Data protection Act: Mind the gaps

TV RAMACHANDRAN

Honorary fellow, IET (London),
and president, Broadband India Forum
Views are personal

While the focus on consent as the cornerstone of data processing makes for a robust mechanism, it is impractical to ask businesses to give microscopic, granular notices

Data is often referred to as the new oil, though the description is a gross understatement. Data is far more powerful. Like nuclear fission, it has the power to do enormous good or wreak incalculable harm. This double-edged characteristic underscores the importance of having adequate rules or laws for oversight over data generation, processing and usage. Hence, the government is to be lauded for coming out with the Digital Personal Data Protection (DPDP) Act recently, which attempts to "provide for the processing of digital personal data in a manner that recognises both the rights of individuals to protect their personal data and need to process such personal data for lawful purposes and for matters connected therewith or incidental thereto." Of course, this Act has been many years in the making and that is a strong indicator of the challenges and the many debates and consultations needed. However, "being right is more important than being fast". With this legislation, the government of India has clearly demonstrated its commitment to data protection. While the industry-friendly DPDP Act is a significant and commendable step towards safeguarding digital privacy and data handling practices in India, traces of concerns with the previous versions of the law are lingering, in addition to some new concerns arising from the introduction of new concepts and revisions.

Understandably, the Act empowers the Union government to exempt any government agency from the Act on grounds like sovereignty and integrity of India, security of the state, friendly relations with foreign states, law and order management, etc. Such exemptions are doubtless essential; however, certain aspects of these exemptions do not gel well with principles of necessity and proportionality as laid down by the Supreme Court's judgment in the *Puttaswamy* matter that recognised the right to informational privacy as a fundamental right and specified certain requirements to be fulfilled for this right to be restricted.

The government collects vital data from all citizens and is one of the biggest data fiduciaries. Hence, such exemptions must be narrowly constructed to foster greater trust among the citizenry regarding sharing and processing their personal data. Moreover, clause 17 (1) (d) that denies the protections of the Act to foreign data principals must be revisited, considering its inconsistency with the protection norms provided in other progressive jurisdictions and the obstructions that might arise due to it in seamless fulfilment of adequacy conditions during bilateral and multilateral trade deals. Experts recommend that Clause 17 (1) (d) be removed from the Bill.

The clause denying protection to foreign data principals also needs to be relooked at, to harmonise the law with the protections accorded in other jurisdictions

While the Act's focus on consent as the primary ground for data processing is to be welcomed, it is equally important to address the difficulties this could pose for both individuals and businesses. To ensure ease of approach, emphasis on 'clear and plain language' must be given while giving organisations time to adjust their privacy policy.

It would be appreciated that it is impractical to ask businesses to provide microscopic granular notice, and no user will take the trouble to go through a long list and tick boxes (yes or no) for scores of boxes every time they sign it to an app or website.

The government has taken welcome steps to protect the interests of children and disabled people. However, it would be useful for the Indian rules to establish an age-appropriate framework based on best global practices. Exemptions for such data processing could be modelled in a manner encouraging responsible data usage without hampering business innovations. At the same time, rules should provide exemption in relation to monitoring and profiling in the best interests of children like safety and security.

The Act has brought far more clarity than earlier on the important aspect of the Data Protection Board (DPB). However, it is noted that the Board's selection process is executive-driven, where the government will select the chairperson and members of DPB in addition to setting the terms of office. The Board's function seems significantly diluted in terms of its actions protecting the interests of the data principals and promoting awareness about data protection, while emphasis is laid on determining non-compliances and imposing penalties. The earlier clause for enhancing functions of the DPB has also been removed, which is unfortunate.

On cross-border data transfers, the government is to be lauded for allowing this for data processing. It would add further strength to this aspect if there is more clarity provided regarding mechanisms like Binding Corporate Rules, Contractual Clauses, etc.

The government deserves rich kudos for coming out with a benchmark Act that could, in many respects, be a model for other countries. Of course, harmonising India's data protection rules with the global best practices requires a nuanced approach. Recognising that every legal framework has distinct merits, our rules should be an optimised blend of these insights, sculpted in accordance with India's socioeconomic context. Drawing from the world's best data protection practices and integrating business-friendly provisions, we can ensure a thriving digital ecosystem that respects individuals' rights while propelling innovation and growth.