third, data fiduciaries may find it cumbersome to implement anonymisation when it has no direct benefit for their business model. Fourth, substantial investment is often put in by

[9] Ministry of Commerce, (2018), *Report on Artificial Intelligence Task Force,* available at https://dipp.gov.in/sites/default/files/Report_of_Task_Force_on_ArtificialIntelligence_20March2018_2.pdf

[10] Telecom Regulatory Authority of India, (2017), *Privacy, Security and Ownership of Data,* available at https://main.trai.gov.in/sites/default/files/Consultation_Paper%20_on_Privacy_Security_ownership_of_data_09082017.pdf

[11] https://meity.gov.in/writereaddata/files/constitution_of_committee_of_experts_to_deliberate_on_data_governance_framework.pdf

private entities to organise non-personal data and derive value from the same. Acquiring this business moat through a compulsory expropriation is unfair and can serve as a disincentive for data-driven businesses and innovation in India.

Fifth, non-personal data is not capable of solving any problem unless a robust data governance architecture is in place. India needs a holistic strategy on data standards, interoperability, platformisation and data accuracy. Mere agglomeration of data in the hands of the State cannot automatically propel data-driven solutions for public good. A national data strategy that focuses on data quality and standards will therefore need to be outlined. At the same time, important incentives and disincentives need to be created in favour of open data models. These issues, however, lie outside the remit of a personal data protection law. Therefore, clause 91(2) & (3) must be deleted.

3) *Data Protection Impact Assessment*

Significant data fiduciaries (SDFs) are classified under clause 26 on the basis of several factors, most of which are very subjective. This subjectivity has implications for digital innovation. This is so because SDFs have several additional compliances under the Bill, extending far beyond what other data fiduciaries must comply with. Even ignoring for a moment, the compliance costs that the PDP Bill will bring about, we are concerned with clause 27.

Under this clause, a Data Protection Impact Assessment (DPIA) has been made mandatory for SDFs, if such entities undertake any processing that involves "*new technologies or large scale profiling or use of sensitive personal data … or any other processing which carries a risk of significant harm to data principals.*" Without clearance from the DPA, SDFs will be practically unable to try out new technologies. This is so because the DPIA has to be reviewed by the DPA, which can in turn direct data fiduciaries to cease processing of personal data if such processing is likely to cause harm to data principals.

While this is a laudable objective, it can cause inordinate delay in the launch of new technologies and data processing solutions in much the same way as has happened with the electronics industry in India because of the Compulsory Registration Order regime. This is partly because regulatory capacity has not evolved in a manner fit enough to complete DPIA review within a realistic timeframe. Therefore, we recommend that clause 27 be deleted.

III. Lack of Regulatory Vision

The PDP Bill establishes a Data Protection Authority[12] to protect the interests of the data principal, prevent any misuse of personal data and ensure compliance with the provisions of the Bill. The DPA, thus, is an authorised regulatory body to oversee the processing of personal data by public and private data fiduciaries, and performs the below functions:

a) **Norm-setting and approval /certification functions[13]:** The norm-setting function of the DPA flows from two important powers it has been vested with, namely the power to issue regulations and the power to issue codes of practice. The DPA can issue regulations to guide the operationalisation of several loosely defined obligations in the PDP Bill, including the manner of deletion of data, the manner of taking consent from parents or guardians of children, the procedure for enforcing any of the data principal rights, the process of registration of significant data fiduciaries, clarifying the class of research, archival or statistical purposes exempted from the bill, and many other modalities of operation. Similarly, it can frame codes of practice on a range of subjects such as data quality, data retention, valid consent, processing of sensitive personal data. Under clause 22, the DPA also has the authority to certify the privacy by design policies which every data fiduciary is required to create. It is evident from a cursory look into these provisions in the bill that the norm-setting and approval/certification functions vested with the DPA are quite wide and capable of setting the tone for how the bill plays out in practice.

b) **Identification, anonymisation, and personal data transfers[14]:** The DPA has the power to approve cross-border data transfers in the case of sensitive personal data. Additionally, the DPA has the power to assess whether the data protection impact assessment carried out by a significant data fiduciary reveals the risk of significant harm, and accordingly restrain such fiduciary from carrying out the plan at all or till further changes are made to mitigate the risk.

c) **Scrutiny, inquiry and investigation functions[15]:** The DPA has the power to issue directions to any particular data fiduciary or call for any information from such fiduciary. It can commence an inquiry against any data fiduciary if it has reasonable grounds to believe that activities of such fiduciary are being conducted in a manner detrimental to the interest of data principals, or to suspect contravention of any of the statutory provisions in the PDP Bill. The DPA can appoint an Inquiry officer to investigate third-party complaints or action taken by the DPA on its own accord. The Inquiry officer can compel data fiduciaries to produce books, registers, documents, records and any data in their custody or power, that the officer may deem necessary for purposes of such investigation.

[12] Clause 41, Bill
[13] Clauses 49 and 50, Bill
[14] Clauses 50, 51, 52, Bill
[15] Clauses 53, 54, Bill

d) **Adjudicatory and penalising functions[16]:** The data regulatory body can reprimand or temporarily suspend the activities of the data fiduciary if the inquiry report reveals contravention of obligations under the PDP Bill. In addition, the DPA can also impose a penalty of up to fifteen crores on the fiduciary for its failure to ensure appropriate security standards[17]. 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[18].

The PDP Bill also prohibits courts from taking cognizance of offences under this law, unless the DPA files a complaint. This formulation has been earlier rejected by the Supreme Court in the context of India's Unique Identification Programme, Aadhaar. It declared a similar provision unconstitutional, 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."[19] The amendment to the Aadhaar Act in 2019[20] remedied this by mentioning that the complaint could be raised by an Aadhaar number holder or an individual. The JPC must take pointers from this ruling to modify the PDP Bill along the same lines.

But going beyond these issues, the larger structural issue is as follows: many of the powers vested with the DPA are technical in nature but limited thought appears to have been placed on its regulatory capacity to carry out these functions. The Indian experience has been far from satisfactory in this regard, be it similarly placed technical areas like food or environment, or the cyber appellate tribunal in the past. Therefore, a rethink on the muscular approach is required, and co-regulatory models may be explored.

Dr. Ananth Padmanabhan **25.02.2020**
Visiting Fellow, CPR

[16] Clauses 55, 56, Bill
[17] Clause 57(2), Bill
[18] Clause 54, Bill
[19] Supreme Court of India, (26 September, 2018), *Justice KS Puttaswamy (retd.) vs Union of India,* available at https://indiankanoon.org/doc/127517806/
[20] The Aadhar and Other Laws (Amendment) Act, 2019 available at https://uidai.gov.in/images/news/Amendment_Act_2019.pdf