The Dialogue™
INFORM ENGAGE IDEATE

THE PERSONAL DATA PROTECTION BILL, 2019

GEOPOLITICAL IMPLICATIONS

Shefali Mehta

GEOPOLITICAL IMPLICATIONS

1. Introduction

The often unwelcome comparisons of data and oil have helped clarify one concept - that data is a global commodity with wide-reaching geopolitical implications. How data is collected, stored, processed, and transferred across geographical borders has increasingly become the subject of discussion in foreign policy. However, data governance globally remains in a nascent stage with constant skirmishes in the manner in which data is regulated across different jurisdictions. How data is regulated also has implications on issues such as tackling misinformation online, protecting citizens from perceived harms and providing redressal when these harms arise thereby compounding its importance and leading to nations adopting varied approaches.

India is rapidly growing to become a key player in the global digital economy. Our nascent attempt at establishing a robust data protection framework will also have far-reaching implications in how we are perceived as a nation in the global market and in our economic prospects. Data and artificial intelligence (AI) are expected to add $500 billion to India's Gross Domestic Product by 2025[1]. Also, considering that India is among the largest generators of user data, along with being a go-to destination for data processing, India's framework must align and work in harmony with international standards and best practices.

This primer will highlight key areas of the Personal Data Protection Bill, 2019 (PDP Bill) that will have implications geopolitically and recommendations to tackle certain drawbacks in this regard.

2. Key provisions and our recommendations

2.1. Inclusion of non-personal data under the ambit of the PDP Bill, 2019

The PDP Bill , gives powers to the Indian Government to "act to promote framing of policies for digital economy", which has been further interpreted to include the regulation of anonymised data or non-personal data sets as well. Besides, there is also provision that empowers the Central Government to direct any data fiduciary/data processor to provide non-personal data to 'enable better targeting of delivery of services or formulation of evidence-based policies.' The definition of non-personal data in the PDP Bill states that 'data other than personal data' is non-personal data which provides room for wide interpretation of the term.

The provision in the PDP Bill undermines the existing business practices wherein the data processor is contractually bound by the data fiduciary and cannot share data (personal or non-personal) or any insights thereof, as they belong to the client of the data processor on whose behalf the data processing entity is conducting data processing activities as per instructions and contract. This will have a massive impact on the business confidence of clients and foreign nationals, of data processing companies in India as they would be apprehensive of the Government of India's access to data.

1 Unlocking Value from Data and AI - The India Opportunity, NASSCOM India and McKinsey, August 2020

Such a provision is likely to discourage innovation and investments in India on the part of foreign partners seeking to invest in India, as the Government is asking for non-personal data as well as anonymised personal data. There are also concerns that business-sensitive information, including trade secrets, may be sought under the Bill (as discussed in our business consideration primer). As data has been defined to include "insights collected from data", such access to data by the Government would infringe upon the intellectual property rights of companies and other businesses. The provisions in the PDP Bill is likely to bypass the control of the data fiduciary and obligations of data processors under their contract with data fiduciary, again leading to hesitance among international companies.

Additionally, there are concerns regarding the safety or privacy of such data sought via provisions in the PDP Bill owing to the fact that combination of different datasets poses re-anonymisation concerns.

Our Recommendations

The MeitY has concurrently been working with a Committee of Experts led by Mr. Kris Gopalakrishnan to look into the governance of non-personal data and its use in evidence-based policymaking. We reiterate our suggestion from the previous primer that non-personal data regulation remains out of the ambit of the personal data protection bill, 2019.

Legislators and the Government may draw inspiration from the EU's move to develop a voluntary sharing mechanism with companies for this end as envisaged in the EU's Data Governance Act.[2]

2.2. Data Localisation Mandates under the PDP Bill, 2019

Data localisation is the act of storing data on any device physically present within the boundaries of a country. A data localisation regime also imposes restrictions on cross border data flows. According to the PDP Bill, the requirement of storing a copy of all personal data in India has been removed, which is a welcome step forward.

However, a copy of sensitive and critical personal data must be stored in India. Sensitive personal data can be transferred outside India in certain situations. Critical personal data can only be processed in India, and the Indian Government will notify the categories of personal data that will qualify as 'critical personal data'. Critical personal data can be transferred outside India on specified limited grounds.

Restrictions around the flow of data will hurt the objective of enabling a trillion-dollar digital economy. According to a study conducted by The Dialogue, it was pointed out that cross-border data flow is fundamental to the growth of the economy. The report suggests that localisation may also cost up to 11% of the average Indian worker's salary. ICRIER's estimates that even a 1% decline in cross border data flows will reduce the volume of trade by US$ 696.71

2 EUROPEAN COMMISSION Brussels, 25.11.2020 COM(2020) 767 final 2020/0340 (COD) Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT

million. This is particularly important given that personal and sensitive personal data (like financial details) are intertwined, and the localisation policy has a spillover effect on all forms of data. The data segregation leads to overhead cost increasing and additional technological cost as well.

Besides, the contours of critical and sensitive personal data are not defined in parent legislation, and the onus of the same being with the Central Government further invites ambiguity.

Our Recommendations

We recommend that the Government implore conducting a cost-benefit analysis to understand the economic effects of data localisation before considering the application of stringent data localisation requirements. Additionally, it would be prudent for the Government to reconsider the data localisation requirement and instead aim to develop a multilateral or bilateral framework that governs the cross-border flow of data in terms of access and sharing. Either bilateral and multilateral avenues along the lines of EU-US Privacy Shield, Convention 108 or the APEC-CBPR privacy model would help the Government achieve its objectives while being at par with other jurisdictions globally. In addition to this, the Government must also consider a bilateral arrangement with the US Government through the CLOUD Act to seek access to data for law enforcement.

2.3. Interoperability of the Indian framework

Interoperability plays a critical role in the digital ecosystem. Benefits from data are maximised when it is Findable, Accessible, Interoperable and Re-usable.[3] In its Digital Agenda, the EU Commission has identified a lack of interoperability as one of seven "most significant obstacles" to digitalisation's "virtuous cycle".[4] However, while placing importance on interoperability in the digital ecosystem, one must remain aware of how interoperability is a means to achieve better efficiency of a system but comes with some costs.

Data interoperability: Interoperability helps enhance the effectiveness of data by presenting or storing in standardised models, coupled with easy data transfer protocols to enable knowledge and insight sharing. Though achieving interoperability may incur costs to institutions and entities, its long-term payoffs ensure that the trade-off between cost and benefit is fair.

In the context of data protection, interoperability is a precondition for the interconnectedness and free flow of data that is crucial for a data-based economy, and therefore for data-driven innovation.[5] Besides, in a data-based economy, interoperability and portability will also bring healthy competition, as data fiduciaries will be nudged to explore alternative value propositions to remain competitive in the market. One of the outcomes of this could be better consumer protection through innovation of privacy safeguards, etc. In addition to this, interoperability and portability could enable a low barrier to entry (through breaking the network effect), which could, in turn, increase penetration of digital services in untapped geographies as more driven-driven businesses emerge in the market.

3 Crouzier, T. (2017). IPR, Technology Transfer & Open Science. European Commission. Retrieved from IPR, Technology Transfer & Open Science.
4 EU Commission, A Digital Agenda for Europe, Brussels, 19.5.2010, COM(2010)245 fin., p. 3.
5 Wolfgang Kerber and Heike Schweitzer, Interoperability in the Digital Economy, 8 (2017) JIPITEC 39 para 1. https://www.jipitec.eu/issues/jipitec-8-1-2017/4531/JIPITEC_8_1_2017_Kerber_Schweitzer.pdf

Data transfer frameworks: The Indian Government has been driving the agenda of interoperability for a long time. However, in India, interoperability with global laws in terms of data transfer cannot be seen anywhere. The Government often ignores the benefit of interoperability in positively impacting consumer choice, ease of use, access to content, diversity, etc.[6] It helps in driving innovation, competition, accessibility, openness and flexibility. For example, in a health care system, interoperability could play a crucial role in accessing the health records of a person who suffers from a critical illness. Even in the case of foreign transfer of the patient for the treatment, an interoperability framework between the Government in terms of sharing health records could be crucial.

Our Recommendations

Though India is at the nascent stage of developing its data protection frameworks and systems, there is scope for developing strong interoperable models with the world. However, the Government must take advantage of lessons from other jurisdictions to inculcate those principles into the law right at the lift-off stage.

2.4. Establishment of an independent data protection authority in India

Data governance norms and frameworks of a nation today form an important part of conversations at the international level. Data privacy concerns are an important aspect of trade-related negotiations across the globe, with countries demanding protection of their citizen's data as it travels across borders. For example, Article 45(2)(b) of EU GDPR requires the European Commission to consider the existence and functioning of an independent data protection authority for a country to pass the adequacy test. It has increasingly been noticed that data protection authorities play a crucial role in facilitating the sharing of data across borders and operationalisation of the same. For India to negotiate on an equal footing and present India as an attractive destination for investment in technology, we must institute a robust data protection authority.

Our Recommendations

We recommend the establishment of a separate and independent regulatory body for data that is free from any undue influence on the part of the Government, either in the form of appointment or in case of functioning through financial dependence.

6 Gasser, U. (2015). Interoperability in the Digital Ecosystem. Information Technology & Systems eJournal.

2.5. Absence of surveillance safeguards and exemption of the Central Government from the Provisions of the PDP Bill

A glaring drawback in India's proposed framework has been the absence of addressing surveillance activities and safeguards being placed on the same. The same issue has been exacerbated by the inclusion of provisions that empowers the Central Government to exempt itself and allied bodies from the provisions of the proposed framework. The presence of poor safeguards pertaining to similar activities or the absence of continued protection of data across borders has formed the crux of disagreements between jurisdictions while working to recognise each other's data protection systems and allow for the free flow of data between them. For example, the recent Scherms II judgment by European Courts held that the present legal system of the USA provides insufficient protections in terms of access to data by their Government and their national surveillance infrastructure, which led to the EU withdrawing their adequacy status (referring to how the EU determines a non-EU country has an adequate level of data protection to facilitate transfer of data freely). For India to continue remaining an attractive destination for data processing and storage, India must ensure such protections are in line with international best practices.

Our Recommendation

We recommend that India enact a surveillance framework at the earliest with adequate safeguards and a due process that respects citizens' rights and ensures there is no scope for misuse.

The Dialogue is a public-policy think-tank with a vision to drive a progressive narrative in India's policy discourse. Founded in 2017, we believe in facilitating well-researched policy debates at various levels to help develop a more informed citizenry, on areas around tech-nology and development issues.

The Dialogue was ranked amongst the Top-Ten think-tanks in the world to watch out for by the Think-Tank Civil Societies Programme, Lauder Institute, University of Pennsylvania, in their 2020 and 2021 ranking index.

Email: info@thedialogue.co
Website: www.thedialogue.co

The Dialogue™

INFORM ENGAGE IDEATE