BANGLADESH'S NEW DATA PROTECTION ACT: BRITTLE SHIELD OR BLUNT SWORD?

BARRISTER SHAHZEB MAHMOOD

The Government of Bangladesh is drafting a data protection and localisation law ("draft data protection act, DPA" or "the law"), which, once enacted, will be the first of its kind data privacy law in Bangladesh.

Broadly, the draft DPA sets out the rights and obligations of data subjects, data controllers and data processors, with provisions on notice-and-consent requirements, collection methods, recordkeeping, data correction and erasure, data breach notifications, and data audits. The law also envisions the establishment of a new regulator, requires the appointment of a data protection officer, and mandates data localisation.

As the preamble of the draft DPA recapitulates, the law is intended to safeguard "personal data as to life, property, freedom of thought, expression, conscience, with special regard to their right to privacy, secrecy, personal identity." This is underscored by several constitutional rights, including the freedoms of thought, conscience, speech and expression, and privacy of correspondence and communication. Besides, the law is also heavily influenced by the global developments in privacy jurisprudence, which in turn is being moulded by the constantly evolving technologies and the exponential growth in data generation and online activity all over the world. It is therefore essential that the law is rooted in time-tested constitutional principles whilst structured to be future-proof.

As Bangladesh flits towards the first cross-sectoral data protection legal framework, it is crucial that we, as responsible citizens, understand and objectively scrutinise how the draft DPA balances the imperatives of safeguarding individual privacy against commercial interests and political agenda. Why? Because not only will the law affect individual rights, it will also invariably impact businesses and establishments both in and outside Bangladesh.

Set out below are key concerns around the draft DPA, based on a review of a draft of the law that was publicly available on the website of the Digital Security Agency on June 1, 2021.

Application too broad

As currently worded, the draft DPA will apply domestically and extraterritorially to all companies or individuals who collect or process data from within Bangladesh or relating to its citizens or any services from within or outside the country. The language suggests that the law will have a worldwide application, irrespective of the location of the data controller or its nexus with the data subjects; accordingly, the law seemingly applies to German retailers in business with Bangladeshi suppliers and small brick-and-mortar in Sajek in the same manner it will apply to technology, financial, healthcare or e-commerce service providers that are collecting large datasets using sophisticated machine-learning algorithms and automated tools.

Such wholesale global application of the law is unreasonable and disproportionate, especially considering that the law stipulates burdensome requirements. For instance, the law obligates all data controllers to appoint a data protection officer and conduct annual audits, irrespective of its location, size of operations or volume of data being processed; this is onerous and expensive and could therefore compel non-resident service providers to pre-emptively restrict access to its services in Bangladesh. This is not unprecedented: three of the Big Four companies, i.e., Apple, Facebook and Google, have recently expressed intention to stop offering services in Hong Kong if the authorities amend the existing data protection law that could hold companies liable for the users' actions.

Secondly, the draft DPA appears to apply to all businesses irrespective of their size or turnover. Bangladesh currently has a minimal number of diversified conglomerates. According to one statistic, 79,00,000 establishments (or around 98 percent of all businesses) in Bangladesh are small and medium-sized enterprises (SMEs), of which 93.6 percent are small and 6.4 percent are medium. Therefore, the overwhelming majority of businesses to be affected by the law will be small entities, which suffer from common constraints like access to capital and technological capabilities.

So, how can the policymakers address these issues? The application of the law should be subject to a two-tiered financial threshold and nexus tests. If an enterprise satisfies both limbs of the test, i.e., it has sufficient financial resources and business interest connected to Bangladesh, then, and only then, it should be subject to the law. In order to ascertain the financial threshold, the government can refer to its policies, like the Small and Medium Enterprise Credit Policies & Programmes or Bangladesh Industrial Policy 2016.

Security risks of locally stored data

The draft DPA contains data mirroring provision, which requires every data controller to store "at least one serving copy of data" in servers or data centres located in Bangladesh. Additionally, user data can be transferred outside the country if the statutory conditions are satisfied. The advocates of data localisation advance three main arguments in its favour, namely, national data sovereignty, law enforcement, and economic benefits for local industries. However, these considerations reflect the entrenched and outmoded mindsets of the policymakers not only in Bangladesh but also in most jurisdictions.

Most significantly, the requirement to store user data locally creates a new avenue for the security agencies (who are exempted from this law) to surveil and intercept data, which clearly contradicts the purported protectionist architecture of the law. Section 97Ka of the Bangladesh Telecommunication Regulation Act, 2001, confers sweeping authority to the government to authorise any national security, intelligence or law enforcement agency to "intercept, record or collect information" of any person on national security or public order grounds. Additionally, under the licenses and various policies and guidelines issued by the Bangladesh Telecommunication Regulatory Commission (BTRC), a licensee must establish monitoring and interception facilities and provide connections to the state agencies to conduct surveillance. Such expansive and intrusive mandate threatens individuals' freedom to express themselves and their right to privacy of communications, which are two sides of the same coin, each an essential prerequisite to the enjoyment of the other. This was recognised by the High Court Division of the Supreme Court of Bangladesh in "The State vs. Oli" [2019], wherein the court observed that the culture of "leaking" personal conversations and videos on social media, and the routine collection of call details and audio records from telecoms by state agencies, without warrant or knowledge of the customers, are a breach of fundamental rights guaranteed under Article 43 of the Constitution.

Additionally, it is worth calling out the fallacies in the assumption that data mirroring will necessarily lead to better privacy, as data security is determined more by technical measures and cybersecurity protocols than by its location. In fact, the concentration of data in servers with poor security would make it susceptible to unauthorised access by malicious actors. As recently as June 2021, over 92 percent of LinkedIn user data was scraped by hackers and put up for sale on the dark web due to insufficient technical safeguards. Furthermore, this may also deter foreign investments, as potential investors may see this measure as an increase in the cost of doing business in Bangladesh or as less incentive to enter the markets altogether.

Accordingly, the best course of action would be for the government to adopt a system that allows data transfer to other countries under certain conditions (e.g., transfer to white-listed countries or countries that maintain the same level of protection as Bangladesh), without any data mirroring requirement. However, if the provisions are to be retained, the law should incorporate proportionality and necessity tests to ensure that it does not become a tool for enabling uncontrolled state surveillance. Additionally, the government should create a stronger, legally binding framework with a clear penalty and compensation regime to ensure that data security is not compromised due to suboptimal capabilities.

Consent-and-notice regime inadequate

A cornerstone of the proposed data protection framework is the notice-and-consent regime. Like most jurisdictions, the draft DPA mandates that a data controller must obtain free, specific and clear consent from the data subject as a prerequisite to collecting and processing data. Consent, once given, must be capable of being withdrawn.

The notice-and-consent regime is based on the assumption that consent is the best mechanism for data protection and that it will result in better accountability on the part of the data controller and give better control to the users. However, while the accountability and autonomy arguments are facially compelling, in reality, the consent-based mechanism provides inadequate protection to the citizens. This is primarily because consent is usually obtained through long, legalistic and complex notices and agreements that cannot be negotiated, that are seldom read and even more rarely understood. Moreover, when a language barrier is added to the mix, arguably, consent is not being given on an informed basis. In fact, failure to give consent to the standard terms would mean that the users cannot access most online services. Whilst some might argue that individuals are free to not use such services, in reality, as online connectivity is increasingly becoming an integral part of modern life, the option to withdraw oneself from internet-based services completely is hardly a genuine choice. As a result, consent is swiftly given without a second thought. According to a 2017 Deloitte survey, around 97 percent of those surveyed aged between 18 and 34 accepted the terms and conditions without reading them. In another experiment by two academics from York University and the University of Connecticut a few years ago, 98 percent of participants surveyed agreed to terms that contained disclosures that the users will have to give up their first-born child as payment.

Furthermore, the current ecosystem runs contrary to the data minimisation principles. The value of data resides not in its primary purpose but in its incalculable secondary purposes. Therefore, as data are constantly being transformed and reconstructed into complex datasets to meet endless secondary purposes, and as these secondary purposes are innately unforeseeable, consents can become redundant very quickly.

Practically, the notice-and-consent regime in the draft DPA is not ideal and is clearly at odds with the evolving nature of the digital economy: consent, in one elegant stroke, would allow unfettered and perpetual access and retention rights to most data controllers. Unfortunately, there is no viable alternative. Therefore, it is imperative that stronger emphasis be made on preventing abuse, with clearer articulation around limiting the use of data for secondary purposes, fairness of processing, and allowing opt-out options without discontinuation of services.

Data Protection Office not independent

A data protection office (DPO), which will serve as the nodal authority for data protection matters and be responsible for the overall implementation of the law, is proposed to be established under the direct control and administration of the Digital Security Agency. This statutory agency will broadly have advisory, investigative, corrective, enforcement and law-making powers.

The agency will maintain a publicly accessible data protection register containing information on all the data controllers and processors and the reason for collecting and processing the data. Paradoxically, very clearly, these mandates oversupply government intervention – the register, the purpose of which is still unclear, should be subject to a high standard of confidentiality.

Furthermore, the draft DPA intends to create a regulatory structure that is not sufficiently independent. It is paramount that the DPO is independent of the Digital Security Agency, as data protection encompasses more than just digital security. Reviewing data protection values from the lens of digital security can result in overly conservative policies that stifle innovation and development. Therefore, an independent body would be better equipped to intermediate between the priorities between digital security and data privacy. In fact, the DPO should consist of both government representatives and independent members with requisite expertise and experience in data protection, telecommunication, consumer rights, finance and digital security.

Other issues

Generally, a law comes into effect immediately when the government publishes it in the official gazette. As currently worded, it is unclear as to when the law will become effective. However, it is imperative that implementation of the law is deferred by at least a three-year period to allow businesses to have a clear understanding of the legal requirements, introduce or upgrade its infrastructures, facilities, and internal policies, without technically being in violation. This "cooling-off" period is equally important for the state agencies, which need time to modernise their system to ensure compliance and avoid a system regulatory capture.

The draft DPA proposes fine and/or imprisonment for non-compliance and the offences are cognisable (i.e., an arrest can be made without a warrant) and non-bailable. It also purports to hold companies as well as their directors, employees, officers and agents liable. Such punitive sanctions are disproportionate, would likely deter foreign investment, and may prompt non-residents to block access to its services in the country as a precautionary measure. A tiered approach to sanctions should be adopted, with warnings and show cause notices to be issued in the first instance, followed by administrative fines limited to systemic non-compliance and compensation in circumstances of provable breach leading to quantifiable damages. Any personal liability should be removed in its entirety, and the offences under the law should be non-cognisable and bailable.

Sections 26 and 33 of the Digital Security Act, 2018 makes the unauthorised collection, use, transmission or preservation of identity information or other data a criminal offence punishable with stringent imprisonment and fine. While the "conflict of laws" provision in the draft DPA states that it will take precedence over any inconsistent law, it does not completely extinguish the right to initiate proceedings under the 2018 Act, making it possible for a highly spirited litigant to file cases under both laws. Therefore, to prevent abuse, the law should repeal the aforementioned provisions of the 2018 Act.

The European Union (EU)'s General Data Protection Regulation took about four years of preparation and debate before it was finally approved in 2016. India started drafting its own version of the data protection law in 2017, which has undergone a substantial consultation process and is still being debated. Bangladesh government too should take time to craft this complex new legal framework, bearing in mind that the effectiveness of the law is not dependent simply on its introduction but also on capacity and infrastructure, financial liquidity, security measures, and the ability of resident and non-resident companies to calibrate its existing system to meet the requirements. While the overall structure of the draft DPA is a good start, the legislation would benefit from multi-stakeholder consultation and review. It is noted that the drafters "are going through laws and legal frameworks as enacted by [other jurisdictions] or being adhered to in other jurisdictions" in preparing this draft, but it is vital that the law does not become an outcome of a simple cut-and-paste exercise. It is also essential to understand the economic fallout of implementing the law. Once finalised, the draft DPA should be made available for public opinion in accordance with the rules of parliamentary procedure.

Shahzeb Mahmood is a Research Associate at the Centre for Governance Studies and an Associate at Syed Ishtiaq Ahmed & Associates, a full-service law firm. He can be reached at mahmood.shahzeb@gmail.com