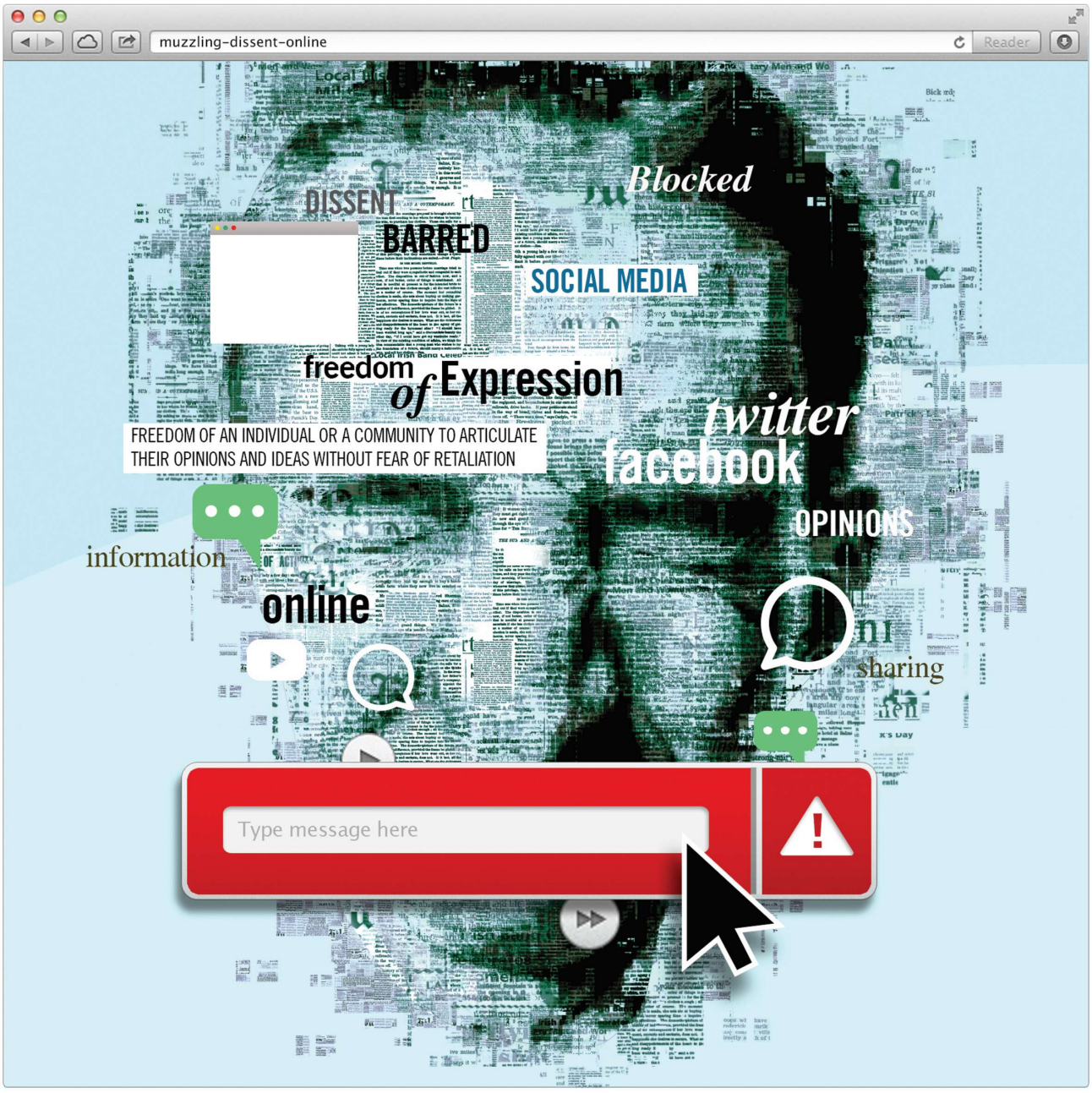

MUZZLING DISSENT ONLINE

BANGLADESH: AMEND THE DRACONIAN DIGITAL SECURITY ACT

AMNESTY INTERNATIONAL

MUZZLING DISSENT ONLINE

BACKGROUND

The Digital Security Act of Bangladesh ("the Act"), passed on 8 October 2018, is even more restrictive than the Information and Communication Technology ("ICT") Act[1] it replaces. The new Act is deeply problematic for three major reasons: ambiguous formulation of multiple sections that are vague that they may lead to criminalizing of legitimate expression of opinions or thoughts; broad powers granted to authorities which are not clearly defined; and provisions which allow for removal or blocking of content and the seizure/ search of devices without sufficient safeguards. A good example is section 21 of the Act, which criminalizes "propaganda or campaign" against "the spirit of liberation war", and "the father of the nation, national anthem and national flag"; terms which are so vague that they may be used to restrict free speech. Furthermore, extremely broad powers have been granted to the authorities to remove and block information on the strength of such vague and imprecise clauses. The authorities are empowered to not only investigate alleged offences, but also seize data and arrest people – in some cases, without a warrant.

Following Bangladesh's Universal Periodic Review (UPR) this year, the state party accepted recommendations to guarantee freedom of expression in the country, including specific recommendations to reverse the draconian provisions of the ICT Act.[2] These recommendations were made at the UPR Review in May 2018 and the outcome report was adopted at the recent Human Rights Council sessions in September 2018. Even as the government acknowledged flaws in the ICT Act, it persisted with its use.[3] In August 2018, for example, the prominent photographer Shahidul Alam was arrested under section 57 of the ICT Act for comments he made on Facebook and in an interview with Al Jazeera English. He currently languishes behind bars, having been denied bail.

Instead of breaking with the past, Bangladesh has now passed a law which is repressive, criminalizing freedom of expression, and potentially causing a chilling effect across Bangladeshi society. Under section 21 of the Act, an offender may face life imprisonment and/or a hefty fine of 30 million taka if they are found to have engaged in "propaganda" or a "campaign" against the "spirit of liberation war", the "father of the nation", the "national anthem" or "national flag" – a punishment far more severe than the punishment provided by the previous Act. The ICT act imposed a maximum punishment of up to 10 years' imprisonment and/or a fine of 10 million taka. The minimum wage in Bangladesh is 8,000 taka (USD 93.60) per month.[4]

Section 57 of the ICT Act was controversial for its vague, overbroad and coercive provisions. Offences included publishing or transmitting material deemed to be: "false or obscene"; which may "influence the reader" to become "dishonest or corrupt"; or "causes to deteriorate or creates possibility to deteriorate law and order"; "prejudice[s] the image of the state or person"; "causes to hurt or may hurt religious belief"; or "instigate[s] against any person or organisation".[5] These terms are not defined in the Act. Since the ICT Act was amended in 2013 – dispensing with legal protections to allow for arrests without warrant,[6] greater restrictions on bail and

---

[1] Act No. 39 of 2006

[2] For example, it accepted a recommendation from Latvia to "Bring legislation into conformity with the obligations under the International Covenant on Civil and Political Rights by repealing restrictive provisions that limit the rights of journalists, human rights defenders and civil society organizations to freedom of expression and free speech", Recommendation 147.7, and to "Guarantee Freedom of Expression" (France), Recommendation 147.70; Report of the Working Group on the Universal Periodic Review, Human Rights Council, 10-28 September 2018, A/HRC/39/12 available at https://documents-dds-ny.un.org/doc/UNDOC/GEN/G18/211/03/PDF/G1821103.pdf?OpenElement

[3] For example, in the National Report submitted at the Universal Periodic Review in 2018, the government stated that "With a view to establishing balance between freedom of expression and public morality & interest, the GoB has approved the Digital Security Bill, 2018 repealing the Information and Communication Technology Act, 2006". National report submitted in accordance with paragraph 5 of the annex to Human Rights Council resolution 16/21, Bangladesh, 26 February 2018, A/HRC/WG.6/30/BGD/1, Human Rights Council, available at https://documents-dds-ny.un.org/doc/UNDOC/GEN/G18/050/26/PDF/G1805026.pdf?OpenElement. See also comments made by Ministers on section 57 of the ICT Act: 29 November 2017 when Information Minister Hasanul Haq Inu spoke on the issue, https://bdnews24.com/bangladesh/2017/11/29/controversial-section-57-of-ict-act-will-go-information-minister-inu, and 16 September 2018 when Post, Telecommunications and IT Minister Mustafa Jabbar spoke on the issue https://www.thedailystar.net/country/news/section-57-go-passing-digital-security-bill-2018-minister-mustafa-jabbar-1634221

[4] Reuters, Nagaraj, A., "Pay more for your clothes, Bangladesh workers tell global fashion brands", 17 September 2018, https://www.reuters.com/article/us-bangladesh-labor-fashion/pay-more-for-your-clothes-bangladesh-workers-tell-global-fashion-brands-idUSKCN1LX23X. Channel NewsAsia, "Bangladesh unions reject $95 minimum wage for garment workers", 14 September 2018, https://www.channelnewsasia.com/news/asia/bangladesh-unions-reject-95-minimum-wage-for-garment-workers-10721812

[5] New Age, "Section 57 should not be incorporated in any new law: NHRC", 6 December 2017, http://www.newagebd.net/article/29855/section-57-should-not-be-incorporated-in-any-new-law-nhrc

[6] Under section 81 of the original ICT Act of 2006, before amendment, the powers of search, seizure and arrest were governed by the Code of Criminal Procedure of Bangladesh. However, by the amendment brought in 2013, section 57 was amended to increase the punishments and allow arrest without warrant, and the offences under that section were deemed non-bailable offences. See analysis in International Commission of Jurists (ICJ), "Briefing Paper on the amendments to the Bangladesh Information Communication Technology Act 2006", November 2013, https://www.icj.org/wp-content/uploads/2013/11/ICT-Brief-Final-Draft-20-November-2013.pdf

longer prison terms for those convicted under it – the police have used it to charge more than 1,200 people, most of them under section 57.[7]

Article 19 of the International Covenant on Civil and Political Rights (ICCPR) – to which Bangladesh is a state party – states that everyone has the right to freedom of expression, which includes the "freedom to seek, receive and impart information and ideas of all kinds, regardless of frontiers, either orally, in writing or in print, in the form of art, or through any other media of his choice".[8] The only grounds on which the right to freedom of expression may be restricted are set out in Article 19(3): "(a) For respect of the rights or reputations of others; (b) For the protection of national security or of public order (*ordre public*), or of public health or morals", and in order to be lawful, any such restrictions must be provided by law and meet the requirements of necessity and proportionality.[9] Article 20(2) further requires states to prohibit – but not necessarily criminalize – "advocacy of… hatred that constitutes incitement to discrimination, hostility or violence."

> **"…freedom to seek, receive and impart information and ideas of all kinds, regardless of frontiers, either orally, in writing or in print, in the form of art, or through any other media of his choice"**
>
> Article 19, ICCPR

The Act is repressive not only because of what it criminalizes, but also because it essentially suspends the operation of provisions in any other law which is incompatible with the Act.[10] This effectively overrides express provisions in other laws which protect human rights. The Act also applies extra-territorially, and therefore even if the individual charged or suspected of involvement in any of the crimes set out within the Act is outside of the territorial jurisdiction of Bangladesh, the provisions of the Act could still be used to take action against that person.[11]

Punishments where companies are involved will apply not only to the company itself as a "legal person entity", but will also be assumed to have a direct link to all levels of staff, from its manager or chief executive to its employees. The burden of proving their innocence or that they "tried his/her best to prevent the crime" falls on the person accused of the crime,[12] whereas in ordinary criminal law, the prosecution would ordinarily carry the burden of proving both act (*actus reus*) and the intention (*mens rea*). Shifting the burden on to the accused or defendant is contrary to accepted principles of criminal liability.

REMOVING AND BLOCKING DIGITAL DATA

The Act establishes an agency called the Digital Security Agency ("the Agency") which is empowered with a wide mandate in terms of various offences under the Act.[13] The Agency can request the removal or blocking of information and data if it believes that such information or data, "published or disseminated through digital media", *may* create a threat to digital security.[14] Not only is this provision vague, it also gives the power to the Agency to make blanket requests on the Bangladesh Telecommunication Regulatory Commission (BTRC) to remove and block information and data on nothing more than their own assessment of a situation. There appears to be no judicial oversight of such decisions, and there is no appeal process listed in the relevant section. Section 8(2) of the Act affords wide powers, this time to law enforcement agencies, to block data, if it appears to them that such information (a) violates the solidarity of the country or any part of the country; adversely affects (b) economic activity (c) security (d) defence (e) religious values or public order; or (f) infuse[s] racial prejudice and hatred. In such instances, law enforcement agencies may request the BTRC to block the dissemination or publication of that data or information, through the Director General of the Agency. Section 8 of the Act makes it mandatory for the BTRC to remove or block information when requested to do so by the Agency.[15]

These provisions are repressive on a number of levels.

No judicial review or appeal: The manner in which section 8(2) is drafted does not allow for a review of this objective criteria in order to impose restrictions on freedom of expression; in fact, a decision by a law enforcement agency, without any judicial oversight or opportunity to appeal the process, is sufficient to block websites or other digital means of sharing information and data.

---

[7] Dhaka Tribune, Rabbi, A.R., "Number of ICT cases on the rise again", 10 August 2018, https://www.dhakatribune.com/bangladesh/law-rights/2018/08/10/number-of-ict-cases-on-the-rise-again; Human Rights Watch, "No place for criticism: Bangladesh crackdown on social media commentary", 9 May 2018, https://www.hrw.org/report/2018/05/09/no-place-criticism/bangladesh-crackdown-social-media-commentary

[8] Article 19(2), ICCPR

[9] Article 19(3), ICCPR

[10] The only exception to this blanket provision appears to be the Right to Information Act of 2009 under which the right to information is protected.

[11] Section 4, Digital Security Act

[12] Section 36(1), Digital Security Act

[13] Section 5, Digital Security Act

[14] Section 8, Digital Security Act

[15] Section 8(3), Digital Security Act

Vague and undefined criteria: The problematic nature of the unchecked power to remove or block content is compounded by the vague and undefined aims for which the Act allows such removals or blocking. For a restriction on the right to free expression to be consistent with international human rights law, it must – *inter alia* – "be formulated with sufficient precision to enable an individual to regulate his or her conduct accordingly."[16] The lack of definition of terms such as "solidarity of the country", "economic activity", "security", or "religious values" in the Act leaves room for abuse. For example, it is conceivable that any legitimate protest against human rights violations could be deemed a violation of the solidarity of the country. Critique of national budget allocation priorities or economic policies could be deemed violation of economic activity of the country. Moreover, "infuse racial prejudice and hatred" is also vague, and thus may allow for blocking or removal of content that falls below the threshold for "advocacy of hatred" in the ICCPR, which protects even expression that is "deeply offensive".[17] The vagueness of these terms, with no definitions provided, coupled with the mandatory blocking of such data on request by the Agency, creates a serious concern for guarantee of the right to freedom of expression.

HURTING RELIGIOUS SENTIMENT OR HATRED AMONG COMMUNITIES

Section 28 criminalizes the publication or broadcast of "any information that hurts religious values or sentiments". The act must be carried out with the knowledge of or intention to hurt or provoke religious values or sentiments. As described previously, the right to freedom of expression extends to the right even to be deeply offensive.[18] Moreover, "the right to freedom of religion or belief, as enshrined in relevant international legal standards, does not include the right to have a religion or a belief that is free from criticism or ridicule,"[19] and "subjective feelings of offensiveness… should never guide legislative action, court decisions or other State activities."[20] The ICCPR requires the prohibition – but not necessarily the criminalization – of only the narrow category of expression that amounts to "advocacy of… hatred that constitutes incitement to discrimination, hostility or violence."[21] The crime set out in section 28 attracts a punishment of up to five years' imprisonment and/or a 10 million taka fine and, for repeat offences, up to 10 years' imprisonment and/or a 20 million taka fine.

Section 31, although termed "Deteriorating Law and Order", contains similar provisions criminalizing content that "creates hostility, hatred or prejudice among different classes or communities" or "destroys communal harmony or creates unrest or disorder or deteriorates law and order". It falls foul of human rights law governing advocacy of hatred for many of the same reasons that section 28 does. The lack of clear definitions could invite arbitrary applications and the punishments for this crime are also severe, with up to seven years' imprisonment and/or 500,000 taka fine and, for a repeat offence, up to 10 years' imprisonment and/or one million taka fine.

RESTRICTIONS ON ABILITY TO CHALLENGE HISTORICAL NARRATIVES

One of the most worrying aspects of the Act is section 21, which sets out as a crime the running of any "propaganda or campaign against the liberation war, the spirit of liberation war, father of the nation, national anthem or national flag". Anyone supporting such an act using digital media attracts the same punishment as those who carry out the act itself. The punishment for the crime is 10 years' imprisonment and/or 10 million taka fine and, for a repeat offence, it attracts life imprisonment and/or a 30 million taka fine.

The term "the spirit of liberation war" is defined as "all great ideals inspired our heroic people to dedicate and martyrs to self-sacrifice their lives for the national liberation struggle – those ideals of nationalism, socialism, democracy and secularism".[22]

SECTION 21 OF THE DIGITAL SECURITY ACT

"Punishment for any type of propaganda or campaign against the liberation war, the spirit of liberation war, father of the nation, national anthem or national flag. –

(1) If anyone runs any type of propaganda and campaign against the liberation war, the spirit of liberation war, father of the nation, national anthem or national flag, or supports such activities using digital media, then similar act of said person shall be a crime.

(2) If a person under the sub-section (1), commits an offense, then (s)he shall be punished with imprisonment for a term not exceeding 10 (ten) years, or with a fine not exceeding 1 (one) crore taka, or with both; and

(3) If a person commits the offense mentioned in sub-section (1) for the second time or repeat it, then (s)he shall be punished with life imprisonment, or with a fine not exceeding 3 (three) crores taka, or with both."

According to Article 19(1) of the ICCPR, all forms of expression are protected, be they political, religious, historic, scientific or moral. The Human Rights Committee has clearly stated that laws that penalize the expression of opinions about historical facts are

[16] UN Human Rights Committee, General Comment 34, para. 25
[17] UN Human Rights Committee, General Comment 34, para. 11
[18] Human Rights Committee, General Comment 34, para. 11, *European Court of Human Rights, Handyside v UK (1976), para. 49*
[19] The Rabat Plan of Action on the prohibition of advocacy of national, racial or religious hatred that constitutes incitement to discrimination, hostility or violence, A/HRC/22/17/Add.4, para. 19
[20] Report of the Special Rapporteur on freedom of religion or belief, A/HRC/31/18, para. 61
[21] ICCPR, Article 20(2)
[22] Section 2(u), Digital Security Act

incompatible with Article 19 of the ICCPR.[23] The Human Rights Committee has stated that "The Covenant does not permit general prohibition of expressions of an erroneous opinion or an incorrect interpretation of past events".[24]

The manner in which section 21 is drafted is clearly contrary to the state obligations of Bangladesh under the ICCPR, in that it generally prohibits and criminalizes what it terms "propaganda or campaign" on historical facts or political facts. The concept of the right to freedom of expression protects both the right to hold such opinion and to express an opinion on any of the grounds of political, religious, historic, scientific or moral opinion or belief. The only restriction can be in terms of Article 20 where prohibitions are permitted on grounds of incitement to hatred, and where such prohibition meets the triple criteria set out in Article 19(3), as mentioned above. Section 21 of the Act does not meet the exceptions set out in the ICCPR for such restrictions.

CRIMINALIZING VAGUE OFFENCE OF SENDING OR PUBLISHING "OFFENSIVE, FALSE OR INTIMIDATING" DATA

Section 25 of the Act is not just alarming because it contains vague and undefined terms that may be prone to abuse, but also because it affords special protection to the state and thus may be used to prohibit or punish legitimate political expression. The Act includes a crime of disseminating data, which it defines as "invasive", "intimidating", "being well-known lie", with the intention of "annoying, insulting or humiliating".[25] Even more troublingly, the next section reads:

> "Despite being known as propaganda or false, with the intention of tarnishing the image or reputation of the state, or spreading confusion, or for the purpose of doing so, express or disclose, or publish any information completely or partially, or promote or help to promote the same."[26]

The way the section is drafted could well allow the application of this crime to legitimate expression of either opinion or facts relating to all manner of political, scientific, historic, religious or moral issues. The crime attracts a punishment of up to three years' imprisonment and/or with a fine up to 300,000 taka.

The terms used in this section are not defined in section 2 or in any other part of the Act, and therefore what amounts to "tarnishing the image or reputation of the state" could include highlighting or reporting violations of international human rights standards by state agencies or even prohibit critique of non-state actors. Similarly, the terms "annoying, insulting, or humiliating" and "invasive or intimidating or being well-known lie", are all vague terms that are undefined. These terms may be used to include all manner of legitimate exercise of the right to freedom of expression and opinion.

INTRODUCING ENHANCED PUNISHMENTS FOR EXISTING CRIMES: DEFAMATION

Defamation is criminalized under this Act although defamation is already a criminal offence under section 499 of the Penal Code of Bangladesh.[27] The Act prescribes a punishment up to three years' imprisonment and/or 500,000 taka fine. A repeat offence would earn a sentence of up to five years' imprisonment and/or a fine of 1 million taka. It is unclear why defamation is specifically included in the Act when it is already a crime under the Penal Code of Bangladesh. The punishment in the Penal Code, however, is lower, with up to two years' imprisonment with or without a fine. To protect the right to freedom of expression, defamation should not be dealt with as a criminal offence but as a civil matter.

THE DEFINITION OF CYBER-TERRORISM

The manner in which the Act deals with what it terms "cyber-terrorism" arouses the same concerns highlighted above. It is a vague and imprecise offence which is likely to be subject to abuse. The definition of cyber-terrorism is in section 27 of the Act. Section 27(1)(a) says that if a person "restrains legitimate access or enters or help someone else to enter illegally to any computer or computer network or internet network" where the intention is to "end state integrity, security and sovereignty and creating fear among the public", it is deemed an act of cyber-terrorism, along with several other acts which are similarly deemed acts of terrorism.

[23] Human Rights Committee, General Comment 34, para. 49
[24] Human Rights Committee, General Comment 34, para. 49
[25] Section 25(1), Digital Security Act
[26] Section 25(b), Digital Security Act
[27] Penal Code, Act No. 45 of 1860

PUNISHMENT FOR THE OFFENCE OF CYBER-TERRORISM

A conviction for cyber-terrorism can lead to a punishment of up to 14 years imprisonment and/or a 10 million taka fine.

A repeat offence would be punished by a maximum sentence of life imprisonment and/or a 50 million taka fine.

The phrase "intention to… creating fear among the public" is vague and undefined, and may be used against those who legitimately exercise their right to freedom of expression. The section also ascribes the crime to any person who either "restrains legitimate access" or helps someone else illegally access *any* "computer or computer network or internet network".[28] The way this section is drafted may allow application of this section to non-criminal acts. For example, it may apply to someone who allows another person to access his/her password, since the *actus reus* of intention to "end state integrity, security and sovereignty" or even "creating fear among the public" is vague and undefined.

Therefore, the determination of what constitutes "cyber-terrorism" remains extremely vague and subject to abuse, especially given the heavy punishments ascribed to this crime. A conviction for cyber-terrorism can lead to a punishment of up to 14 years' imprisonment and/or a 10 million taka fine. A repeat offence would be punished by a maximum sentence of life imprisonment and/or a 50 million taka fine.

POWERS OF INVESTIGATION, SEARCH, SEIZURE AND ARREST

POWERS OF INVESTIGATION OF THE DIGITAL SECURITY AGENCY

The Agency's powers of investigation under the Act appears troubling given the vagueness of several of these provisions. In terms of section 15, the government can announce, through a Gazette notification, that a specific computer system, network or even information infrastructure is "Important Information Infrastructure". The Director General of the Agency has the role of monitoring and inspecting such infrastructure to ensure it is properly maintained. More problematically, the Agency also can initiate investigations into anyone whose activities they have "logical reason" to believe are threatening or harmful to such infrastructure.[29] This may be either based on a complaint to that effect, or on its own motion (*suo moto*).

Crimes that may be committed directly against such "Important Information Infrastructure" include illegal entry and harm to the infrastructure through such illegal access. The punishments for the crime are high, with seven years' imprisonment and/or up to 2.5 million taka fine for illegal entry, and 14 years' and/or a fine of up to 10 million taka for causing harm through such illegal entry or attempted entry. Repeat offenders attract a sentence of life imprisonment or a fine of up to 50 million taka.

The Agency's powers of investigation in relation to offences under this section are not clearly defined in section 16 and therefore such decisions to investigate based on a "logical reason", which is also undefined, is alarming. According to section 5, the "powers, responsibilities and functions of the Agency shall be determined by rules or provisions".[30]

POWERS OF INVESTIGATION OF INVESTIGATING OFFICERS

In terms of section 39, a police officer not below the rank of a sub-inspector shall be deemed an "investigating officer" and will investigate any crime committed under this law. The powers of the investigating officer include the confiscation of computers, computer programs, systems, networks, digital devices and any program or information data that is stored on a retrieval system on or in any other way.[31]

While it is unclear whether investigations initiated under section 16(3) will be carried out by the office of the Agency or by an investigating officer under section 41(2), it is clear that where an investigating officer undertakes the investigation, both hardware and software may be confiscated in the course of such investigations. Given that the decision to commence an investigation is on vague grounds, not subject to judicial overview, this creates a real danger of invasive investigations that may violate the right to privacy or other human rights.

[28] Section 27(1)(a), Digital Security Act
[29] Section 16(3), Digital Security Act
[30] Section 5(3), Digital Security Act
[31] Section 41(2), Digital Security Act

POWERS OF SEARCH, SEIZURE AND ARREST WITHOUT WARRANT

The Act authorizes any police officer to search premises, to seize computers and similar hardware, and to search the body of a person and to arrest a person present in that place – without a warrant. The only conditions to be fulfilled for such a search, seizure or arrest are that they: (a) believe that a crime under the Act has occurred, is occurring or is likely to occur; (b) evidence is likely to be lost, wasted, washed or altered or in another way making it rare; and (c) record the reasons for such belief.[32] Moreover, there is a lack of clear safeguards for the use and storage of such data. Data must be seized and stored under clear regulations on access to such stored data, requirements to immediately destroy any data which is not relevant to the purpose for which it was gathered. There must be clear regulation on how such data will be handled or destroyed at the conclusion of an investigation or trial.[33]

In terms of section 47 of the Act, internet (or other) service providers, who provide information for the sake of investigations under the Act, will not be liable for criminal or civil suit. This effectively grants immunity to what may be government or private corporations, who may breach the right to privacy of their clients and provide information to the government for such investigations. There also does not seem to be any requirement for the service provider to notify the person – whose data is being shared – that such a breach has occurred. The only safeguard appears to be that any person who receives such data during an investigation has a duty to protect the privacy of such information (section 47(2)).

The broad powers of seizure allow the Agency to take possession of a computer, or another piece of hardware, not only if it was used to "occur the crime" but also if it is suspected to be "helpful to prove the crime". Computers and other equipment may also be seized if it is not possible to otherwise access the system, or if there is a possibility of data loss or destruction.[34] While section 45(1) states that an inquiry should take place in such a way that "the legitimate use of computer… is not hampered", the provisions in section 45(2) largely negate this precautionary step, since any computer which is password protected or encrypted can be lawfully seized under the Act.

> **"The broad powers of seizure allow the Agency to take possession of a computer, or another piece of hardware, not only if it was used to "occur the crime" but also if it is suspected to be "helpful to prove the crime"."**
>
> Amnesty International

These powers of arrest are doubly problematic because no fewer than 14 of the crimes enumerated are non-bailable offences. Therefore, if a person has been arrested by a police officer under section 45, under the offence of propaganda or campaign against the spirit of liberation (section 21), or for collecting information (section 19), for cyber-terrorism (section 27), for hurting religious values (section 28), or deteriorating law and order (section 31), bail would not be an option. Given that a person can be arrested merely on the suspicion of a police officer that evidence may be destroyed, it is possible that these provisions might lead to abuse of the right to freedom of expression in Bangladesh, and to arbitrary deprivations of liberty.

OVERBROAD OFFENCES CRIMINALIZE LEGITIMATE USE OF COMPUTERS

The definition of "malware" in the Act in section 2 is also a cause for concern. The use of malware in terms of the Act can be considered an act or "cyber-terrorism" if there is a possibility of death or severe injury – and the crime is extremely loosely defined.[35] The Act covers any software that adversely affects the performance of a device.[36] Even the slightly narrower definition in the next section does not require any intent, or deal with the question of whether this software is used without the permission of the device's owner.[37] Thus, there would not necessarily be a differentiation between legitimate access to a computer remotely for use of or even repair of software or when a criminal attempt to infiltrate a victim's computer to steal credit card information. Both could be considered malware.

We recommend that this definition be amended and narrowed to protect the legitimate use of software, including for internet security research.

A related concern is the extremely broad and vague provision related to hacking in section 34. The definition of hacking focuses on the effect of an act of "hacking" such as "alter…of computer information storage" (section 34) or "damaging a computer"; however, this could apply to a very large amount of software or equipment. The provision should include reference to deliberate damage to a

[32] Section 43(1), Digital Security Act
[33] Report of the United Nations Office of the High Commissioner for Human Rights, The Right to Privacy in the Digital Age, A/HRC/39/29 (August 3, 2018), para. 37
[34] Section 45(2), Digital Security Act
[35] Section 27(b), Digital Security Act
[36] Section 2(1).t.i, Digital Security Act
[37] Section 2(1).t.ii, Digital Security Act

computer system to make the offence more specific. In terms of section 34(2)(a), "hacking means – (a) Destroy, cancel, alter or reducing its value or usefulness or otherwise damaging of computer information storage". This provision also is overly broad, since reducing the value or usefulness of a computer information storage could be through as innocent an act as issuing an updated version of the same computer. Hacking carries a severe punishment of up to 14 years' imprisonment and/or 10 million taka fine.

In this context, section 19 also deserves mention. For example, section 19 of the Act is extremely alarming in the formulation of the crime:

> "19(1) If a person – (a) Collects any data, database, information or excerpts of same information from any computer, computer system or computer network, or collects information stored on that computer, computer system or computer network, or collects copies or portions of any data, including stored by transferable information-data… then similar act of said person shall be a crime."

The crime in this instance is unclear; and legitimately retrieving data from any computer, including what may be one's own computer, may very well be deemed a crime. In terms of section 19(b), entering or attempting to enter any "malware" in any computer, system, or network is a crime.

The penalty for commission of a crime under section 19(1) is up to seven years' imprisonment and/or with a 1 million taka fine. For a repeat offence, the punishment is up to 10 years' imprisonment and/or with a 2.5 million taka fine.

SEVERE PUNISHMENT FOR CRIMES

The controversial nature of many of the provisions of the Act is exacerbated by the severe punishments stipulated for a number of crimes under the Act.

For some crimes such as "propaganda or campaign against the liberation war, the spirit of liberation war, father of the nation, national anthem or national flag" the punishment for repeat offence is a mandatory sentence of life imprisonment and/or 30 million taka fine. Others range from discretionary prison sentences of seven to 14 years' imprisonment, and/or fines ranging from 200,000 taka to 30 million taka.

TRYING OF OFFENCES UNDER THE ACT

The Act appears to set up a Special Tribunal under the Code of Criminal Procedure, as amended by section 4 of the Criminal Law Amendment Act No. XII of 1923. All offences under the Act will be tried by this Special Tribunal, which will be deemed to be a session court (that is, the initial criminal court). Problematically, though it appears that the prosecution need not be by a public prosecutor, in terms of section 50(3), "the person acting on behalf of the complainant in the Tribunal shall be deemed to be a public prosecutor". An appeals process is set out from a decision of the Special Tribunal, to "the Appeal Tribunal".[38]

CONCLUSIONS

In its current form, the Digital Security Act poses a grave threat to the right to freedom of expression, the right to privacy and other human rights in Bangladesh. This law, just like the Information and Communication Technology Act before it, may be used to arrest and intimidate journalists, crush dissent and silence contrary opinions. It could be used to carry out invasive forms of surveillance and to intimidate users of social media sites, to prevent the uncovering of human rights violations against minorities and marginalized groups, and to muzzle both the media and civil society.

We are particularly concerned about the possibility of this Act being used to repress the independent functioning of the media. The Human Rights Committee has, in its General Comment to Article 19, emphasized the importance of free communication of ideas and the role of the media: "There is now a global network for exchanging ideas and opinions that does not necessarily rely on the traditional mass media intermediaries. States parties should take all necessary steps to foster the independence of these new media and to ensure access of individuals thereto."[39] The way the Act restricts the free exchange of ideas through digital means will significantly restrict the ability of the media to function freely and independently. The previous use of the ICT Act to target the media and journalists provides a precedent for these abuses. As of April 2018, 1,271 people were charged under section 57 of the ICT Act.[40] The draconian provisions of that law have now been replaced by what appears to be an even more alarming piece of legislation, the Digital Security Act of 2018.

[38] Section 48(2), Digital Security Act
[39] General Comment 34, Human Rights Committee, para 15
[40] Human Rights Watch, "Bangladesh: Protect Freedom of Expression | Repeal Draconian Section 57 but New Law Should Not Replicate Abuses", 9 May 2018, available at https://www.hrw.org/news/2018/05/09/bangladesh-protect-freedom-expression

In this context, Amnesty International urges Bangladesh to amend this draconian law, in a manner that is in line with the spirit of the ICCPR, protecting the rights that it has committed to protecting for all persons. This will both be in keeping with its international human rights law obligations, and the recommendations it accepted at the Universal Periodic Review earlier this year.

RECOMMENDATIONS

In this light, Amnesty International makes the following specific recommendations to the government of Bangladesh, to urgently bring the Act in line with its international human rights law obligations:

- The DSA should be repealed unless it can be promptly amended such that it complies with international human rights law, including the ICCPR, to which Bangladesh is a state party.
- Vague or undefined provisions in the Act should be removed, or narrowed to provide sufficient precision that they meet the test of legality required for restrictions on the right to freedom of expression, for example offences in sections 21, 25 and section 28 which are so vague, that they may lead to criminalizing of legitimate expression of opinions or thoughts.
- Provisions which allow for removal or blocking of content, or for the seizure or search of devices or data, such as section 8, must include safeguards such as judicial authorization or oversight and be brought within international human rights law and standards.
- Decriminalize defamation.
- Powers of various agencies including the Digital Security Agency and investigating officers, should be clear and well defined, and subject to safeguards and oversight to prevent possible abuse of powers by any of those authorized to restrict freedoms in terms of the Act.
- Amend section 53 of the Act so that release pending trial is the general rule, while pre-trial detention is restricted to cases where a court finds specific, concrete and compelling reasons to do so in the interest of justice or safety. Such a decision must be reviewed frequently and be subject to appeal.

CONTACT US

info@amnesty.org

+44 (0)20 7413 5500

JOIN THE CONVERSATION

www.facebook.com/AmnestyGlobal

@Amnesty

Front Cover illustration *by Colin Foo copyright 2018*

First published in 2018

by Amnesty International Ltd

Peter Benenson House, 1 Easton Street

London WC1X 0DW, UK

Index: ASA 13/9364/2018

NOVEMBER 2018

LANGUAGE: ENGLISH

amnesty.org

AMNESTY INTERNATIONAL