Blue Paper | Justice Srikrishna Committee Documents on Data Protection

@TakshashilaInst
@matthan
@nasac
@ajaybpatri

TAKSHASHILA
INSTITUTION

The Takshashila Institution hosted a Roundtable on 10 August 2018 to discuss select issues identified in the documents released by the Justice Srikrishna Committee on 27 July 2018. This included the report titled *A Free and Fair Digital Economy: Protecting Privacy, Empowering Indians* (the Report) and the draft *Personal Data Protection Bill*, 2018 (the Bill).

This Blue Paper collates and presents the comments, remarks, and analysis made during the Roundtable by the participants.

Background

The discussion at the Roundtable broadly addressed the following issues:

1. Underlying Principles of the Report and the Bill.
2. Cross-border data transfers and data localisation.
3. Exemptions for state surveillance and law enforcement actions.
4. Capacity and independence of the relevant authorities.

Agenda of the Roundtable

Framing of the Bill

The use of terminology such as *data principal* and *data fiduciary* places the individual at the centre of the proposed law and is a positive measure.

Equally, the Bill shifts the onus of proving mindful and accurate consent to the data fiduciary. This is also a desirable change from the current position.

A surfeit of categories

The Bill is applicable only to *personal data*, defined as the data of a natural person who is identifiable. However, personal data is further delineated into *sensitive personal data* and *critical personal data*. At the same time, the Bill places anonymised data outside the scope of the law, even though irreversible anonymisation may not be feasible.

An alternative approach to this could be to do away with categorising data as sensitive or not. Instead, the classification framework could be based on the purpose of data collection.

On Data Classification

Inferred data

The Bill is silent on the treatment of inferred data, i.e., data that is non-personal and does not relate to a natural person but which can still be used to identify an individual. For instance, it is possible to layer an anonymised data point such as an area pin code on top of another innocuous data point such as the number plate of an individual's vehicle to identify where they live, or work.

On Data Classification

Data ownership and the exercise of rights

The emphasis on a relationship of trust between a data principal and a data fiduciary places the onus of compliance on the latter. This frames the data principal as a passive entity to the use and evolution of their data. Additionally, the implications this framework might have for principals' ownership over their data is uncertain.

Data ownership and monetisation

On the other hand, it is desirable that the Bill does not carve out an express right to data ownership. Doing so would bring up questions of monetisation of data, which is not the path a data protection legislation ought to take.

On Data Ownership

Serving copy to be stored in India

The Bill brings in the requirement to store a serving copy of personal data in India. While this is acceptable, one cannot deny the extensive costs data fiduciaries will have to incur to maintain local servers. The transition will also be easier if data fiduciaries use cloud-based systems to store data. It will be significantly more cumbersome for entities that use storage systems that rely on old mainframes.

At the outset, data localisation for all kinds of data (at different levels) need not have been inserted in the statute. There were other ways of leveraging this such that it did not come in the way of innovation or security.

Sensitive Personal Data

Storing specific kinds of sensitive personal information within India might be desirable (for instance, genomic datasets collected for genetic research within India should be aimed to be stored within the country.)

On Data Localisation

Critical Personal Data

Neither the Report nor the Bill draw clear boundaries on the scope of *critical personal data*. While the term is not defined in the Bill, the Report does not provide much clarity either. Among other kinds of data, *critical personal data* is included to mean any information that might be important to the growth of the Indian economy.

The Bill allows the Union Government to determine what constitutes critical personal data at a later stage, but prohibits the cross border transfer of any data that falls within the scope of this term. There should be some criteria on the basis of which the critical nature of a dataset is measured. This will also help create checks and balances to hold the executive answerable.

On Localising Critical Personal Data

Ambiguity in the intent behind a data localisation mandate

The Report outlines four primary benefits of data localisation: facilitation of enforcement, avoiding vulnerabilities associated with fibre optic cable networks, building an AI ecosystem, and preventing foreign surveillance. These may not necessarily be achieved through a localisation mandate. The Report should have provided a larger vision of why data localisation is necessary for the progress of the nation.

Further, while localising data that is critical to Indian national security might be acceptable, the data in question should be narrowly defined and the authorities restricting the flow of this data should be held accountable for not exceeding this limit.

On the Intent Behind Data Localisation

Reduced access to technologies and solutions

The Report acknowledges that domestic industries might suffer some economic consequences of data localisation but that the benefits of such a move outweigh the costs. However, it does not recognise the impact that such a mandate might have on ordinary citizens. For instance, nascent industries offering innovative technologies and services that are based abroad might be disincentivised from extending their operations into India.

Alternatives to data localisation

The threat of localisation could have been used effectively without committing to it in the statute.

Real time access and real time capabilities for enforcement, similar to those provided in the CLOUD Act, would have been a less drastic and more desirable change.

Another alternative to localisation is to strengthen existing instruments such as the Mutual Legal Assistance Treaties, to enable access to law enforcement.

On Alternatives to Data Localisation

Transparency

There should be more transparency with regard to the internal workings of the DPA. This could be achieved by the inclusion of an independent director or a board of professionals/advisors within the management structure of the DPA.

Tenure of members

Given that members of the DPA are only eligible to serve one term, their tenures must be staggered to provide a measure of continuity to the functioning of the institution.

On the Structure of the DPA

Funding

The DPA should have an independent source of funding to ensure that it is free from the influence of the Union government.

Location

The DPA's primary mandate should be the regulation of data intensive industries. Hence, in order to be effective, it should be located in a place that has significant representation of such industries.

On the Structure of the DPA

Decentralisation as a means of being more effective

The functioning of the DPA would be more effective if it is distributed across regional and/or zonal offices. The law should make it more accessible as a grievance redressal and rectification forum to data principals.

This could have been achieved along the lines of existing mechanisms for consumer protection and the right to information.

Decentralisation as a means of avoiding regulatory capture

A regulator that is as big and powerful as the proposed DPA would become a target for regulatory capture by the State and the industry alike. A diffusion from decentralisation would make any such capture more difficult.

On the Decentralisation of the DPA

Separation of powers

The regulation and adjudication wings of the DPA must exhibit a clear separation from each other to avoid conflicts of interest.

Search and seizure

The DPA is vested with wide powers of search and seizure under the Bill. The Bill must provide appropriate checks and balances on such powers.

On the Functions of the DPA

Impact on industry

The scope of the DPA's activities under the Bill is vast. It is unclear if the small organisational setup envisaged will have the capacity to handle these tasks effectively. For instance, the DPA is tasked with the power to approve cross-border transfers, codes of practice for an industry or trade association, issuance of certificates of registration to data auditors and significant data fiduciaries, etc. Any delay in the performance of such functions can have adverse economic repercussions on the industry.

In addition to its role as a regulator, the DPA is also likely to receive a large volume of complaints for adjudication under its separate adjudicatory wing. Its capacity to resolve such complaints in a timely manner must also be examined.

On the Capacity of the DPA

Need for proportionality

Section 13 permits the State to process personal data without consent if it is *necessary*. Similarly, Section 19 permits the processing of sensitive personal data if it is *strictly necessary*. These provisions set a low standard for non-consensual processing by the State.

The additional standard that should have been included is that of *proportionality*. While necessity supplies the basis for the processing, proportionality helps define the extent to which such processing can take place. This would also conform to the standard discussed in Justice KS Puttaswamy (Retd) v Union of India.

On Processing of Data by the State

Imposition of penalties on State entities

The penalties under the Bill are monetary in nature and some of them are pegged to *total worldwide turnovers*. Aside from the fact that using worldwide turnover as the basis for penalising a fiduciary might be excessive, this standard is unclear in cases where the data fiduciary is a State entity.

Imposing liability on individuals

The Bill imposes liability on individual civil servants when offences are committed by government departments. A similar standard must be adopted for contraventions of the Bill that lead to penalties arising from harm occurring to a data principal.

On Penalties for State Entities

Uncertainties in the application of the law

Section 32 of the Bill requires data fiduciaries to report data breaches to the DPA, with the latter tasked with determining whether a data principal ought to be notified on a case by case basis. Given the frequency of data breaches, it is unclear if the DPA will have the capacity to examine each breach report in detail.

Further, the incentives that the DPA might have to not disclose incidents to individuals must also be considered.

It is also unclear if a data fiduciary will have the right to notify a data principal about a data breach without the need for prior permission from the DPA in this regard.

On Data Breach Notifications

Prescriptive nature

Despite the emphasis on a fiduciary relationship between an individual and an entity managing data, the Bill is highly prescriptive in nature, imposing stringent requirements on data fiduciaries.

The Bill seems to have followed the command and control model instead of a co-regulatory model. This narrative is visible in provisions that give the DPA the power to frame standards and guidelines, something that industry should develop outside of the statute.

Other General Comments

On harm

The Bill should have an exhaustive list of harms, instead of an inclusive one. This will reduce the uncertainty for data fiduciaries who will have more clarity on the permissible limits of their actions.

An alternative to this approach is a right against harm. This would be wider and more protective of the interests of individuals.

Applicability of a right to be forgotten against a data processor

The Bill provides for a qualified right to be forgotten. However, this right can only be exercised against a data fiduciary. In order to be truly effective, it should also be made applicable against a data processor.

Other General Comments

Prioritising access, information symmetry, and decentralisation

It is not just information asymmetry between the data principal and the data fiduciary that legislation should seek to reduce. There is considerable asymmetry between different legislations on the topic of collection and storage of data, which should also aimed to be reduced by the mechanisms provided in this Bill.

Just as it focused on reducing information asymmetries, it should also have brought in principles of systemic risk mitigation, ensuring data principals' access to appropriate recourse mechanisms, and opting for a more decentralised approach.

Other General Comments

Differing perspectives on surveillance

The Bill provides an exemption to surveillance activities of the State with the exact contours of such surveillance to be set out in a separate statute.

Some participants welcomed this move. Given that the primary focus of the Bill is the protection of data in transactional contexts, creating provisions for data as a surveillance tool would have been beyond its ambit, and would not have been done justice to.

Other participants were of the opinion that an exemption with minimal safeguards, namely that of fair and reasonable processing and security requirements, would provide wide discretion to the State to frame a surveillance law in the future.

Other General Comments

The Roundtable was chaired by Rahul Matthan, Fellow, Technology and Policy Research at the Takshashila Institution, and Manasa Venkataraman and Ajay Patri, researchers at the Takshashila Institution. The following is the list of participants to the Roundtable:

1. Amlan Mohanty, Senior Associate, PLR Chambers
2. Alok Prasanna Kumar, Senior Resident Fellow, Vidhi Centre for Public Policy
3. Beni Chugh, Research Associate, Dvara Trust
4. Biju Nair, Executive Director, SFLC.in
5. Divij Joshi, Research Fellow, Vidhi Centre for Public Policy

List of participants

6. Nayantara Narayan, Head of Policy, Office of Baijayant Jay Panda, Member of Parliament (Lok Sabha)
7. Nikhil Narendran, Partner, Trilegal
8. Pranav MB, Policy Officer, The Centre for Internet and Society
9. Pranesh Prakash, Independent lawyer and researcher
10. Sandesh Anand, Managing Consultant, Synopsys Inc.

List of participants (continued)

11. Shweta Mohandas, Programme Officer, The Centre for Internet and Society
12. Smitha Prasad, Programme Manager, Centre for Communication Governance
13. Subhashish Bhadra, Investment Principal, Digital Identity, Omidyar Network
14. Dr. Vijay Chandru, Chairman, Strand Life Sciences
15. Vinay Kesari, Independent lawyer and researcher

List of participants (continued)

In addition to the above participants, the following individuals contributed to the Blue Paper:

16. Nehaa Chaudhari, Public Policy Lead, TRA Law
17. Pushan Dwivedi, Associate, TRA Law
18. Tuhina Joshi, Associate, TRA Law

List of participants (continued)