

The limitations of ICT and Cyber Security Acts

MEER AHSAN HABIB

THE Cyber Security Act is now open for virtual consultation on the ICT ministry's website. Little was known about this development until the law minister, at a seminar, revealed that the government was working on a befitting cyber security law. However, the ICT ministry neither transmitted any information about its availability nor invited any expert opinions. The move seemed to be an off-putting one to many, as they considered it a measure to further curb freedom of expression, especially on different social media platforms.

The present government has amended or enacted a few laws and policies on ICT. These are the Bangladesh Information Security Policy Guideline 2013, the much debated National Broadcasting Policy 2014 and the Information and Communication Technology (Amendment) Act 2013. The first ICT Act, enacted in 2006, awarded a maximum of 10 years imprisonment and fine of BDT 1 crore for crimes (Section 56 and 57) like hacking and displaying false and vulgar information online. It also gave ample power to the law enforcing agency to confiscate (Section 77-2) any related hardware including but not limited to computers, discs, network equipment etc, though it limits their authority to confiscate (Section 77-4) any such government property. Experts feared that this was done to provide indemnity to government agencies and individuals involved in internet, communication and computer network surveillance.

Interestingly, during the last couple of months, a few tele-conversations mainly of politicians surfaced. Though its sources are still unclear, it is an undeniable fact that without a well-equipped surveillance system such conversations cannot be tracked. Needless to mention, any such surveillance is a clear violation of the ICT Act. The Act also provides indemnity (Section 86) to public servants involved while implementing this Act, as any action against them will be punishable under this Act.

Section 18 and 18-1 of this Act regarding the appointment of controller, deputy controller and assistant controllers were amended in 2009. Maximum prison sentence was increased to 14 years from existing 10 years, after the Act was amended in 2013. Besides, offences under Section 54, 56, 57 and 61 were made cognisable and non-bailable.

Abundant scope of misuse by law enforcing agencies was also created after Section 80 was amended, as it empowered them to arrest anyone, anywhere without any warrant. Despite strong criticism from stakeholders, the government moved forward with these amendments in the name of ensuring transparency and accountability in the ICT sector.

Then came the National Broadcasting Policy 2014. The various clauses of the law (for example, 3.2.1, 3.2.2) mainly contains 'broadcasting don'ts', which are against constitutional rights of freedom of expression. This, too, faced backlash from the media, civil society and individuals as it appeared to be yet another regulating tool curbing the independence of broadcasting media in the

country. They advocated forming an independent commission which would work on the policy. In the face of strong criticism, the information ministry tried to calm down the situation by tabling the idea of the National Broadcasting Commission within the next six months that would work on a media friendly broadcasting policy. Looks like the government backtracked from its stance, as we are yet to see any visible step toward forming the commission.

The latest of this kind is the Cyber Security Act, which has no qualitative difference apart from further extending the definitions of cyber crimes, awarding more power to law enforcing agencies and extending imprisonment. Imprisonment for crimes done under Section 13 has been extended to the maximum sentence of 20 years in prison from 14 years. Crimes done under Sections 9, 10, 11, 12, 13, 14, 15 and 16 are now cognisable and non-bailable. Furthermore, the proposed Act has awarded law enforcing agencies to search any place, even arrest anyone if s/he believes a crime has been committed or planned.

According to available newspaper reports, in the last three years, 136 cases have been filed under the ICT Act. Verdicts of only 47 such cases were given. Many such cases have been filed under the ICT Act by law enforcing agencies or by party loyalists for defaming the prime minister or her family members. This scenario unveils two different dimensions - a) the misuse of the Act for undue favour and b) a possible gridlock in cyber crime related cases.

Recently, the Anti-Corruption Commission's website was hacked and the authority is yet to track down the wrongdoers involved. Till date, no one has been brought to book for hacking government websites. Under these circumstances, the draft Cyber Security Act stands defenceless. Do the Law and ICT ministries have any shield to defend their move? If yes, both should immediately table it for discussion, if not they should backtrack immediately and amend the ICT Act, as demanded by stakeholders, to guarantee freedom of expression.

In March this year, the Indian Supreme Court scrapped Section 66A of the Information Technology Act that empowered police to arrest people for Facebook and Twitter comments. The Supreme Court observed that it curbed people's right to express freely and it was in direct conflict with democratic values of India. "Section 66A is unconstitutional and we have no hesitation in striking it down. The public's right to know is directly affected by Section 66A," said Justice R F Nariman in court. Immediately after the verdict, #Sec66A started trending on social media. Let us wait a bit to see what happens in Bangladesh - the Honourable High Court in July 26, 2010 directed the then Ministry of Information Communication Technology, among others, to show cause as to why Sections 46 and 57 of the ICT Act 2006, allowing for the blocking of websites and electronic communications, and providing for prosecution of certain offences, should not be held to be ultra vires (beyond the authority) of the constitution.

The writer is a communication for development professional. He can be reached at ryadh_ju@yahoo.com