The issues around data localisation

The contentious clauses on local data storage in the revised Personal Data Protection Bill need re-examination

RISHAB BAILEY

Among the many important laws that were introduced in the winter session of the Lok Sabha was the Personal Data Protection (PDP) Bill, 2019. The Bill was referred to a joint parliamentary committee, which is currently engaged in a process of public consultation.

The draft law is a comprehensive piece of legislation that seeks to give individuals greater control over how their personal data is collected, stored and used. Once passed, the law promises a huge improvement on current Indian privacy law, which is both inadequate and improperly enforced.

The PDP Bill, however, is not without its flaws. It has attracted criticism on various grounds such as the exceptions created for the state, the limited checks imposed on state surveillance, and regarding various deficiencies in the structures and processes of the proposed Data Protection Authority.

Data localisation in draft Bill

One of the more contentious issues in the law Bill are the provisions pertaining to "data localisation". The phrase, which can refer to any restrictions on cross-border transfer of data (for instance, requirements to seek permission for transfer, the imposition of taxes for foreign transfers of data, etc.), has largely come to refer to the need to physically locate data within the country.

The PDP Bill enables the transfer of personal data outside India, with the sub-category of sensitive personal data having to be mirrored in the country (i.e. a copy will have to be kept in the country). Data processing/collecting entities will however be barred from transferring critical personal data (a category that the government can notify at a subsequent stage) outside the country.

These provisions have been changed from the earlier version of the draft Bill, released by the Justice Srikrishna Committee in 2018. The 2018 draft imposed more stringent measures that required both personal and sensitive personal data to be mirrored in the country (subject to different conditions).

The move to liberalise the provisions in the 2019 version of the Bill is undoubtedly welcome, particularly for businesses and users. Liberalised requirements will limit costs to business and ensure users have greater flexibility in choosing where to store their data. Prima facie, the changes in the 2019 draft reflect a more proportionate approach to the issue as they implement a tiered system for cross-border data transfer, ostensibly based on the sensitivity/vulnerability of the data. This seems in accord with the Supreme Court's dicta in the 2017 Puttaswamy case, where the Court had made it clear that an interference in the fundamental right to privacy would only be permissible if *inter alia* deemed necessary and proportionate.

GETTY IMAGES/ISTOCKPHOTO

However, on closer examination it appears that even the revised law may not actually stand the test of proportionality.

Purpose of localisation

There are broadly three sets of arguments advanced in favour of imposing stringent data localisation norms: Sovereignty and government functions; referring to the need to recognise Indian data as a resource to be used to further national interest (economically and strategically), and to enable enforcement of Indian law and state functions. The second claim is that economic benefits will accrue to local industry in terms of creating local infrastructure, employment and contributions to the AI ecosystem. Finally, regarding the protection of civil liberties, the argument is that local hosting of data will enhance its privacy and security by ensuring Indian law applies to the data and users can access local remedies.

But if data protection was required for these purposes, it would make sense to ensure that local copies were retained of all the categories of personal data provided for in the Bill (as was the case with the previous draft of the law). In the alternative, sectoral obligations would also suffice (as is currently the case with sectors such as digital payments data, certain types of telecom data, government data, etc.).

Protecting user privacy?

In a 2018 working paper published by the National Institute of Public Finance and Policy, we pointed at the fallacies in the assumption that data localisation will necessarily lead to better privacy protections. We note that the security of data is determined more by the technical measures, skills, cybersecurity protocols, etc. put in place rather than its mere location. Localisation may make it easier for domestic surveillance over citizens. However, it may also enable the better exercise of privacy rights by Indian citizens against any form of unauthorised access to data, including by foreign intelligence.

Overall, the degree of protection afforded to data will depend on the effectiveness of the applicable data protection regime.

We note that insofar as privacy is concerned, this could be equally protected through less intrusive, suitable and equally effective measures such as requirements for contractual conditions and using adequacy tests for the jurisdiction of transfer. Such conditions are already provided for in the PDP Bill as a set of secondary conditions (the European Union's General Data Protection Regulation too uses a similar framework).

Further, the extra-territorial application of the PDP Bill also ensures that the data protection obligations under the law continue to exist even if the data is transferred outside the country.

If privacy protection is the real consideration, individuals ought to be able to choose to store their data in any location which afford them the strongest privacy protections. Given the previously mentioned infirmities in the PDP Bill, it is arguable that data of Indians will continue to be more secure if stored and processed in the European Union or California (two jurisdictions which have strong data protection laws and advanced technical ecosystems).

In the circumstances, it becomes important for the joint parliamentary committee currently examining the Bill to conduct a more in-depth evaluation of the localisation provisions in the law. The joint parliamentary committee ought to, ideally, identify the need, purpose and practicality of putting in place even the (relatively liberal) measures contained in the PDP Bill. Further, in order for localisation-related norms to bear fruit, either in terms of protecting citizen rights, enabling law enforcement access to data or enabling development of the local economy, there has to be broader thinking at the policy level. This may include for instance, reforming surveillance related laws, entering into more detailed and up-to-date mutual legal assistance treaties, enabling the development of sufficient digital infrastructure, and creating appropriate data-sharing policies that preserve privacy and other third party rights, while enabling data to be used for socially useful purposes.

Rishab Bailey is a fellow at the National Institute of Public Finance and Policy, New Delhi, where he works on technology policy