HUMAN RIGHTS

Private university student Sumon (not his real name) had already gone to bed when the police came to his bachelor pad, last month. The cops were on a "block raid"—a security exercise that Dhaka Metropolitan Police executed over several areas in the city in the aftermath of the Safe Roads movement waged by student protestors.

"They came into my room, woke me up and told me to fire up my laptop and give them my phone," describes Sumon. The cops then proceeded to look through his Facebook and checked his WhatsApp messages, claims the student. "They found a text message forwarded to me by a neighbor saying that the police are doing a block raid, so I should be alert and speak to them politely."

The policeman checking his phone got alarmed by the text message. "Who tipped you off about the block raid? Was it someone from the opposition party?" Sumon claims the police said, before calling the higher official supervising the raid. Along with five of his other flatmates, he was then rounded up and taken to the local police station for further questioning. It was only in the early hours of the morning that Sumon's brother managed to make phone calls and get Sumon released.

The relevant police station was asked to confirm that Sumon was indeed picked up from his house, but they claimed that nobody was arrested on the night of the block raid, so *Star Weekend* is refraining from naming them. Technically it is true—Sumon was never booked in as arrested—he was only "brought to the police station" for a few hours, which is equivalent to detention.

But this does not change the fact that Sumon was allegedly picked up for having received a text message that the entire city was getting. People all over Facebook were sharing statuses about cops knocking on doors, and police cars cordoning off areas. In fact, during the days block raids were happening in the areas around Dhanmondi and Bashundhara, *The Daily Star* and every other major news organisation too reported on what was going on.

Yet Sumon was allegedly interrogated on "how he got the information". The police arrested 97 "agitators" this past month on charges of "spreading misinformation and rumors on social media" under Section 57 of ICT Act, but that's hardly a new story. Since the amendment of the law in 2013—eliminating the need for arrest warrants and official permission to prosecute—and April 2018, the police submitted 1,271 charge sheets under Section 57, many of which had multiple accused[1]. Special public prosecutor of Cyber Tribunal, Nazrul Islam Shamim told *Dhaka Tribune* last year that the majority of the cases filed under Section 57 cannot be proven in court. "Some cases are fabricated and filed to harass people," he added. "Most of these cases are settled out of court."

And while the government will be scrapping Section 57, as declared by Posts, Telecommunications and IT Minister Mustafa Jabbar last week, it will be replaced with more problematic sections curtailing freedom of speech. In the new draft Digital Security Act, Section 30 is basically a reworded Section 57, and sets prison terms for vague offenses like publishing "aggressive or frightening" information. The law would also impose sentences of up to 10 years in prison for posting information which "ruins communal harmony or creates instability or disorder or disturbs or is about to disturb the law and order situation."

The criticism of laws restricting freedom of speech barely scratches the surface of a wider, more important discussion on digital rights and privacy of the ordinary citizen. Digital rights describe human rights that allow individuals to access, use, create and publish digital media or to access electronic devices and communication networks. Unassumingly European-sounding in its definition, digital rights were initially established through the Association of Progressive Communications (APC) Internet Rights Charter in Prague in 2001, and later adopted under the Universal Declaration of Human Rights by the United Nations. In response, several countries today recognise the right to Internet access—related to existing rights to privacy and freedom of expression—by law.

Arguably, in Bangladesh, where 24.3 percent of the population live in poverty, digital rights seem like a lofty, elitist goal. Digitising the country has been central in the current government's political manifesto since 2008, yet comes with little discussion on the rights associated with access to digital tools. The Bangladesh Telecommunication Regulatory Commission report that 152 million Bangladeshis today have a mobile phone subscription, creating a tremendous market for digital economy. However, discrepancies between administrative and international statistics of Internet users, paint an incomplete picture of Internet prevalence.

Effective enactment of digital rights in Bangladesh nevertheless comes with stipulations. The ordinary individual should have the freedom to choose what digital tools they access and when, what they consume on it, and what they communicate through it without being exploited by the government or private corporations. Low-cost, readily available Internet does not give a free pass to the provider to limit people's access to information available on it, nor to collect data on the users, as was the case with Facebook Basics initially. The right to access comes with the right to know how to effectively use the tool (digital literacy), the right to choose what information to consume through it (informed consent), the right to protect the information shared through it (freedom of expression) and the right to own and protect personal data collected through it (privacy controls). The government's current digital policies do not provide clarity on the rights of the people enabling the state to control information, provide no legal safeguards on privacy, and prosecute those sharing "misinformation".

To be fair, the government's nervousness towards the rampant adoption of digital tools and services is not completely unwarranted. Majority of platforms and services used by the public are headquartered in North America, Europe, or East Asia—meaning, the private corporations behind them are accountable to foreign regulations. This substantially decreases a local government or law enforcement's ability to control and react to their changing policies or the data they collect. Between July and December last year, for example, the government of Bangladesh alone sent 60 unique requests to Facebook to release data on users, of which just less than 50 percent resulted in some very limited data release.

Unable to control the platform, frustrated politicians and policymakers often come down harder on the users—severely surveilling and scrutinising their activities. Despite 141 million Bangladeshis still being offline, much of the state's recent investments have haphazardly honed on increased government surveillance. The most recent procurement tenders issued by Rapid Action Battalion (RAB) showed that they were seeking Wifi Interceptors and Tactical Detection Units to track mobile phones for long periods of time. While it is unclear whether these devices have been imported, the tenders have been closed. Last month, the DMP also advertised an intent to purchase a backpack-mounted IMSI monitor i.e. a tool that can be used to gather data from a large number of mobile phones located within a certain area. Security websites claim that this device is for use in public places, including but not limited to, public demonstrations and protests. RAB, seemingly is ahead of the game—their website has procurement notices for IMSI monitors dating back to 2015.

There is obvious tension in the administration between digital access and information control as a method of ensuring national security. The nature of information that the government routinely asks Google to remove from the internet, has changed. According to the Google transparency reports that log government requests made to the organisation, previously the state used to ask them to remove content that hurt religious sentiment, while in the recent periods, they have been requesting the internet giant to take down things that jeopardise national security. This shift happened from June 2014.

On the flipside, platforms like Facebook are not above scrutiny. The ease of access and use coupled with unrestricted growth has transformed Facebook in recent years into a ripe ground for sharing false allegations and rumors to defame individuals, disproportionately affecting women and minority groups. Despite multiple allegations from human rights groups in the past on the use of Facebook to spread violence in the developing world, the platform *really* took notice when the same affected the US, thereby raising questions on its accountability to countries where it's used but does not have an office. How can governments and institutions protect digital rights of its people when the tools to implement such rights are from lands afar?

The issue of digital rights is both political and technical. On one hand, pro-public digital policies should give people the right to express and enforce net neutrality, while technology companies should give people the right to privacy and protection from unwarranted surveillance. Algorithms should not reinforce echo chambersand allow people to choose what they consume. The existing technocratic language for "poor countries" like Bangladeshis often limited to improved connectivity as a force for good, allowing people to communicate faster and avail services more cost-effectively. What it fails to take seriously is that ordinary people, many of whom are illiterate, also have certain digital rights such as privacy. The notion of privacy and consent is seldom sold to poor farmers or small business owners as possibilities—and better digital literacy is essential in ensuring people's digital rights.

The gaps between policy and reality are abundant. Much of these gaps can be explained by the government's inadequate capacity in designing pro-public digital rights legislation and infrastructure.

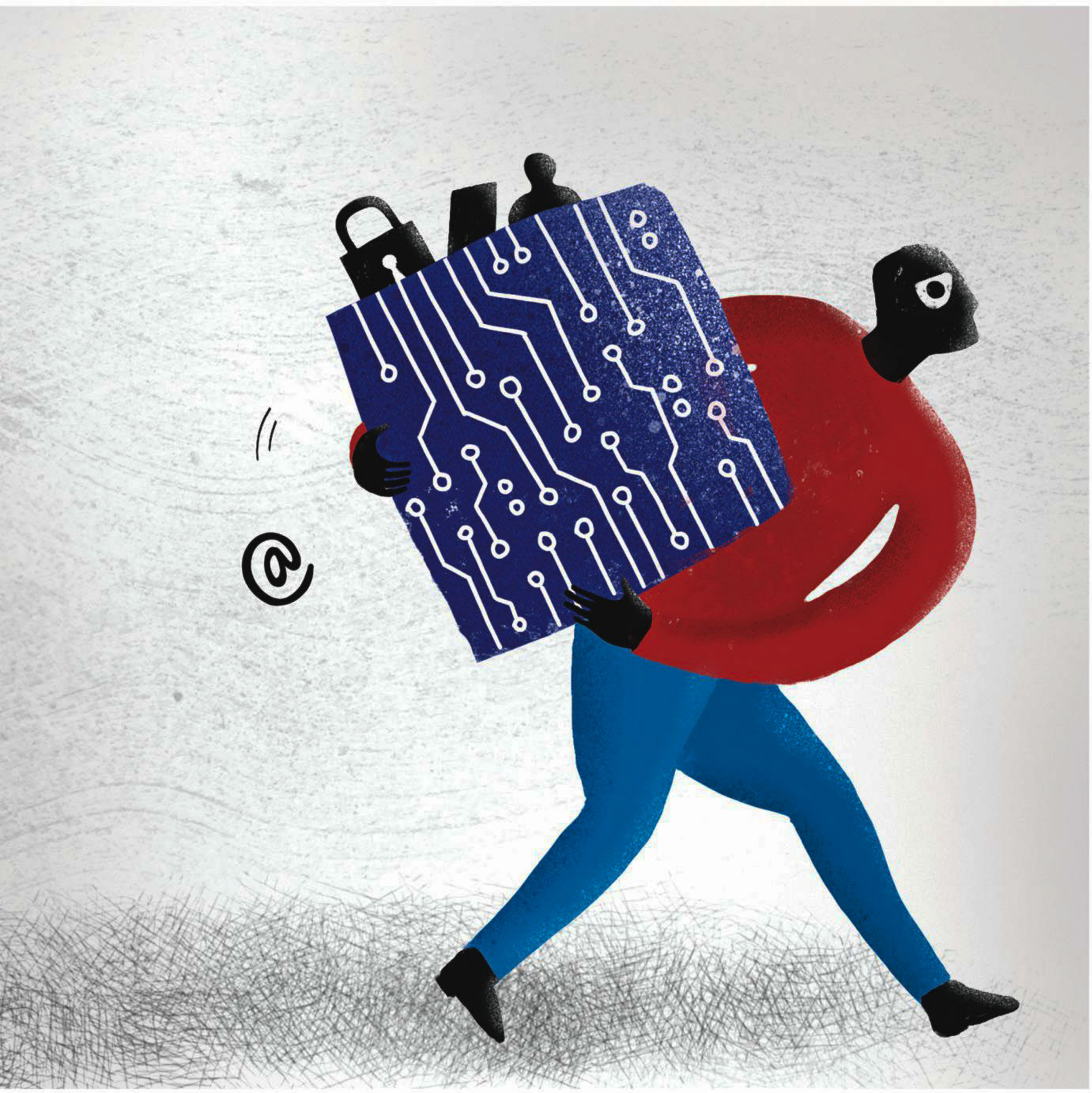

ILLUSTRATION: NOOR US SAFA ANIK

Additionally, a functioning digital economy needs flexible trade policies to encourage local companies to grow in Bangladesh. Local companies can provide people with much-needed context and control of their digital experience. Facilitating competition between foreign and local private corporations can provide the government with a market of checks and balances—and an ecosystem of pro-public, localised solutions.

The requirement of biometric identification itself raises privacy concerns in Bangladesh that lacks the legal safeguards against identity theft, and organisations found mishandling it cannot be legally prosecuted under existing local legislation. This poses additional danger to persecuted or vulnerable groups, unauthorised access to whose personally identifiable information can lead to increased violence. In a fitting twist, like a double-edged sword, the government has been using this same argument to deny digital access to Rohingya refugees in camps, enforcing strict information control protocols to "protect them" and "manage violence in the camps"[7]. Global statistics, contrarily, show refugee households spend one-third of their income on connectivity[8] and benefit from communicating with loved ones and cost-effective service delivery.

The gaps between policy and reality are abundant. Much of these gaps can be explained by the government's inadequate capacity in designing pro-public digital rights legislation and infrastructure. Assistant Inspector General in Police Headquarters, Soheli Ferdous, told Dhaka tribune that the police is not trained in handling cybercrimes. "Forensic facilities are more developed for investigating other crimes, but ICT crimes are a new thing." she said. "Labs take a lot of time to produce reports. Besides, there are shortcomings in preserving data and evidence." She further alluded much of the investigation is outsourced to IT experts, however there is a mismatch between how police and technologists approach cybercrimes. The inadequate capacity and understanding are more prominently felt among government ministers who are frequently caught making fleeting statements about the misuse of Internet—instead of addressing the problems at the core. A panel from the Ministry of Education, for example, advised Internet service providers and mobile network operators ahead of SSC exams this year to limit speed in efforts to prevent questions leakage but was proven ineffective when the questions were released ahead of shutdown schedule.

The subject of inadequate capacity in the public sector is a decade old problem for Bangladesh. Late May in 2006, the BNP government launched the first fiber-optic submarine cable in Cox's Bazar. The government, at the time, was heavily criticised for delaying the launch and depriving the country of high-speed connectivity because of fear of "information hacking" and "interference by foreign adversaries." The Bangladesh Telephone and Telegraph Board then refused to participate in an expansion scheme and failed to set up the domestic interface to leverage high-speed connectivity. The Awami League government's present stance on frequent Internet shutdowns and draconian policies to tackle "information leakage" and "interference in law and order" is eerily familiar with the events from over a decade ago. A progressive government, as political parties promise to be during election campaigns, should build its own capacity in taking advantage of the worldwide digital ecosystem, delivering pro-public digital rights policies that can facilitate checks and balances in the market. Anything short of it is not only a violation of human rights, but a state's personal failure to provide people with sufficient tools and protection to leverage global opportunities—and far behind the digital economy Bangladesh envisions to create.

The views expressed in this article are those of the author and do not reflect on the views of any organisation or institution s/he may or may not be affiliated with.

Zyma Islam contributed to this article