Right to privacy in Bangladesh in the internet era

CONTINUED FROM PAGE 14

ILLUSTRATION: STAR

A few advocates of data nationalism have made fallacious economic and commercial arguments in favour of data localisation: more data centres would mean increased economic growth and more high-tech jobs, investments and innovations.

This, in effect, creates a new avenue for security agencies to carry out surveillance and interception activities under the Bangladesh Telecommunication Regulation Act, 2001, citing the vague and variably interpretable "national security" and "public order" grounds.

Furthermore, as the draft also confers exemptions and indemnifications to the government agencies, this removes the element of accountability and transparency from the law enforcement process and that has the potential to undermine rights of citizens (particularly critics, dissidents and opposition) in a way similar to how the Digital Security Act, 2018 and the Information and Communication Technology Act, 2006 have been used.

Additionally, the establishment of the data protection office under the direct control and administration of the Digital Security Agency also points to the failure of the government to separate data protection objectives from digital security concerns.

Finally, the potentially global application of the law is unreasonable and disproportionate and is fated to result in its poor enforcement. On the whole, the overall structure of draft legislation appears to undermine the spirit of the law to codify citizens' right to privacy and seemingly strengthens regulatory and supervisory authority of the government over citizens and businesses.

More often than not, discussions about privacy start with collateral considerations. Let's look at the thorny issue of data localisation: it is premised on the apprehension that a nation's sovereignty is threatened by the government's inability to control its citizens' data stored outside the country (in addition to national security, law enforcement and intelligence gathering considerations).

Ultimately, these considerations result in negative impacts on human rights and further dilution of privacy, especially in weaker democracies. Resultantly, data territorialization contributes to increased internet fragmentation, endangers global interconnectedness, and weakend security of individual privacy.

As the Russian experience shows, similar localisation requirements were heavily criticised by businesses and several technology companies still do not comply with the requirements since the law was enacted in 2015.

A few advocates of data nationalism have made fallacious economic and commercial arguments in favour of data localisation: more data centres would mean increased economic growth and more high-tech jobs, investments and innovations.

However, evidence suggests that while data centres will create some short-term construction jobs, but once it is operationalised, much of the activities will be automated and only a limited number of employees (some of whom may be expatriates) will be employed.

Moreover, evidence also shows data localisation increases the cost of doing business and limits the availability of technology-based products and services.

As a result, in recognition of these arguments, a declaration was reportedly signed at the digital and tech ministerial meeting ahead of the 2021 G7 Leaders' Summit, with a commitment to preserve "an open, interoperable, reliable and secure internet, one that is unfragmented, supports freedom, innovation and trust which empowers people."

It is worth noting that, where the law is so egregious that it cannot be complied with, offshore service providers can simply pull the plug on its services. In Hong Kong, the big tech companies reportedly warned the government that they would cease offering their services in the country if the authorities amended the data protection laws that could make service providers directly liable for content shared by users.

Any discussion on privacy should start with privacy considerations, and have privacy considerations as its main component.

Despite its far-reaching implications, policymakers at home and abroad are not having enough in-depth, nuanced and meaningful conversations to counteract and mitigate the effects of privacy dilution.

Any discussion on privacy should start with privacy considerations, and have privacy considerations as its main component, pristine and unencumbered by peripheral considerations, lest it is trivialised and brushed aside.

Other relevant issues should be given due consideration, but primacy to privacy is paramount to an effective conversation. Otherwise, the discussions will become, in the words of Greta Thunberg, all "blah blah blah ..."