NUS National University of Singapore | ISAS Institute of South Asian Studies

ISAS Brief
No. 1035 – 6 July 2023

Finalising India's Data Protection Bill

Karthik Nachiappan

Summary

After years of discussion, debate and dissent, the end is near for India's much-awaited data protection legislation as it moves toward the final parliamentary approval.

Almost six years after the Indian Supreme Court declared that privacy was a constitutional right for all Indians, the government is now close to passing a legislative framework that protects the data of Indian citizens. The Indian cabinet passed the Digital Personal Data Protection Bill (2022) on 5 July 2023, the first critical move toward getting the bill passed and enshrined into law. This bill will now be tabled in parliament during the upcoming monsoon session. So far, the passed bill's provisions remain confidential until it is brought to parliament but this version is expected to largely reflect the version revised late last year. Some of the most debated and controversial aspects of the bill will likely remain, especially the exemptions granted to the Central government and its agencies that remain beyond the purview of this legislation. There will likely be no mega data regulator or data protection authority to oversee the law's implementation and compliance. Little is known about how the Indian government will negotiate and sign data-sharing agreements with other countries. That said, the cabinet's assent and imminent passing of the bill, once parliament opens, represents an important moment and achievement for India and one that will have massive domestic and international implications.

The Digital Personal Data Protection Bill (2022) will serve as the overarching privacy and digital framework alongside other technology regulations that the government is drafting like the Digital India Bill, the IT Act's (2000) successor; the draft Indian Telecommunication Bill and a framework to govern non-personal data. Before submitting the revised version of the bill last November, the government overhauled the bill after intensive and iterative reviews by a parliamentary joint committee and consultations with other stakeholders, including technology companies and civil society organisations. The revised 2022 bill limits the framework to personal data alone; the processing of personal data in India; and to processing of personal data of Indian citizens abroad. It also mandates data fiduciaries – entities that collect personal data – to protect and secure data, maintain its accuracy and follow strict guidelines for its deletion and removal. The bill will be governed by a small Data Protection Board that will ensure compliance and review cases when fiduciaries violate the law. The board can levy fines and penalties, given the nature and size of the transgression. Once the bill becomes law, citizens can also question fiduciaries over how the data they collect is being treated, stored and processed.

Concerns remain over the framework revised last year. Still, the central government and key agencies remain exempt from the bill's provisions. Why? The bill justifies the government's exemption on the grounds of national security and public order but this sweeping claim fails to account that the government also functions as a data fiduciary, collecting and processing

data. Additionally, the bill has not clarified whether the board will include representatives from non-governmental organisations or will be entirely staffed and managed by bureaucrats. That said, it is expected that the board will include industry and government representatives but speculation remains over what methodologies or approach they will use to identify breaches and sanction violators to eliminate arbitrary use of this power. Finally, concerns exist over the law's congruence with the Right to Information Act which functions as a torch pushing government officials to disclose information but this data protection framework gives the government the ability to conceal information. How can these two critical frameworks be reconciled?

What are the international implications of the bill? Importantly, the government will have to clarify how it wants to deal with cross-border data flows and whether it will move from a whitelisting approach which allows global data flows to a blacklisting approach that identifies countries where data transfers from India will be prohibited. The previous version mentioned that the government will only whitelist jurisdictions or identify countries where the personal data of Indian citizens will be transferred. Whitelisting will involve negotiating agreements with countries on how they will manage and protect the personal data of Indian citizens, a judgement that will ostensibly have to be made by assessing that country's data protection regulations and its relationship with India. The government will have to reveal how this process will unfold, given India's dramatic digital transformation and its importance to other countries and their tech firms.

Finally, the eventual passing of the bill will mark an important moment because of India's dynamic digital economy and digital economic potential. It is also a critical juncture in global data governance that is characterised by three existing models – the European Union's General Data Protection Regulation that prioritises user rights; the United States' libertarian model that delegates protection to firms; and China's security approach that sequesters all data. India's developmentalist model anchors the state at the centre of data governance that could serve as a model for countries looking to challenge and discipline technology companies that have collected, misused and abused personal data.

. . . . .

Dr Karthik Nachiappan is a Research Fellow at the Institute of South Asian Studies (ISAS), an autonomous research institute at the National University of Singapore (NUS). He can be contacted at isaskn@nus.edu.sg.
The author bears full responsibility for the facts cited and opinions expressed in this paper.