Data localisation norms: A key pillar for privacy protection

December 2019

Introduction

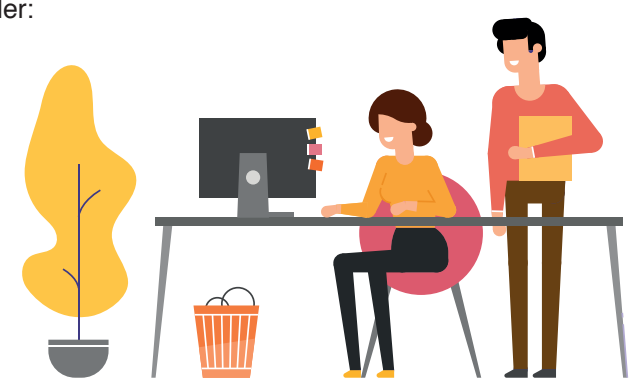
Privacy is now recognised as a fundamental right in India. On 24 August 2017, a nine-judge bench of the Supreme Court ruled that the right to privacy is a fundamental right for Indian citizens under Article 21 of the Indian Constitution.[1]

The need to categorise privacy as a fundamental right in India has increased as technological innovations have become more common, and organisations regularly come up with new modes of collecting, processing and dealing with personal information of individuals. The rapid digitisation of India's economic infrastructure has led organisations and authorities to believe that data plays a critical role in the advancement of the economy. Even advanced economies such as the European Union and the United States of America have recognised data as the basis of economic advancement and have implemented new Legislation to protect and conserve sensitive data.

Current regime and changing landscape

The present laws related to data protection in India come under:

- the Information Technology Act (IT Act), 2000, and the rules framed there under
- the Indian Penal Code (IPC), 1860
- other sectoral regulations.



Despite their existence, data protection laws and regulations in India often do not cater to the changing needs of the country's business environment. To address these shortcomings, the Ministry of Electronics and Information Technology (MeitY), Government of India (GoI), had constituted a committee of experts under the chairmanship of the retired Supreme Court judge Justice B N Srikrishna. The objective of the committee was to identify the lapses in the present data protection regulations and prepare data protection laws which were more robust and comprehensive, and draft the Personal Data Protection Bill (PDP), 2018, which is yet to be enacted.

1 KS Puttaswamy v Union of India (2017), 10 SCC 1

Over the last few years, GoI is increasingly trying to tap the transformative potential of the digital economy. GoI's initiatives towards data localisation and cross-border data transfer indicate that data is a collective resource and a national asset, over which citizens have a sovereign right and sharing of data requires certain restrictions to be set in place. These concepts broadly refer to the practice of limiting data storage and processing and/or movement of data to specific geographies. One of the directions given to the Justice Srikrishna committee studying data protection issues in India said that GoI's objective was to 'unlock the data economy, while keeping data of citizens secure and protected'.

Localisation and cross-border framework

Data localisation requirements and cross-border transfer can be imposed in two ways, either by mandating the storage of local copies of data within the territories in India, with exceptions of mirroring, as per data classification, or by creating certain restrictions on the cross-border movement of data. One of the first requirements for local storage of data was brought about in 1993, with the Public Records Act, 1993, which restricts the transfer of public records outside India. However, the first directives regulating non-government data took a more flexible approach.

Over the next few years, other acts and regulations related to data security came up in India. In 2006, the Reserve Bank of India (RBI) allowed banks to outsource non-core banking activities to other countries (as per the circular on Guidelines on Managing Risks and Code of Conduct in Outsourcing of Financial Services by Banks, November 2006). The Information Technology Act, 2000 (read with the Information Technology [Reasonable Security Practices And Procedures And Sensitive Personal Data Or Information] Rules, 2011), allowed the transfer of sensitive personal data or information outside India, as long as those countries ensured the same level of data protection and upheld confidentiality agreements.

Presently, the framework for transfer of electronic data between the governments of two countries is initiated vide Mutual Legal Assistance Treaties (MLATs). MLATs are binding treaties signed by countries to assist each other with domestic legal processes.

Under such framework, law enforcement agencies of one country request evidence held in another country for criminal or civil prosecution, frequently pursuant to an MLAT in place. However, gathering evidence through MLAT processes is time consuming, which results in delay of justice, at times. Hence, storing data, localising it and restricting access to it, typically by classifying it as sensitive and critical (to be listed by the relevant authorities of any country in due course), becomes imperative.

There have been a flurry of regulations across sectors which have stricter norms on storing data in India. Some sectoral recommendation reports for machine-to-machine (M2M) communication[2] and the storage of financial data on the cloud[3] recommended that data should be stored in servers located in India. In 2017, several directives and regulations were put in place for data localisation across sectors. For example, the Insurance Regulatory and Development Authority of India (IRDAI) issued regulations on outsourcing activities by Indian insurers, restricting outsourcing of certain activities such as legal services, banking services, and courier services. The regulations also stipulate that all original policyholder records should be maintained in India.[4]

2 Department of Telecommunication, Ministry of Communication, National Telecom M2M Roadmap 2015

3 Institute for Development and Research in Banking Technology (IDRBT), Cloud Security Framework for Indian Banking Sector (Best Practices) 2012

4 Insurance Regulatory and Development Authority of India (Outsourcing of Activities by Indian Insurers) Regulations, 2017

Similarly, MeitY released guidelines for government departments that are engaged in providing cloud services to incorporate clauses in their contracts that mandate storage of data and computational results in India.[5] The latest and one of the most stringent measures imposed has been the RBI's April 2018 mandate to store all payments system data exclusively in India. The payments industry was given six months to comply with the notice without any exceptions. However, in June 2019, the RBI clarified that data can be sent outside India for processing, under the condition that no copy of the data is kept outside India. As a result, payments service providers will need to set up data centres or store their data with cloud service providers who use data centres in India.

Some observations

Data localisation norms may entail greater investment in terms of time, cost and new infrastructure. As a result, companies, especially start-ups, may face financial stress. However, these norms would aid the growth of data centres and the cloud computing industry in India.

The government needs to develop robust internet infrastructure to support the implementation of data localisation norms, so that setting up barriers for data privacy does not impact trade and business between countries.

A strong data localisation framework and laws/regulations could play an important role in protecting Indian consumers and the country's national and economic interests. Such norms would secure citizens' data and enhance data privacy and sovereignty from foreign surveillance.

Restricting cross border transfer of data shall ensure national security by providing ease of investigation to Indian law enforcement agencies as they would not be required to rely majorly on MLATs to obtain access to data and may minimise conflict of jurisdiction due to cross border data sharing and delay in justice delivery in case of data breach.

5 Ministry of Electronics and Information technology (Meity) Guidelines for Government Departments on Contractual Terms Related to Cloud Services under the Meghraj Cloud Initiative, 2017

About PwC

At PwC, our purpose is to build trust in society and solve important problems. We're a network of firms in 157 countries with over 276,000 people who are committed to delivering quality in assurance, advisory and tax services. Find out more and tell us what matters to you by visiting us at www.pwc.com.

In India, PwC has offices in these cities: Ahmedabad, Bengaluru, Bhopal, Chennai, Delhi NCR, Hyderabad, Kolkata, Mumbai, Pune and Raipur. For more information about PwC India's service offerings, visit www.pwc.in

PwC refers to the PwC network and/or one or more of its member firms, each of which is a separate legal entity. Please see www.pwc.com/structure for further details.

Acknowledgements

This article has been researched and authored by Debashree Mukherjee, Kanwarpreet Singh and Goldie Dhama

Contact us

Dhritimaan Shukla
Partner and Privacy Leader
dhritimaan.shukla@pwc.com
+91-9899038326

Sonali Saraswat
Associate Director, Privacy
sonali.saraswat@pwc.com
+91-9620701515

PD/Decemeber 2019-M&C 3761