2020

LEGAL BASES OF INFORMATION PRIVACY

EGCS Brief No.1

This Brief is an outcome of the investigation undertaken on the legislative design of the Personal Data Protection Bills 2018 and 2019. It brings into light the underlying assumptions of the present bill and elucidates the conceptual framework the bills have employed. The troubles with the model have been identified and a few solutions have also been suggested in this brief. Indications for an alternative model are also given in this brief. A detailed version of the alternate model, build exclusively on indigenous theoretical framework and extensive suggestions on the bill 2019 are available on request.

"षट् कर्णाद् भिद्यते मन्त्रः"

That which is heard by a third pair of ears is no more personal or private.

(Kautilya)

Proposed Centre for Data Protection Laws and Privacy
Chinmaya Vishwavidhyapeeth Deemed to be University
Cochin, 15th February 2020

Introduction

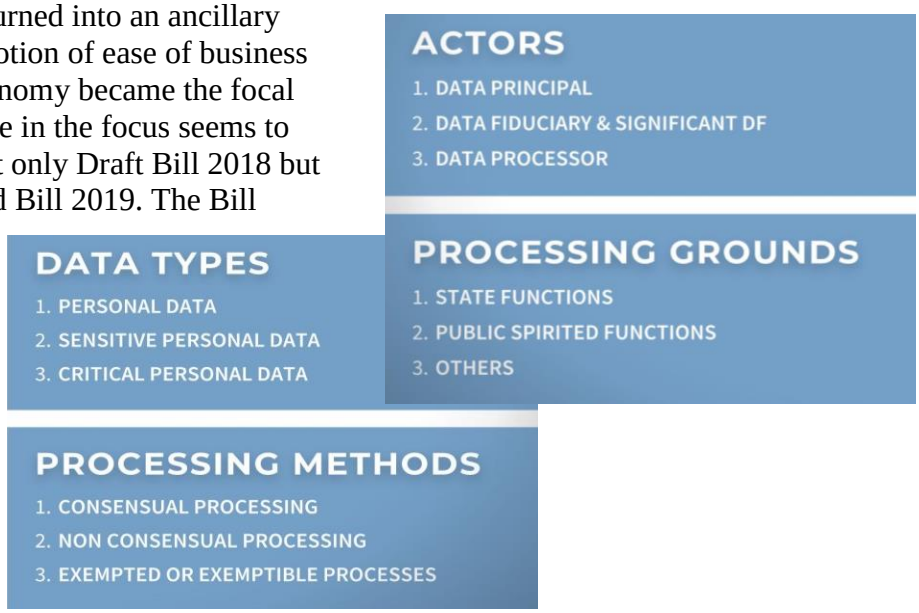
The Ministry of Electronics and Information Technology introduced the Data Protection Bill, 2019 in the Lok Sabha on December 11, 2019. The bill was put forth into discussion and has received varied comments.

The Puttaswamy judgement in 2017 conclusively held the Right to Privacy as a fundamental right, it became a positive duty imposed over the government to protect the privacy of the individuals.

The Government hence constituted an Expert Committee headed by Justice. B. N. Srikrishna to:

1. Study the issues relating to Data Protection In India
2. Make specific suggestions for consideration of the Central Government.
3. Suggest a draft Data Protection Bill.

The Committee did a tremendous job by coming out with an extensive report and a draft bill. The committee however, opted for a framework style bill incorporating a broader vision for its work: "to create a collective culture that fosters a free and fair digital economy, respecting the informational privacy of individuals, and ensuring empowerment, progress and innovation." The primary goal of data protection thus turned into an ancillary status, and promotion of ease of business in the digital economy became the focal point. The change in the focus seems to have affected not only Draft Bill 2018 but also the proposed Bill 2019. The Bill works primarily on these conceptual tools (refer boxes):



Conceptual Framework and Theoretical Assumptions

The current bill does not provide the individual an option to not to participate by not parting away with his personal data.

The bill opts for implementing curative measures rather than preventive ones. In the case of the Right to Privacy, it is those preventive measures which need to be effective for better protection of itself.

The existing bill also provides extensive list of grounds for recognition of non-consensual processing of data. Further, substantial items on the list are exempted from the scope of the bill. This way, consent needs to be obtained only in very few cases. Also the State can literally waive off application of any provision to any agency.

On further analysing the conceptual framework of the Bill 2019, it can be said that the individual's Right to Privacy is not being considered sacrosanct and personal data hence is being reduced to a trade-able commodity. The provisions conceive digital space as "a market" where such personal data can be traded at will.

The provisions of the bill seem to convey the meaning that digital economy is feasible only through laws enabling ease of business. The bill gives minimum mention to commercial purposes and its distributional effects.

Existing Standards

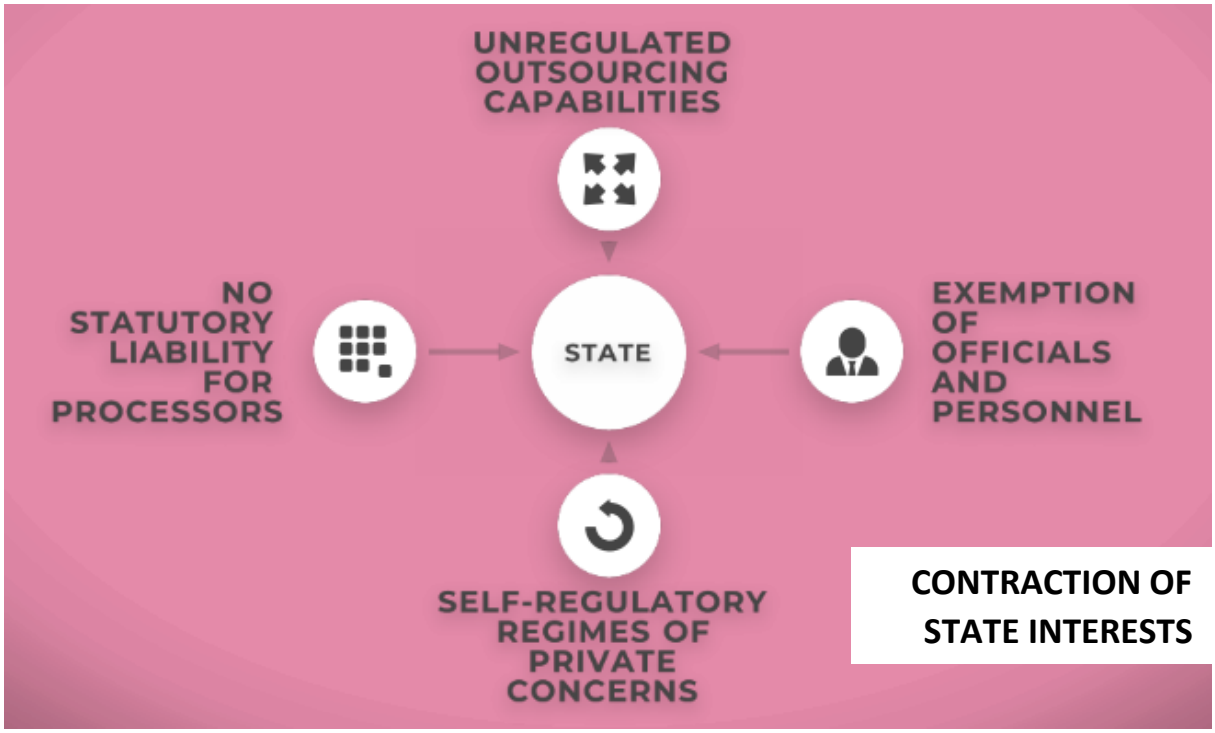
(a) Definition of Processing: The term 'processing' as defined by the bill includes several activities relating to collection, use, storage, organizing, alteration, erasure, dissemination, etc. These distinct activities potentially pose different threats to privacy whereas the consent for all is obtained as whole.

(b) Standard of Consent: The standards established regarding "consent" and "explicit consent" is ambiguous in nature and provides scope invasion of the Right to Privacy. According to the Bill 2019, consent needs to be free, informed, specific, clear and withdraw-able. Additionally the bill requires explicit consent for processing sensitive personal data. In this case the Data Principal needs to be informed of the harm or risk; he must have clarity without contextual reference and must be given choice for separate consent for different purposes and operation. The bill overlooks the potential confusion that arises in the application of the two standards whereby one could easily argue that there is no need of "informing Data Principal about harm or risk" in ordinary circumstances.

c) Discretionary Powers: The wide discretionary powers given to state to exempt certain categories of data processing and agencies from the provisions of the proposed law are antithetic to the principle of the due process of law. Although this is attempted to absolve the government fiduciaries from liabilities, it is counter-productive to governmental interests as well. The provisions of the bill almost stipulate no statutory liabilities for private data processors who most often take up outsourced state functions.

(d) Inefficient Categorisation: The global model of data processing laws rely upon the one-size fit all definition of processing and also upon differential standards in consent for specified and identified purposes. The Indian adaptation but further develops the idea of differential standards of consent into two different categories of "consent" and "explicit consent" applying to wide list of identified processing activities.

(e) *Jurisdictional Reach:* The trust based model of law requires data fiduciary to internally arrange for officers dealing with complaints. Failing which data principal can approach adjudicators. However no provisional measures are indicated in the bill. Also geographical concerns are not addressed.



Zeroing of Statutory Liabilities

The provisions of the bill also reduce the statutory liabilities that may be fixed on the fiduciaries and processors in protecting personal data.

1. The private data fiduciaries can develop a self-regulatory scheme which is monitored by the Data Protection Authority.

2. The Government fiduciaries are insulated from the provisions in the name of sovereign authority.

3. The private contractors of government fiduciaries too are liable only according to the terms of the contract.

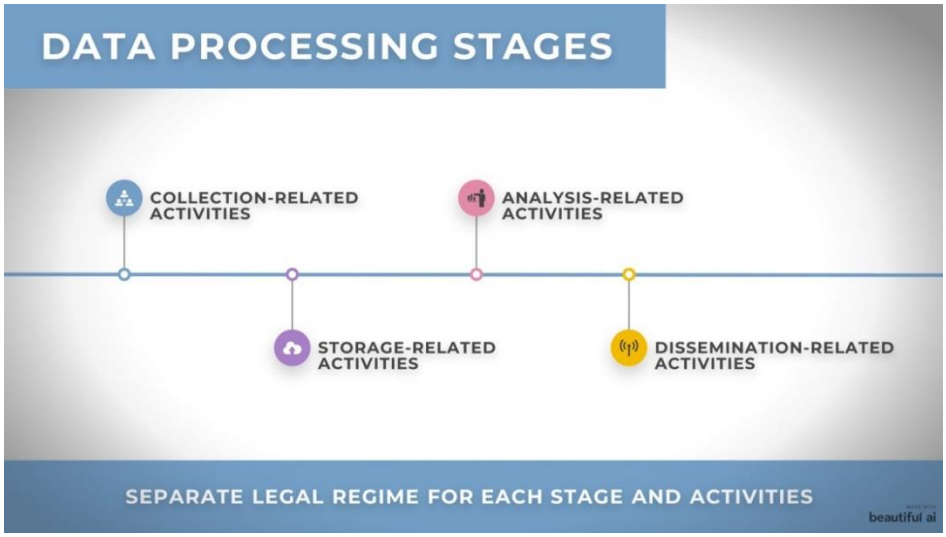
This leaves the data principal at a very high risk while parting away with his personal data. Also, it is the data principal who is held responsible for all the consequences for not providing access and for withdrawing consent.

Given the capacity of the State as a fiduciary in the digital economy, there is every chance that its business interests will get overturned badly.

Legislative intervention in this area can expand the state interests, both economic and political.

Recommendations

1. Separate legal regimes for the distinct stages of processing need to be developed and incorporated into the provisions of the bill. For instance, major stages involved can be Collection related activities, Storage related activities, Analysis related activities and Dissemination related activities.



2. *Single Standard of Informed Consent:* The consent to be obtained should be free, informed, unambiguous, granular and withdraw-able. Data Protection Authority to specify field-specific additional requirements, after analysing the special needs of said field.

3. Self-determination of Sensitivity: Individual should be able to deny consent for processing personal data based on what he considers as sensitive for his life, and his privacy. Denial of consent by the person on the grounds of sensitivity should not lead to denial of service. Data protection officer of the Data Fiduciary or Processor must attempt reconciliation strategies. Any dispute may be referred to the Adjudicators office.

4. Expand Access to Justice and Indicate Provisional Measures: The legislation of the present model must call for tribunals in every state and adjudicators in every district without leaving it policy decision of the Central Government. Since data breach or privacy violation most likely is of continuous in nature, the legislation must provide for the provisional measures to be taken by Data Protection Officers, Adjudicators, and Tribunals pending any decisions on the complaints.

5. Doctrine of Essentiality: Personal data should be processed on the grounds of 'essentiality' rather than the current standard of 'necessity'. Not only access, but also scope of activities such as organisation, storage, analysis and dissemination should be limited under the same rule. Individuals must have the right to contest any inefficient application of the doctrine.

6. Statutory Liabilities for Data Processors: Statutory liabilities for all Data recipients are the only way by which state interests as well as human rights can be safeguarded.

Alternatives Possible?

Yes, indeed. The legislative design and policy have to answer few inherent questions such as (1) Foundational Elements and Material content of Right to Privacy; (2) Nature of Personal Data Transactions; (3) Nature of Digital Space; (4) Ascendance of Information Science. For the answers and the alternative model, please see Policy Study Report PSR_EGCS 2020/1