

India unfurling the Domain of Data Privacy: The Personal Data Protection Bill

The adoption of some or the other form of legal framework for data privacy and security by 107 countries is a clear indication of data privacy gaining momentum worldwide. India has become the latest entrant in the arena of data protection with the approval of Personal Data Protection Bill drafted by Shri Krishna committee, by the union cabinet of the Government of India. Among 60 countries in Asia Pacific Region about 45 percent that is 27 countries has incorporated some laws for data privacy. This figure is less than half of the implementation rate in Europe, which is 98 percent. Since the scandal of Cambridge Analytica, data privacy has become a topic of public discussion and somehow forced all the major economies to frame legislations to regulate the use of data. European Union came up with GDPR in 2018 and China announced the Data Protection Regulation Guideline in June 2019, whereas, the United States formulated CLOUD Act in March 2018.

Unlike America and Europe, where the data privacy laws have been adopted for long now and are currently moving towards handling the data at micro level, India is still characterized as a data rich economy with poor culture of data protection. In India, the awareness of digital users concerning their personal data is alarmingly low and in many cases they are unconcerned about privacy of their personal data.

Lab survey conducted by Stella in 2019 of 311 used devices which included memory cards, smartphones and hard drives revealed that out of 10 used devices 7 had Residual Data which could be accessed and misused easily. The further investigations highlighted that due to lack of awareness regarding safe disposal of storage media, 45 percent of these devices were disposed of unsafely and the data was present as it is on these devices, without any action by the owner or the seller. The business organisations are in urgent need to secure data. A study by Gartner reveals that 80 percent of enterprises in today's scenario of technological shift are bound to migrate from on-premises data centres to cloud and most of the companies are yet not prepared to tackle the sensitive and vulnerable data.

With the emergence of Personal Data Protection Bill the companies operating in India would need to upgrade their systems, policies and practices to comply with the norms of the bill, failing to do so will put these companies at risk of lawsuit and huge fines. The expert committee under the chairmanship of Justice BN Srikrishna classified the data is General, Sensitive and Critical. General data is permitted to be stored and processed without any restrictions while critical data will be from time to time defined by the government and is required to be processed and stored in India. The sensitive data that includes religious and political beliefs, financial indicators, health and biometric data is permitted to be stored only in India, however, in exceptional conditions it can be processed out of the country with due permission. Failing to abide by these norms will attract financial penalties for the companies which can be up to rupees 15 crore or 4 percent of the global turnover if they share the data without the consent of the user and on the breach of data and inaction to resolve the same will attract the financial penalty of rupees 5 crore or 2 percent of global turnover.

Besides, the concern for data privacy, the PDP bill also addresses the issues of essential domains like national security, foreign investment, data infrastructure and law enforcement. Investment in local data centres, manpower investments, loss of economies of scale and tight control by regulators are few of the challenges seen by the experts in concern to foreign players. On the other hand experts also feel that, right to access the large undeveloped Indian consumer market by the global companies should come at a price. Joint ventures between a foreign partner and a Indian company will enhance technology transfer and increase the expertise of the local partner in learning the technical knowhow of the foreign partner. It could be a fair price paid by the foreign companies if they invest in local data centres and train Indian engineers to manage them, thereby getting access to one of the world's largest consumer markets. With 270 million users as of July 2019, India is Facebook's largest market. Out of 15 data centres globally, one is in Singapore, four in Europe and 10 are in North America. So having a data centre of Facebook in India does not seem unlogical. It is not a surprise when ByteDance, the parent company of tik tok announced to setup a data centre in India as the country is the world leader in installing mobile apps with 4.5 billion downloads in the first quarter of 2019 and tiktok was India's most downloaded application. The recent announcement of the Adani group to have a tie up with US based data centre solutions provider to setup data centre infrastructure in Hyderabad, will definitely have a positive outcome.

Apart from securing the national interest and avoiding over dependence on other countries for essential infrastructure development, government is also considering the other beneficiaries like Indian law enforcement agencies under the ambit of PDP bill. The agencies will get access to data for anti terrorism purposes directly without passing through the hassle of international channels.

Presently, the enforcement agencies are facing quite a challenge in accessing personal data from companies that are governed by U.S. laws.

The PDP bill is undoubtedly right step for the large unexplored market like India. But to extract benefit of it without restricting innovation and discouraging foreign investment, the government should have clear policies and should avoid shifting goals. Further, there will be the requirement of legislation to bound the technology companies to decrypt encrypted communications.



(Prof Mahima Birla)

Editor in Chief