With a new data protection act on the way, time for a reality check

There is a thin line between protection and control

MD SAIMUM REZA TALUKDER

THE internet has been developed as a transborder, decentralised and virtual space which everyone can access, irrespective of their nationality, race, creed or culture. Since its public launch in the 1990s, the internet has been intentionally kept outside the control of national jurisdiction. It is a borderless abstract space that is controlled and regulated mostly by private groups and entities—e.g. the Internet Corporation for Assigned Names and Numbers (ICANN), the Internet Engineering Task Force (IETF), the Internet Research Task Force (IRTF), regional internet registries (RIRs), etc.

But for quite some time, the world has been polarised regarding the characteristics of the internet. One group, e.g. the North American and European countries, want the internet to remain borderless and free from national jurisdiction. The other group—i.e. China, Russia, North Korea, Iran, Turkey, Brazil—wants to make it a subject of national jurisdiction and want to exercise "sovereignty" in cyberspace. In fact, there is a critique that authoritarian regimes and states with fragile democracy tend to regulate the use of internet by exercising "state sovereignty." So the regulation and control of the internet should be a cause for concern for any freedom-loving, rights-respecting individual.

There has been a lot of discussion on the implications of authoritarian and restrictive policies and laws targeting the internet. Draconian laws related to the cyberspace have met with strong protest and resistance all around the world. But very little has been done to criticise and protest the architectural control over the internet. Lawrence Lessig, professor of law and leadership at Harvard Law School, developed his theory "Code is Law" in 2006, where he warned that by controlling the architecture (code) of the internet, we can regulate the market, norms and the law of society. NSA whistleblower Edward Snowden has revealed how pervasive the mass surveillance conducted by the US and UK—in the name of protecting the so-called national interests and fighting terrorism worldwide—is. According to Statista, the global surveillance industry was a market worth USD 45.5 billion in 2020, which will rise to USD 74.6 billion by 2025.

When the internet itself is an abstract space without any border, such notion of data localisation confines cyberspace according to geographical boundaries. The question is, are we ready to accept concepts like Russian cyberspace or American cyberspace?

Among several architectural controls, "data localisation" is a technique that allows states to impose and exercise "sovereignty" in borderless and neutral cyberspace. It simply means data collected from citizens of a state has to be stored in physical devices located within the state territories. When the internet itself is a distributed abstract space without any border, such notion of data localisation confines cyberspace according to geographical boundaries. The question is, are we ready to accept concepts like Russian cyberspace or American cyberspace?

We have to be very cautious about ideas like data localisation. Russia controls its version of the internet (RuNet) by data localisation. Yarovaya Law, introduced in 2016, allows the Russian authorities to localise the content data from the internet, which is being criticised as a digital lock on free speech online. Recently, a Moscow court fined Google over USD 40,000 for refusing to localise users' data in Russia.

Concerns over data protection in Bangladesh

Recently, the *Daily Samakal* reported the Bangladesh government was drafting a personal data protection act (PDPA). According to a report by *The Daily Star*, the government is considering data localisation to protect personal data through the new law.

Will the new data protection law ensure that the citizens have autonomy over their personal information?

ILLUSTRATION: **BIPLOB CHAKROBORTY**

The news reports mentioned the government's concern about having more control on social media companies and storing the citizens' data in physical devices located in the country. Bangladesh is proposing such a law when the Digital Security Act (DSA) is still in effect. According to reports by Amnesty International, 433 Bangladeshis have been imprisoned under the DSA and nearly 1,000 have been arrested since the law was enacted in 2018. So, when the government proposes a new law like the PDPA, a reasonable suspicion also arises: Will this law protect personal data or curb the freedom and autonomy over our personal information?

The core objective of a data protection law is to protect the privacy of personal and sensitive data, so that people can safely communicate in cyberspace. Facilitation of e-commerce or digital commerce is also another prime focus of any data protection law. Though necessary, criminalisation and penalisation are not the main concern of such legislations. Theoretically, it does not differentiate between whether data is localised within a geographic boundary or distributed among several servers situated in different parts of the world. In fact, data localisation might be beneficial for certain sectors, e.g., ensuring data privacy of critical information infrastructures. However, the main concerns for citizens should be: What will be done with their personal data? How does the architectural control proposed by the data protection law affect citizens' rights?

Collection, protection of localised data

Data mining is collection of data from different sources through different means, and then storing it in a physical storage. According to the news reports mentioned previously, the proposed law requires personal data to be stored within the geographical location of Bangladesh. In the tech world, there is a saying: There are two types of computer systems in the world—systems that can be hacked, and systems that will be hacked again. That is why the confidentiality of critical information infrastructure (such as a data centre) is crucial. This is the key reason why tech giants like the FAANG—Facebook, Amazon, Apple, Netflix and Google—keep their data in distributed servers. As there are a few data centres in Bangladesh which can serve the purpose of the proposed law, are we risking our data centres to be identified and made targets by the hackers? If publicly known IT firms run those data centres, it is not difficult for cybercriminals to hack or disclose sensitive information about the data centres through malicious means. So, the information on data centre location, identity of its staff, operational methods, etc should be kept confidential. The Bangladesh Bank heist of USD 81 million is a good example to understand the importance of such confidentiality of a data centre facility.

Another matter of great concern is how data is collected. Our personal data is our property, so our consent must be taken before our personal data is collected. Due diligence has to be done when collecting data. I can recall the instance of biometric data collection for mobile SIM registration through agents of telecom operators across the country. Should we allow third parties (agents assigned by mobile phone operators) to collect biometric data because the government asked for it? Did it not expose our personal data to various interested groups?

I assume the PDPA will contain data protection principles that bans such practices of data collection.

We should also consider Section 43 of the DSA, which allows law enforcement agencies to confiscate all devices owned by a suspect—which may also contain personal information of the suspect's friends, family members and acquaintances—without a warrant. Will the PDPA exempt law enforcers from obeying its data protection principles and keep similar provisions as Section 43 of DSA? If so, then is it not a risk to the privacy of journalistic sources, human rights activists and cyber dissidents in Bangladesh?

I hope that the proposed PDPA will also provide detailed policy to secure personal data at three basic levels of the internet: a) Node level (individual computers, servers, and routers connected to the network); b) Network level (connection between the nodes); and c) Application level (software running and communicating between the nodes).

Who can access what data, and to what degree?

Another major issue of concern is access to the data. We cannot impose absolute ban on data collection and storage, in order to facilitate criminal investigation, judicial decision-making, running key administrative work of the government, collection of taxes and revenues, etc. But the data should not be fully accessible to everyone. For example, population census data should not be shared with all government institutions without specific requirements, or data of sensitive litigation matters should not be accessible to law enforcement agencies without court permission. If the government stores data within Bangladesh, the access level to that storage must be classified. What are the propositions of the PDPA in this regard?

Different government agencies (e.g. police, judiciary, ministries) need to process, analyse and disseminate personal data to do their jobs. In the era of Fourth Industrial Revolution, we see the use of artificial intelligence to process and analyse Big Data in order to identify risks or prospects, foreseeing opportunities, determining development priorities, etc. For example, health data has been collected through different online apps during the Covid-19 pandemic, which helped governments worldwide to contact-trace or map community transmissions. But such data usage must be regulated and transparent. It must not discriminate while identifying and targeting people, and there must be a mechanism for accountability if something goes wrong. Also, people should have a minimum level of autonomy over their personal data and should be able to decide what information is to be shared. Is such type of data usage policy maintained in Bangladesh?

According to a report published by Banglanews24.com last year, the Implementation Monitoring and Evaluation Division (IMED) under the Ministry of Planning identified 11 risks and 29 weaknesses in the National Board of Revenue's (NBR) "Strengthening Governance Management Project." The report also mentions an allegation that the Vietnamese IT company, which was given the job of developing the NBR database, had access to that database containing confidential information of Bangladeshi taxpayers. If such an allegation is proven true, does the PDPA propose provisions of right to be forgotten, data portability with safety precautions, restricting automated processing of data, data rectification, right to access, right to be informed about a data breach, etc to deal with future incidents?

There needs to be a data controller for the prompt response to such risks. If the PDPA proposes a data controller, how will they be appointed, and what will be the accountability mechanism for them? Will there be judicial monitoring over the data controller to maintain checks and balances?

Another matter of great concern is how data is collected. Our personal data is our property, so our consent must be taken before our personal data is collected. Due diligence has to be done when collecting data. I can recall the instance of biometric data collection for mobile SIM registration through agents of telecom operators across the country. Should we allow third parties to collect biometric data because the government asked for it? Did it not expose our personal data to various interested groups?

Compliance with international standards

Data protection compliance is a crucial issue for the global business community which is dealing with cross-border data. In the 2015 Maximillian Schrems vs Data Protection Commissioner case, the Court of Justice of the European Union struck down the Safe Harbour Agreement, a trans-Atlantic pact between the US and the EU countries, which was used by thousands of companies to transfer the Europeans' personal information to the US. The EU Court of Justice was not convinced that the US data protection policies were in compliance with the European standard of data protection. Is the Bangladesh government formulating the PDPA with data protection principles that are in compliance with the requirements of the EU, North America, Asean or Far East countries? If not, then our private companies—mainly those providing information society services—will be facing hassles, which would not bode well for digital Bangladesh.

As we exist both online and offline, anything that happens online has consequences offline and vice versa. Perhaps that is the reason why the UN Human Rights Council, in its 2018 report on human rights on the internet, affirms that the same rights that people have offline must also be protected online. Although we need a law like the PDPA, we must also ensure that any such measures for the internet must comply with the fundamental rights of people stated in the international human rights instruments as well as Bangladesh Constitution.

Md Saimum Reza Talukder teaches cyber law at Brac University and is member of the Artificial Intelligence Working Group by the Hannah Arendt Humanities Network.

QUOTABLE *Quote*

ALBERTINA SISULU
(1918 – 2011)
South African anti-apartheid activist

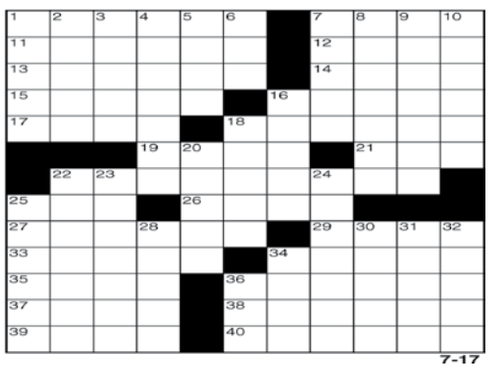
We are each required to walk our own road and then stop, assess what we have learnt, and share it with others. It is only in this way that the next generation can learn from those who have walked before them.

CROSSWORD BY THOMAS JOSEPH

ACROSS
1 Not dressy
7 Fight memento
11 Immediately
12 Account
13 Third-largest island
14 Leaf carriers
15 Pays to play
16 Wine grape
17 Tragic king
18 Gloomy
19 Turn suddenly
21 Stripling
22 Hit film of 1999
25 Alphabet end
26 "Frozen" queen
27 Goofs
29 Auction bids
33 Adrien with an Oscar
34 Eye colour
35 Foray
36 Couch potato's need
37 Skin woe
38 Freed of wrinkles
39 Oracle
40 Creators

DOWN
1 Plotting group
2 Be penitent
3 In a way, informally
4 Rattle
5 Best pair
6 Summer sign
7 Flight part
8 Cheese-filled pastry
9 Charlie Parker played it
10 Took a breather
16 Docking spots
18 Café offerings
20 Abrasive powder
22 Patio's kin
23 Jane Eyre, for one
24 Went wild
25 Horses' kin
28 More unusual
30 UV stopper
31 Hamper
32 Snow gliders
34 Vengeful goddess
36 Brink

WRITE FOR US. SEND US YOUR OPINION PIECES TO **dsopinion@gmail.com.**



YESTERDAY'S **ANSWERS**

R	I	S	E	N	■	T	A	B	L	E
U	N	C	L	E	■	O	C	E	A	N
S	T	A	K	E	■	Y	E	A	S	T
S	O	N	■	D	E	E	■	C	S	I
E	N	D	■	L	A	D	■	H	I	T
T	E	A	S	E	R	■	O	B	E	Y
■	■	L	U	S	T	F	U	L	■	■
E	L	S	E	■	H	O	R	A	C	E
R	A	H	■	B	E	L	■	N	R	A
A	T	E	■	E	N	L	■	K	I	T
S	I	E	G	E	■	O	B	E	S	E
E	N	T	E	R	■	W	A	T	E	R
R	O	S	E	S	■	S	A	S	S	Y

BEETLE BAILEY BY MORT WALKER

BABY BLUES BY KIRKMAN & SCOTT