The data-locker law

By Meenakshi Lekhi | Issue Date: January 24, 2021 | Updated: January 14, 2021 14:24 IST

Since the advent of internet technology in the early 1990s, the world is dealing with swarm drones! This is a huge leap, all made possible because of foundational technologies evolving around artificial intelligence, the Internet of Things and cloud computing. Given these explorations and innovations, one thing which has become the focal point is—data. Yes, data is the buzz word, and rightly so. It is the new oil propelling the digital economy. It has gained all the more importance after the pandemic restricted physical movement across the globe.

Now, data is not restricted to a collection for limited purposes. Rather, it is generated at an exponential rate, heavily consumed, and put to algorithmic setups to gain the minutest of the insights never imagined before.

Given this sea of change, challenges, threats and opportunities, the data universe needed an urgent legislation to protect national security and the interests of its citizens. As a result, governments all over came up with legislative frameworks to define, categorise, regulate—and the associated intricacies to deal with—data protection. India, too, is coming up with a Personal Data Protection Bill.

As a result of extensive deliberations, suggestions and improvements, personal data stands defined and its legal and regulatory framework for legislative scrutiny is in place, safeguarding the right to privacy of the data principal and the corresponding interplay with the data fiduciary, along with a gamut of checks and balances. Data, broadly classified under personal and non-personal heads with respective sub-classifications, are bound to have overlapping definitions, guidelines and regulations, but still, the broad classification is necessary to make sure that the entire data regime serves the objective, making it amply clear as to "who stands where", "within what jurisdiction", and "within what mandate".

Illustration: Bhaskaran

At a very simplistic level, anything which does not fall under the definition of personal data constitutes non-personal data. But taking this simplistic approach as the only way to understand non-personal data is a risky proposition that could be full of pitfalls. Often, personal data is the source that leads to the production of non-personal data, when the former undergoes "anonymisation" procedures. The key distinguishing feature of non-personal data is the non-identification of the data principal. But, the risk of re-identification always remains. This possibility cannot be ruled out because today's data economy is full of technological advances that can always make it possible—both the "backward integration" as well as the "forward integration"—to produce one from the another—that is, non-personal data from personal and vice versa. Hence the necessity for a set of legislative and regulatory frameworks for both personal and non-personal data, which shall act in unison, leaving no scope of grey areas, especially when it comes to individual's privacy as well as sensitive data protection, which is imperative from the strategic and national security viewpoint.

Any piece of legislation is dynamic, and goes through amendments to meet the changed circumstances as and when required. But the dynamism of data protection legislation is not going to be just one clause; rather it will be a unique and defining feature. After all, we are in a stochastic environment where digital footprints are being produced in the continuous-time domain and our ensemble as discussed above is left with a Hobson's choice to stay put in the continuous state space, hence the course corrections have to be continuous to meet the unforeseen challenges.