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

ISAS Brief

No. 1049 – 14 August 2023

The Final Passage: India's Digital Personal Data Protection Act 2023

Karthik Nachiappan

Summary

Both houses of the Indian parliament have passed the personal data protection bill into law after years of debate, discussion and dissent.

On 3 August 2023, the Lower House of the Indian parliament – the Lok Sabha – passed the Narendra Modi government's Digital Personal Data Protection Bill, 2023. The bill became law after the Rajya Sabha – the parliament's Upper House – passed the bill on 9 August 2023. The passage marks the culmination of six years of lawmaking, characterised by fierce lobbying, consultations, revisions, public discussions, withdrawals and resubmissions. The most recent iteration reflects a bill that has changed considerably, much too cosy to the state, not citizens' interests.

The first revision of the bill, released in 2019, called for a comprehensive data protection framework backed by a strong regulator – a data protection authority that had the power to make and enforce regulations. Privacy was a clear motivation. The bill pushed for a regime that protected personal data and ensured its processing occurred carefully. Sanctions for potential breaches and violations were not the focus. This bill empowered data principals – the users providing the data – certain rights in the processing of their personal information; and data fiduciaries – those holding and storing data – to follow specific rules and procedures to ensure privacy and security.

The 2019 bill also exempted the state and all its agencies from the rules it imposed on all other data fiduciaries, given overriding national security and public order considerations. This data regime would have been predictable, reasonable and user-centric, with exceptions strewn in for state authorities. The 2019 bill represented a massive expansion of public authority with little precedent; no Indian regulator had experience dealing with data-related issues or making and enforcing data protection regulations. The process from a bill to an act would have been difficult and filled with complications related to capacity and implementation creating enormous regulatory uncertainty.

The bill's second revision (2022) and largely the version passed now is different. It is a highly simplified, pithier version that reduces the institutional burdens of the state to regulate personal data while creating a regime that expects data fiduciaries to undertake lesser obligations to protect, process and store data or face penalties if they fail to do so. The law defines 'personal data' rather broadly by covering necessary information identifying an individual. The bill requires companies and organisations to secure adequate consent from users before collecting personal data and bars them from using or misusing it for purposes other than what was categorically mentioned; that said, consent may not be required for specified uses such as voluntary sharing of personal data by the individual or processing by

the state when providing direct services. The law also prevents companies from anonymising personal data and deploying it through artificial intelligence or other kinds of models.

Potential data breaches will produce steep fines levied on fiduciaries who neglect or discharge their responsibilities. Exemptions reserved for state agencies remain; the bill, however, does not expand on what it means by 'security and public order' nor does it define what standards it uses for sovereignty, and integrity which could be intentional to keep the state's remit wide. More problematically, the bill also allows government agencies to access user data from companies and individuals without consent. Rather controversially, the law revises the 2005 Right to Information Act of 2005 (RTI Act) by removing prevailing exceptions when disclosing personal information for the public interest; the RTI Act effectively obliges public authorities to reveal personal information, like income, when it could serve the public interest.

The incoming regulator – the proposed Data Protection Board – would have limited regulatory power and oversight with the government retaining more powers over how the board functions, who sits on it, and its authority to sanction organisations and firms who fail to adequately protect data. The board will be a creature of the Ministry of Electronics and Information Technology lacking effective writ and independence to govern. The government will also determine how personal data transfers and flows occur between India and other countries; flows will only occur to countries notified by the central government and ostensibly barred everywhere else. With enormous power to draft subordinate legislations, grant exemptions, decide how transfers occur, and control the functioning of the Data Protection Board, the government has placed itself at the apex of India's information order.

The new data protection act marks an important moment in India's digital economy and governance. Undoubtedly, this law will have a massive impact on India's economy as sectors digitalise rapidly; the Indian state as it digitalises its architecture and functioning; and India's politics as citizens use digital technologies for various purposes; and the Indian society as internet users negotiate how to best protect themselves online.

. . . . .

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.