Data Localisation

Background

The Personal Data Protection Bill (PDPB) 2019[1], requires explicit user consent, as well as approval of the Data Protection Authority (DPA) or the central government, as the case maybe, and certain conditions being met, for transferring sensitive personal data (SPD) outside the country.[2] Also, a copy of the same is mandatorily required to be stored within the country.[3] Additionally, critical personal data (CPD), which is yet to be defined clearly by the PDPB, has not been allowed to be transferred outside the country, unless for a few narrow exceptions relating to health services or emergency services, or to certain entities outside India only after the approval of the Central Government, if it is satisfied that such transfer does not prejudicially affect the security and strategic interest of the country.[4] Notably, these requirements are a dilution from the Data Localisation (DL) requirements of the Draft Bill of 2018,[5] which imposed local storage of a copy of all personal data.

Shortcomings

Segregation of Types of Data: A substantial portion of SPD is being shared by data principals (users) with different data fiduciaries (service providers) while availing various data driven services. A few instances include financial data being shared with ride hailing apps, food delivery service providers, e-commerce companies and many others. Religious beliefs are being shared with social media platforms, as well as online dating service providers and matrimony websites. Sharing biometric data (finger print scanners and facial recognition software) has become popular amongst consumers for securing their mobile devices from unauthorised use. Given that such SPD is shared in combination with other personal data, it may become burdensome for service providers to segregate the two. This is especially true for smaller service providers, who may not be able to devote adequate resources for such a process, and be compelled to store the entire personal data shared with them, in India, or stop serving Indian consumers (particularly in case of smaller foreign service providers, operating in multiple countries).

Additionally, the bill empowers the government to prescribe more categories of SPD and CPD in future under Section 15 and Section 33(2) respectively, without setting clear standards for defining their scope. Also, there is no mention of a timeline for compliance with local data storage

requirements of SPD/CPD, which is notified in future. This creates ambiguity for service providers to formulate ways for organising their data, for meeting the localisation requirements under the bill.

Potential Impact of DL on Consumers: A Consumer Impact Assessment study undertaken by CUTS[6] highlighted adverse impact of DL on users in terms of possible reduced uptake of select data-driven services, such as e-commerce, social media and communication services. The study suggests that DL is expected to enhance risks of privacy violation, cyber-attacks and data breaches, while adversely impacting the availability of services and curbing innovation.[7] Hence, while the current bill dilutes certain requirements of DL, there still persists challenges in terms of assessing the effect of DL for SPD and CPD on users.

Possible adverse economic impact: CUTS study 'Digital Trade & Data Localisation'[8] showcased the adverse impact of DL on India's IT-BPM industry, with respect to digital services export. The scope and extent of data restrictiveness may plunge the digital services exports between 10 to 19 percent. This may translate to a shortfall of US$19-US$36bn in achieving the US$1tn economic value potential of the digital sector in 2025. The decline in digital services export will negatively affect the gross domestic product (GDP) by 0.18 to 0.35 percent, causing a shortfall of US$9bn to US$17bn in US$5tn economy objective in 2025.

Recommendations

Regulatory Impact Assessment (RIA): Before taking any decision on prescribing more categories of SPD and CPD, as well as dis/allowing transfer of SPD and CPD, the DPA and/or central government must undertake RIA. Conducting RIA in these scenarios, will ensure that costs imposed by data localisation does not outweigh its intended possible benefits, not only for the consumers but other stakeholders such as service providers.[9] Additionally the findings of such RIA should be published in public domain.

Explore least intrusive means of achieving valid regulatory objectives: The focus of the current bill must remain on upholding privacy and ensuring data protection, and should not be allowed to become a tool for LEA's to access data or propelling economic development. With regards to ensuring regulatory objectives of LEAs the government should strengthen Mutual Legal Assistance Treaties, and pursue international cooperation by becoming a member of 'Chart of signatures and ratifications of Treaty 185: Convention on Cybercrime', or entering into bilateral treaties on the lines of United States Clarifying Lawful Overseas Use of Data (CLOUD) Act. With respect to economic development, encouraging domestic innovation and creating jobs, a separate

policy to incentivise processing of data in India may be formulated, instead of forcing DL (as has also been called for in budget 2020)[10].

Strengthen Cross Border Data Flows & adopt best practices: The benefits of cross-border data flows are well documented. In order to encourage the same, India should consider best practices around the world in developing guiding principles for allowing processing of data outside India. The government may consider Asia Pacific Economic Cooperation (APEC) privacy framework[11], APEC Cross-Border Privacy Rules[12] and the recent Digital Economy Partnership Agreement (DEPA) signed between Singapore, Chile and New Zealand, which seeks to enable trusted cross-border data flows between them.

1 The Personal Data Protection Bill 2019. Available at: http://164.100.47.4/BillsTexts/LSBillTexts/Asintroduced/373_2019_LS_Eng.pdf

2 Section 34(1) of the Bill

3 Section 33(1) of the Bill

4 Section 34(2) of the Bill

5 Draft Personal Data Protection Bill 2018, available at:

6 Findings available at: https://cuts-ccier.org/pdf/Findings_of_Consumer_Impact_Assessment_of_Data_Localisation.pdf

7 https://cuts-ccier.org/consumer-impact-assessment-on-cross-border-data-flow/the study involved in depth interaction with 40 subject experts, and a survey of over 1200 consumers.

8 Study available at: https://cuts-ccier.org/pdf/project-brief-dtdl.pdf

9 Regulatory Reform Bill

10 https://www.livemint.com/news/india/govt-s-nudge-may-help-india-become-a-global-data-centre-11580664564132.html

11 APEC Privacy Framework , 2015

12 APEC Cross Border Privacy Rules , CBPR