AN ANALYSIS OF THE PROPOSED INDIAN DATA PROTECTION ACT

Introduction

In a landmark judgment delivered on the 24th of August 2017, now popularly known as the Puttaswamy judgement, a 9 judge bench unanimously ruled that every citizen of India had a fundamental right to privacy which was guaranteed by the Constitution of India within Article 21 in particular and Part III on the whole.

In response to the need to protect the personal data of citizens, The Union Government of India, acting through the Ministry of Electronics and Information Technology constituted a Committee of Experts to deliberate on a data protection framework for India. Justice B N Srikrishna was appointed as the Chairman and the committee was given the following terms of reference:

a) To study various issues relating to data protection in India
b) To make specific suggestions for consideration of the Central Government on principles to be considered for data protection in India and suggest a draft data protection bill.

The Committee completed its work and submitted its report and a draft Personal Data Protection Bill to the Ministry of Electronics and Information Technology for further consideration on 27th of July 2018. This document is referred to as the (Indian) Draft Personal Data Protection Bill (PDP) 2018.

The Draft PDP Bill of 2018 was reviewed internally by the Union Government, and was tabled in Lok Sabha as Bill No 373 of 2019. This Draft Bill was referred to a Joint Parliamentary Committee by the Lok Sabha on 11th December 2019. This Bill was also referred to the above mentioned Joint Parliamentary Committee by the Rajya Sabha on 12th December, 2019.

The JPC made a total of 91 recommendations for change as part of their report. A total of 8 members of this JPC submitted dissent notes/memos, which are annexed to the JPC report.

Objectives of the proposed Act

The JPC proposed the following objectives for the proposed Data Protection Act in its report, presented and laid in Parliament on 16th December 2021to provide for protection of the digital privacy of individuals relating to their personal data, to specify the flow and usage of data, to create a relationship of trust between persons and entities processing the data, protect the rights of individuals whose data are processed, to create a framework for organisational and technical measures in processing of data, to lay down norms for social media platforms, cross-border transfer, accountability of entities processing data, remedies for unauthorised and harmful processing, to ensure the interest and security of the State and to establish a Data Protection Authority of India for the said purposes and for matters connected therewith or incidental thereto.

Whereas the right to privacy is a fundamental right and it is necessary to protect personal data of an individual as an essential facet of informational privacy;

And whereas the growth of the digital economy has expanded the use of data as a critical means of communication between persons;

And whereas it is necessary to create a collective culture that fosters a free and fair digital economy, respects the informational privacy of individuals that fosters sustainable growth of digital products and services and ensures empowerment, progress and innovation through digital governance and inclusion and for matters connected therewith or incidental thereto.

Analysis of proposed objectives

It can be seen that from being a Bill focussed primarily on the privacy protection of individuals, it has now become a Bill that confers some privacy rights to citizens but provides a legislative basis for the implementation of digital governance schemes, enabled by the curtailment of privacy rights in terms of exemptions to Government Agencies. This was exactly the issue that was raised in the original Puttaswamy writ petition of 2012. The interest and security of the State is now an objective, and the proposed Data Protection Authority (DPA) will have to take that into consideration as well. The subordination of the DPA in all matters of the Central Government creates a classic conflicting situation. The DPA must protect the citizens' privacy but the DPA is subordinate to the Central Government in policy so its ability to be impartial in assessing the justification for exceptions to the Central Government or its agencies on grounds of security and interest of the state is debatable.

Implementation Practicalities

To be successful, the proposed Data Protection Act must be implementable without too much ambiguity and without incurring a prohibitive cost in terms of technology and management costs associated with protecting, managing and governing data. Certain aspects of the proposed Act need careful consideration in order to be practically implementable.

Ambiguity, Subjective Interpretation and Context Dependencies

Data has a complex and multidimensional nature. It can be classified in various ways and these classifications may not be mutually exclusive. Thus data is sometimes viewed as being structured v/s unstructured, real-time v/s non-real time, confidential v/s non-confidential, transactional data v/s master data, personal v/s non-personal.

Apart from the issue of classification of data which is potentially fraught with ambiguity, subjective interpretation and context dependencies can pose challenges.

As an example, the proposed Act permits the use of purposes that are incidental to and lays down some important conditions for processing.

5. Every person processing personal data of a data principal shall process such personal data—

> (a) in a fair and reasonable manner and ensure the privacy of the data principal; and
>
> (b) for the purpose consented to by the data principal or which is incidental to or connected with such purpose, and which the data principal would reasonably expect that such personal data shall be used for, having regard to the purpose, and in the context and circumstances in which the personal data was collected.

It is not clear if the consent is to be sought for any of the incidental or connected purposes or whether that is to be left to interpretation and to be assessed as a matter of fact in case such an incidental or connected purpose is contested. Also the concept of fair and reasonable may be subject to interpretation especially in the situation where several exceptions are allowed to Government agencies and there is no guidance on fair and reasonable. The proposed Act identifies processing that is not legal without consent, but apart from that does not

provide any indication of how that processing can be determined to be fair and reasonable.

Complexity

There are the complexities of codifying purposes of processing, what constitutes critical data and the need to ensure that certain types of data are processed and stored within the country. Thus processing needs to be done with a significant amount of awareness of how and where the data is stored and processed.

The proposed Act places significant data management requirements on data fiduciaries. For example, the requirements to ensure data quality are stated as follows:

> 8. (1) The data fiduciary shall take necessary steps to ensure that the personal data processed is complete, accurate, not misleading and updated, having regard to the purpose for which it is processed.
> (2) While taking any steps under sub-section (1), the data fiduciary shall have regard to whether the personal data—
> (a) is likely to be used to make a decision about the data principal;
> (b) is likely to be disclosed to other individuals or entities including other data fiduciaries or processors; or
> (c) is kept in a form that distinguishes personal data based on facts from personal data based on opinions or personal assessments.
> (3) Where personal data is disclosed to any other individual or entity, including other data fiduciary or processor, and the data fiduciary finds that such data does not comply with the requirement of sub-section (1), the data fiduciary shall take reasonable steps to notify such individual or entity of this fact.

This requires the ability to have comprehensive visibility of the entire information inventory of an organization and ensure that data quality processes are in place to ensure accuracy and correctness as well as reconcile inconsistencies. This may be required to be done in real-time. The complexity of ensuring the information management systems are geared up to managing this volume of data and to introduce new elements in the architecture to deal with the data classification, tagging and consent management requirements, requires an entire information management and governance system to be put in place. In contrast it is revealing to look back upon the cost and complexity of fixing the Year 2000 problem. This was conceptually simple, but fixing it was assessed at costing between $100 billion and $200 billion globally.

Analysis of practicality of implementation

The preceding paragraphs have highlighted the inherent ambiguities, subjectivities and context dependencies inherent in classifying data. Meaningfully classifying data and then processing it based on a system of consent management pre-supposes an existing system of data governance and management. This is unlikely to be true for most organizations. For most organizations either a data governance and management system will need to be introduced or the existing one significantly re-vamped to accommodate the requirements imposed by the proposed Act.

The volume of data being generated, transmitted, processed and stored is increasing significantly. According to an International Data Corporation (IDC) forecast, the "Global Datasphere" is expected to be about 60 Zetabytes in 2022 and grow nearly three times to about 175 Zetabytes in 2025. A very high percentage of this is unstructured data in files, images, videos and other such data stores.

Most organizations are currently running legacy data infrastructures and lack the budgets and adequately trained/ skilled resources to cope with the deluge of data. They are struggling to keep their data infrastructures up and running.

The requirements of the proposed Act mean that now data has to be somehow "marked" to indicate if it is personal, sensitive or critical and applications have to be aware of where it is stored and processed. This will probably imply changes to data storage layout and impacts to applications of a large scale, which will have to be followed with comprehensive testing. A nuance of ensuring that certain types of data remains in the country is that while storage and processing end point are relatively well defined, data in transit may take routes that may cross national borders. This will be an additional factor to consider in implementation.

With the backdrop of significant increase in data volume, diversity of types of data and the shortage of resources, implementing the provisions in any meaningful way will be very difficult without standards or best practices that can be followed. The need for trained auditors will also be extremely large and unless a standardized way can be found to train and up-skill existing auditors, this may prove to be a significant bottleneck.

One of the practical ways to deal with the issues of ambiguity, subjective and context dependent interpretations and complexity is to develop and use standards that will establish practices that can be followed. This is a multi-disciplinary problem and an institution like the Bureau of Indian Standards is well positioned to undertake such an activity. These standards can codify acceptable practices which will lead to uniform implementations of practices and will be an invaluable help to those organizations that do not have the requisite human resources to develop these pracices on their own.

Conclusion

The proposed Data Protection Act has evolved from being a law primarily focussed on the privacy of citizens to one which enables various Digital Governance schemes and regulates social media platform operation. The nature of Data has its own complexities and making laws that are able to balance the needs of all stakeholders is an unenviable endeavour. The law, sometimes on account of the nature of data and privacy themselves and sometimes due to conflicting objectives of different stakeholder communities, has ambiguities and presents significant complexities and scale-up challenges to practical implementation. If we are to do a reasonable job of implementing such a law this will require standardization of good practices and acceptance of these good practices. These practices are more likely to be robust if they are evolved by consensus underpinned by a robust public consultation process such as the one followed by the Bureau of Indian Standards.■

Author

Sundeep Oberoi

(The author is Adjunct Professor – ADCPS IIT Bombay)