ISAS Brief

No. 597 – 10 August 2018

Institute of South Asian Studies
National University of Singapore
29 Heng Mui Keng Terrace
#08-06 (Block B)
Singapore 119620
Tel: (65) 6516 4239 Fax: (65) 6776 7505
www.isas.nus.edu.sg
http://southasiandiaspora.org

India's Quest for Data Protection

Growing concerns about data privacy has led India to formulate a number of policies to protect the privacy of its citizen and other stakeholders, as well as to support its goal of becoming a digital and technologically-advanced economy. This paper assesses the various data protection-related policies enacted by the country and highlights the contradictions among the various policies.

Dr Rahul Choudhury[1]

Background

Like any developing country, India is gearing towards becoming a digital economy and developing into an international data hub. It has embraced technological developments in various fields. To support this goal and due to the concerns about the privacy of its stakeholders, India has formulated a number of policies to regulate the growing digital sector. The latest step in this regard is the setting up of a committee under the chairmanship of retired chief justice of the Supreme Court of India, B N Srikrishna. Although the committee recently submitted its report to the government, it has not been promulgated into law as it must first be approved by the Indian parliament. The significance of the Srikrishna Committee report has increased due recent incidents such as that involving United Kingdom-

[1] Dr Rahul Choudhury is a Visiting 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 rahulchoudhury@nus.edu.sg. The author bears full responsibility for the facts cited and opinions expressed in this paper.

based firm Cambridge Analytica and the enactment of the European privacy law – the General Data Protection Regulation. Apart from the Srikrishna Committee, a number of other committees were also formed in this regard. At the same time, steps were undertaken at the sectoral level to address issues relating to data protection and the digital economy.

Steps Taken so Far

The Information Technology (IT) Act 2000 was perhaps the first step in India to regularise and monitor the growing information technology industry. It is a comprehensive policy which provides legal recognition for transactions carried out by means of electronic data interchange and other means of electronic communication, commonly referred to as 'electronic commerce'.[2] However, being an almost two decade-old policy, it did not incorporate many of the issues which emerged at the later stages of development in the IT industry.

Concerned with the privacy of the citizens and their data due to the unexpected growth of the e-commerce industry and the digital economy at large, India formed a committee of experts on privacy under the chairmanship of the former chief justice of the Delhi High court, A P Shah. The committee studied both national and international privacy principles and recommended the formulation of a privacy policy framework. The committee submitted its report in October 2012.[3] The report defined privacy as rights of the citizen and suggested that the government informs the citizens about the practices of the data collector before collecting information from them. Only the relevant data should be collected and the citizens should be informed about the purpose of the data collection. However, the report did not touch the issue of data sharing with a third party. The provisions of the storage and the location of the data were also missing in the report. The steps taken by the government on the recommendations of the committee were never available to the public. At the same time, the reasons for not enacting the privacy law are also unknown.

---

2 Information and Technology Act, 2000, Ministry of Electronics & Information Technology, Government of India. http://meity.gov.in/writereaddata/files/itbill2000.pdf. Accessed on 14 July 2018.

3 Report of the Group of Experts on Privacy. http://planningcommission.nic.in/reports/genrep/rep_privacy.pdf. Accessed on 12 July 2018.

In 2017, with the aim of ensuring the growth of the digital economy while keeping the personal data of the citizens secure and protected, India set up another Committee of Experts to make specific suggestions on the principles underlying a data protection bill and draft a bill. Once again, it relied on a former justice to undertake the task. Under the chairmanship of the former judge of the Supreme Court of India, B N Srikrishna, a committee of nine members (including the chairman) submitted a white paper for public comments and feedback.[4] The committee studied various aspects of the data, ranging from collection to storage and further sharing with others. The committee also studied the privacy laws enacted in various countries and suggested some key reforms, which included penalties and compensations in the case of data breach. The white paper also suggested creating a data protection authority to monitor, investigate and enforce the laws, set the standards and generate awareness in an increasingly digitised society.

After gathering feedback and comments from the stakeholders, the committee took the task forward and submitted the final report to the Indian government on 27 July 2018. The report made a series of recommendations and mentioned that around 50 existing laws, including the Aadhaar[5] and the Right to Information Act,[6] need to be amended to include the data privacy law. The report defined personal data and maintained that only necessary data should be collected. The committee also recommended that personal data should be stored on servers located within India, and transfers outside the country should be subject to safeguards. Critical personal data, however, should only be processed in India.

Recommendations and Regulations

Both the Shah and Srikrishna committees have extensively studied the existing laws around the world and made their recommendations accordingly.

---

4 White Paper of the Committee of Experts on a Data Protection Framework for India. http://meity.gov.in/writereaddata/files/white_paper_on_data_protection_in_india_18122017_final_v2.1.pdf. Accessed on 14 July 2018.

5 The Aadhaar is a 12-digit unique identity number issued to residents of India, based on their biometric and demographic data.

6 The Right to Information Act 2005 is an act of the Parliament of India to provide for the setting out of the practical regime of the right to information for citizens.

The Shah Committee focused more on the privacy of the citizens while the Srikrishna Committee report emphasised data protection and related issues. The former considered privacy as the right of the citizen and that consent is necessary before the collecting and sharing of personal data. However, this report did not focus on the location of the data.

The Srikrishna Committee cautioned about the cost of data localisation. It recommended partial localisation of the data. It also stated that the different types of data will have to be treated differently, given their significance for enforcement and industry. The committee also felt that an embracing umbrella model may not be the most appropriate. Data localisation may be considered in certain sensitive sectors and it should not be applied unanimously.

Apart from these two drafts, there are many other sector specific regulations that applied to the stakeholders. The Draft National Digital Communications Policy 2018, the Reserve Bank of India's Notification on Payment Data Storage 2018, the Guidelines for Government Departments for Contractual Terms related to Cloud Storage 2017, the Digital Information Security in Health Care 2018 and the Indian Medical Council Regulations 2002 have also notified their stakeholders on the collection and storage of the data. Contrary to the Srikrishna Committee report, all these guidelines have mandated the stakeholders to locate or store the data only in India.

Contradictions and their Implications

The contradiction in the policies on restricting cross-border data flows and mandating the localisation of certain data, in a situation when cross-border data flows contributed US$2.8 trillion (S$3.82 trillion) to the global economy in 2014, and are expected to reach US$11 trillion (S$14.99 trillion) by 2025, may have serious implications on Indian businesses and their stakeholders.[7]

[7] "Approach Data localization with Care", Narayan Sidharth, *The Hindu Business Line*, 29 June 2018. *https://www.thehindubusinessline.com/opinion/approach-data-localisation-with-care/article24281271.ece*

An immediate contradiction of the decision to store data locally relates to India's trade facilitation agreement for services submitted to the Council for Trade in Services at the World Trade Organization. Here, India has advocated the free flow of data across borders.

The motivation for data restrictions includes securing the citizens' data privacy, cybersecurity, data sovereignty, national security and economic mercantilism.[8] However, the value of the data is maximised when it moves.[9] Research and innovation are increasingly driven by how firms collect, transfer and analyse data. The mandatory localisation of the data will increase the cost to the firms which may be discouraged from investing in a country. It will also create barriers for existing companies to share the data across borders for regular activities. In the age of artificial intelligence (AI), big data and machine learning, mandatory data localisation may deprive the country and its citizens of harnessing various technological advancements. With the help of AI and big data, many of the illnesses can be diagnosed and treated more accurately and quickly. However, the clause of not transferring medical data out of the country will have a negative impact on the health sector as well as many other sectors in India. Industries such as business process outsourcing will also be hit as its entire business model is based on data inflow and outflow. Similarly, the agricultural sector, which has begun to embrace modern technology and has benefitted by forecasting weather and productivity growth, will also suffer.

The Way Forward

Given this situation, it is necessary to allow for the free flow of data for the benefit of the Indian economy as well as for its citizens. The contradiction arising from existing policies and committee proposals should be addressed immediately. India should also adopt a consistent stand in domestic and international policy on data movement. Considering the potentials of modern technology, India should formulate a policy that allows it to take advantage of new technology without exposing the data privacy of its citizens. A strict monitoring of data collection will help to avoid another Cambridge Analytica-like incident. Lessons can be learned from the European and other countries which have already

8 Ibid.

9 Cory Nigel (2017). Cross *border data flows: where are the barriers and what do they cost?* Information Technology and Innovation Foundation, USA.

implemented comprehensive data privacy policies. Indian policymakers should also consider that it is not only the location of the data that makes it safe and secure, but the privacy policy and security that is provided to the data by the data controller is also equally important.

. . . . .