ARTICLE 19

Bangladesh: Digital Security Act 2018

November 2019

Legal analysis

Executive summary

In this analysis, ARTICLE 19 reviews the compatibility of the Digital Security Act 2018 (the 2018 Act), adopted in October 2018, for its compliance with international standards on freedom of expression. The 2018 Act was developed following the commitment of the Bangladesh Government to repeal the Information and Technology Act, which has been frequently used to restrict the right to freedom of expression in Bangladesh.

Unfortunately, ARTICLE 19's analysis shows that not only does the 2018 Act expand existing restrictive provisions, it includes several provisions that are in breach of international human rights law. In particular, several definitions contained in the 2018 Act are too vague and overbroad. The Act vests sweeping blocking powers in a government agency. It also contains several speech offences, including criminal defamation, defamation of religions, or the sending of 'offensive' information that would criminalise a wide range of legitimate expression. Finally, the Act grants carte blanche to the government to make rules in areas such as the collection, preservation or decryption of evidence or data, rules that ought to be decided by the Bangladesh Parliament with a view to protect the rights to freedom of expression, privacy and due process.

ARTICLE 19 concludes that the 2018 Act is deeply flawed and that it should be reviewed and its most problematic provisions repealed as a matter of urgency.

Summary of recommendations

- The entire Digital Security Act 2018 must be reviewed and brought into full compliance with international human rights standards.

- The following sections of the Digital Security Act must be repealed, in particular:
  - Section 8, Chapter 3 which grants sweeping powers to DSA, an executive body, to block information online and restrict freedom of expression beyond what is permissible under international freedom of expression standards;

  - Sections 21, 25, 28, 29, 31 of Chapter 6 which include speech offences, defined in vague and overbroad terms;

  - Section 38 which deals with service providers' liability. At the very least, it should be amended to require 'actual' knowledge of illegality and the taking of 'reasonable' steps before liability can be imposed;

  - Sections 56, 59 and 60 of Chapter 9, which respectively set out various powers to delegate, to 'remove difficulties' and to make rules. Or, at the very least, these Sections should be drastically limited in their scope.

- Several definitions in Chapter 2 must be clarified, including data storage, critical information infrastructure, digital security, illegal entrance, cognition of Liberation War and service provider.

- Section 4 of Chapter 1 should be amended to clarify that domestic provisions should only apply extraterritorially when a real and substantial connection can be established between the service at issue and the country seeking to apply its laws in this way.

- Computer-related offences in sections 17-20, 33 and 34 should be reviewed and brought more closely in line with relevant international standards in this area, such as the Cybercrime Convention 2001.

- If sections 21, 25, 28, 29 and 31 are repealed, section 35 should only be reviewed to include a requirement of intent.

Table of contents

Introduction

In October 2019, ARTICLE 19 analysed Bangladesh's Digital Security Act 2018 (the 2018 Act), published in October 2018 through a gazette notification by the Ministry of Law, Justice and Parliamentary Affairs. The Digital Security Act 2018 was passed unanimously by the Parliament of Bangladesh on 19 September 19 2018[1] to ensure digital security and prevent crimes committed on digital platforms.

The Digital Security Act 2018 is in stark contradiction with government promises made in early 2018 that the draconian Information and Technology Act, in particular section 57, would be repealed. Instead of repealing this law, the new Digital Security Act expands and reinforces the draconian Section 57 of the Information and Communication Technology Act that was used extensively to crackdown on freedom of expression in the country.

In April 2018, the then Digital Security Bill was presented to the Bangladesh Parliament. On 19 April, the country's leading editors of print media met with the ministers of the Ministry of Law, Justice and Parliamentary Affairs and the Ministry of Post, Telecommunications & Information Technology respectively to express their deep concerns over some provisions in the Bill. They apprehended that freedom of expression and independent journalism would be severely affected if those provisions were to be adopted by Parliament. Recognising the concerns of the Editor's Council are logical for the most part. In a meeting on 21 May, the Law minister assured representatives of the Editors' Council, the Association of Television Channel Owners and a faction of Bangladesh Federal Union of Journalists that the government would not enact any law that would hamper independent journalism. It was decided at that meeting that the Law minister would ask the Parliamentary Standing Committee of Post, Telecommunications & Information Technology ministry to scrutinise the Bill and that the Editors' Council should put its concerns in writing before the Committee. On 22 May, the Editors' Council duly wrote to the standing committee, highlighting their concerns for freedom of expression. However, the committee did not address them and recommended for the Bill to proceed. On 17 September, the Editors Council denounced the draft Digital Security Act as it failed to make any of the changes that they had recommended in eight sections (8, 21, 25, 28, 29, 31, 32 and 43) of the Act. On 30 September, the Editors Council sat with the government demanding that some sections of the Bill be changed before the President signed it into an Act. However, on 08 October 2018, the President signed the Bill unchanged and the Act came into force accordingly.

Our analysis is based on Bangladesh's obligations under international human rights standards, in particular those on the right to freedom of expression, as they apply to the domestic guarantees to freedom of expression in the Bangladesh Constitution. This analysis not only examines human rights concerns with specific sections of the 2018 Act, but also offers concrete recommendations on how each section discussed below may be modified to ensure their compatibility with international standards. While ARTICLE 19 focuses on freedom of expression concerns with the 2018 Act, the fact that there are no comments on particular sections does not signal our endorsement.

Like earlier drafts of the Act prior to its adoption,[2] ARTICLE 19 concludes that the 2018 Act is deeply flawed; it should be reviewed and its most problematic provisions repealed as a matter

[1] Act No. 46 of 2018
[2] See ARTICLE 19, Bangladesh Draft Security Act, April 2016.

of urgency. We urge the Bangladesh Government to follow the recommendations in this analysis and we stand ready to provide further support in this process.

Applicable international human rights standards

The right to freedom of expression

The right to freedom of expression is protected by Article 19 of the Universal Declaration of Human Rights (UDHR),[3] and given legal force through Article 19 of the International Covenant on Civil and Political Rights (ICCPR).[4] Bangladesh ratified the ICCPR in 2000 and is therefore legally bound to respect and to ensure the right to freedom of expression as contained in Article 19 of the ICCPR.

The scope of the right to freedom of expression is broad. It requires States to guarantee to all people the freedom to seek, receive or impart information or ideas of any kind, regardless of frontiers, through any media of a person's choice. The UN Human Rights Committee (HR Committee), the treaty body of independent experts monitoring States' compliance with the ICCPR, has affirmed that the scope of the right extends to the expression of opinions and ideas that others may find deeply offensive.[5]

While the right to freedom of expression is fundamental, it is not absolute. A State may, exceptionally, limit the right under Article 19(3) of the ICCPR, provided that the limitation is:

- **Provided for by law**; any law or regulation must be formulated with sufficient precision to enable individuals to regulate their conduct accordingly.

- **In pursuit of a legitimate aim**, listed exhaustively as: respect of the rights or reputations of others; or the protection of national security or of public order (*ordre public*), or of public health or morals;

- **Necessary and proportionate in a democratic society**, i.e. if a less intrusive measure is capable of achieving the same purpose as a more restrictive one, the least restrictive measure must be applied.[6]

Thus, any limitation imposed by the State on the right to freedom of expression must conform to the strict requirements of this three-part test. Further, Article 20(2) ICCPR provides that any advocacy of national, racial or religious hatred that constitutes incitement to discrimination, hostility or violence must be prohibited by law.

Furthermore, Article 39 of the Constitution of the People's Republic of Bangladesh guarantees the right to freedom of expression as follows:

> 39. (1) Freedom of thought and conscience is guaranteed.

[3] Through its adoption in a resolution of the UN General Assembly, the UDHR is not strictly binding on states. However, many of its provisions are regarded as having acquired legal force as customary international law since its adoption in 1948; see *Filartiga v. Pena-Irala*, 630 F. 2d 876 (1980) (US Circuit Court of Appeals, 2nd circuit).
[4] The ICCPR has 167 States parties, including Bangladesh.
[5] See HR Committee, General Comment No. 34 on Article 19: Freedoms of opinion and expression, CCPR/C/GC/34, 12 September 2011, para 11.
[6] *Velichkin v. Belarus*, Communication No. 1022/2001, U.N. Doc. CCPR/C/85/D/1022/2001 (2005).

(2) Subject to any reasonable restrictions imposed by law in the interests of the security of the State, friendly relations with foreign states, public order, decency or morality, or in relation to contempt of court, defamation or incitement to an offence–
a) the right of every citizen to freedom of speech and expression; and
b) freedom of the press, are guaranteed.

Freedom of expression online and intermediary liability under international law

In 2012, the UN Human Rights Council (HRC) recognised that the "same rights that people have offline must also be protected online."[7] The HR Committee has also made clear that limitations on electronic forms of communication or expression disseminated over the Internet must be justified according to the same criteria as non-electronic or "offline" communications, as set out above.[8]

While international human rights law places obligations on States to protect, promote and respect human rights, it is widely recognised that business enterprises also have a responsibility to respect human rights.[9] Importantly, the UN Special Rapporteur on freedom of opinion and expression (Special Rapporteur on FOE) has long held that censorship measures should never be delegated to private entities.[10] In his June 2016 report to the HRC,[11] the Special Rapporteur on FOE enjoined States not to require or otherwise pressure the private sector to take steps that unnecessarily or disproportionately interfere with freedom of expression, whether through laws, policies, or extra-legal means. He further recognised that "private intermediaries are typically ill-equipped to make determinations of content illegality,"[12] and reiterated criticism of notice and takedown frameworks for "incentivising questionable claims and for failing to provide adequate protection for the intermediaries that seek to apply fair and human rights-sensitive standards to content regulation," i.e. the danger of "self- or over-removal."[13]

The Special Rapporteur on FOE recommended that any demands, requests and other measures to take down digital content must be based on validly enacted law, subject to external and independent oversight, and demonstrate a necessary and proportionate means of achieving one or more aims under Article 19 (3) of the ICCPR.[14]

In their 2017 Joint Declaration on "freedom of expression, 'fake news', disinformation and propaganda", the four international mandates on freedom of expression expressed concern at "attempts by some governments to suppress dissent and to control public communications through [...] efforts to 'privatise' control measures by pressuring intermediaries to take action to restrict content."[15] The Joint Declaration emphasises that

---

[7] HRC Resolution 20/8 on the Internet and Human Rights, A/HRC/RES/20/8, June 2012.
[8] General Comment No. 34, *op cit.*, para 43.
[9] Guiding Principles on Business and Human Rights: Implementing the United Nations "Protect, Respect and Remedy" Framework (The Ruggie Principles), A/HRC/17/31, 21 March 2011, Annex. The UN Human Rights Council endorsed the guiding principles in HRC resolution 17/4, A/HRC/RES/17/14, 16 June 2011.
[10] Report of the Special Rapporteur on FOE, 16 May 2011, A/HRC/17/27, paras 75-76.
[11] Report of the Special Rapporteur on FOE, 11 May 2016, A/HRC/32/38; para 40 – 44,
[12] *Ibid.*
[13] *Ibid.*, para 43.
[14] *Ibid.*
[15] Joint Declaration on Freedom of Expression and "Fake News", Disinformation and Propaganda, adopted by the Special Rapporteur on FOE, the Organization for Security and Co-operation in Europe (OSCE) Representative on Freedom of the Media, the Organization of American States (OAS) Special Rapporteur on Freedom of Expression and the African Commission on Human and Peoples' Rights (ACHPR) Special Rapporteur on Freedom of Expression and Access to Information, 3 March 2017.

> [I]ntermediaries should never be liable for any third party content relating to those services unless they specifically intervene in that content or refuse to obey an order adopted in accordance with due process guarantees by an independent, impartial, authoritative oversight body (such as a court) to remove it and they have the technical capacity to do that.

In his April 2018 report, the Special Rapporteur on FOE noted that States should only seek to restrict content pursuant to an order by an independent and impartial judicial authority, and in accordance with due process and standards of legality, necessity and legitimacy.[16] He went on to state that States and intergovernmental organizations should refrain from establishing laws or arrangements that would require the "proactive" monitoring or filtering of content, which is both inconsistent with the right to privacy and likely to amount to pre-publication censorship. He also recommend that States should refrain from adopting models of regulation where government agencies, rather than judicial authorities, become the arbiters of lawful expression.

As a state party to the ICCPR, Bangladesh must ensure that any of its laws attempting to regulate electronic and Internet-based modes of expression comply with Article 19 of the ICCPR as interpreted by the UN Human Rights Committee and that they are in line with the special mandates' recommendations.

Online content regulation under international law

The requirement that all limitations imposed by the State on the right to freedom of expression online must conform to the strict requirements of this three-part test have been endorsed and further explained in several reports of the Special Rapporteur on FOE[17] in which he clarified the scope of legitimate restrictions on different types of expression online.[18] He identified three different types of expression for the purposes of online regulation:

- expression that constitutes an offence under international law and can be prosecuted criminally;
- expression that is not criminally punishable but may justify a restriction and a civil suit; and;
- expression that does not give rise to criminal or civil sanctions, but still raises concerns in terms of tolerance, civility and respect for others.[19]

In particular, the Special Rapporteur on FOE clarified that the only exceptional types of expression that States are required to prohibit under international law are: (a) child pornography; (b) direct and public incitement to commit genocide; (c) hate speech; and (d) incitement to terrorism. He further made clear that even legislation criminalizing these types of expression must be sufficiently precise, and there must be adequate and effective safeguards against abuse or misuse, including oversight and review by an independent and impartial tribunal or regulatory body.[20] In other words, these laws must also comply with the three-part test outlined above. For example, legislation prohibiting the dissemination of child pornography over the Internet through the use of blocking and filtering technologies is not immune from those requirements.

The Special Rapporteur on FOE also highlighted his concern that a large number of domestic provisions seeking to outlaw hate speech are unduly vague, and in breach of international standards for the protection of freedom of expression. This includes expression such as

[16] See Report of the Special Rapporteur on FOE, A/HRC/38/35, 6 April 2018.
[17] See the Report of the Special Rapporteur on FOE, A/HRC/17/27, 16 May 2011 and A/66/290, 10 August 2011.
[18] *Ibid.*, August 2011 Report, para18.
[19] *Ibid.*, paras 20-36.
[20] *Ibid.*, para 22

combating "incitement to religious unrest," "promoting division between religious believers and non-believers," "defamation of religion," "inciting to violation," "instigating hatred and disrespect against the ruling regime," "inciting subversion of state power" and "offences that damage public tranquillity."

The protection of the right to privacy and anonymity online

Guaranteeing the right to privacy in online communications is essential for ensuring that individuals have the confidence to freely exercise their right to freedom of expression. The right of private communications is strongly protected in international law through Article 17 of the ICCPR, which provides, *inter alia*, that:

> No one shall be subjected to arbitrary or unlawful interference with his privacy, family, home or correspondence, nor to unlawful attacks on his honour and reputation.

The UN Special Rapporteur on promotion and protection of human rights and fundamental freedoms while countering terrorism has argued that like restrictions on the right to freedom of expression under Article 19, restrictions of the right to privacy under Article 17 of the ICCPR should be interpreted as subject to the three-part test.[21] In 2017, the HRC confirmed this in Resolution 34/7.

The lack of ability of individuals to communicate privately substantially affects their freedom of expression rights. In his report of 16 May 2011, the UN Special Rapporteur on Freedom of Opinion and Expression, Frank La Rue, expressed his concerns that:

> 53. [T]he Internet also presents new tools and mechanisms through which both State and private actors can monitor and collect information about individual's communications and activities on the Internet. Such practices can constitute a violation of the Internet user's right to privacy, and, by undermining people's confidence and security on the Internet, impede the free flow of information and ideas online.

In particular, the Special Rapporteur recommended that States should ensure that individuals can express themselves anonymously online and to refrain from adopting real-name registration systems.[22]

In May 2015, the Special Rapporteur on FOE published his annual report on encryption and anonymity in the digital age.[23] The Special Rapporteur concluded:

> 56. Encryption and anonymity, and the security concepts behind them, provide the privacy and security necessary for the exercise of the right to freedom of opinion and expression in the digital age. Such security may be essential for the exercise of other rights, including economic rights, privacy, due process, freedom of peaceful assembly and association, and the right to life and bodily integrity. Because of their importance to the rights to freedom of opinion and expression, restrictions on encryption and anonymity must be strictly limited according to principles of legality, necessity, proportionality and legitimacy in objective. (…)
>
> 60. States should not restrict encryption and anonymity, which facilitate and often enable the rights to freedom of opinion and expression. Blanket prohibitions fail to be necessary

[21] Report of the Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism, Martin Scheinin, A/HRC/13/37, 28 December 2009.
[22] *Ibid.*, para 84.
[23] Report of the Special Rapporteur on FOE, A/HRC/29/32, 22 May 2015.

> and proportionate. States should avoid all measures that weaken the security that individuals may enjoy online, such as backdoors, weak encryption standards and key escrows. In addition, States should refrain from making the identification of users a condition for access to digital communications and online services and requiring SIM card registration for mobile users (...)

The findings of this report confirmed the earlier findings of the 2013 report of the Special Rapporteur on FOE, which observed that restrictions to anonymity facilitates States' communications surveillance and have a chilling effect on the free expression of information and ideas.[24]

Cybercrime

ARTICLE 19 notes that there is no international standard on cybercrime. From comparative perspective, we note that the Council of Europe Convention on Cybercrime CETS (Cybercrime Convention)[25] provides a helpful guidance on how to draft cybercrime legislation in accordance with human rights standards. In particular, it contains basic definitions, including a definition of computer data, computer system, traffic data and service provider.

The Convention further requires its signatory parties to create offences against the confidentiality, integrity and availability of computer systems and computer data, computer-related offences such as forgery and content-related offences such as the criminalisation of child pornography. In addition, the Convention mandates the adoption of a number of procedural measures to investigate and prosecute cybercrimes, including preservation orders, production orders and search and seizure of computer data. Finally, and importantly, the Convention makes clear that the above measures must respect the conditions and safeguards for the protection of human rights consistent with the Contracting parties' obligations under the European Convention on Human Rights and the ICCPR.

[24] *Ibid.*, paras 48-49.
[25] The Council of Europe Convention on Cybercrime, CETS No. 185, adopted on 23 November 2001 in force since July 2004. The Convention and has been ratified also by countries outside of the Council of Europe, including Philippines, Japan or Australia.

Analysis of the Act

The 2018 Act is divided into nine chapters. Of particular relevance to freedom of expression are

- Chapter 1 that contains a number of definitions and deals with the extra-territorial application of the Act,
- Chapters 2 and 3 that establish the government agency with powers to order a number of preventative measures, including the blocking of information,
- Chapter 6 that provides for a number of computer crimes and speech offences and Chapter 9 that is concerned with a number of miscellaneous powers.

Chapter 1, section 2 - Vague and overbroad definitions

ARTICLE 19 notes that section 2(1) of the 2018 Act sets out a number of definitions of key terms, such as "data storage," "critical information infrastructure," "digital security," "illegal entrance," "defamation," "Cognition of Liberation War" or "service provider." Section 2 (2) further makes explicit reference to the Information and Communication Technology Act 2006 for any other term not otherwise defined in the 2018 Act.

ARTICLE 19 is concerned that several definitions in the 2018 Act are overly broad and fail to meet the legality requirement under international human rights, particularly when seen in light of the sweeping powers granted to the Bangladesh Director General (See next section of our analysis):

- **"Data storage"** is defined as "text, image, information presented as audio or video format, knowledge, incident, principle idea or guidelines, which (i) has been or is being formally produced by means of any computer or computer network or system; and (ii) has been prepared with the aim of using it in any computer or computer network or computer system." ARTICLE 19 notes that this definition seems to be referring to 'digital data' rather than defining "data storage." 'Data *storage'* (our emphasis) is generally concerned with the recording of data in a storage medium, which might be a computer system or other technology such as the cloud.

- **"Critical Information Infrastructure"** (CII) is broadly defined as "any physical or virtual information infrastructure declared by the government, which is capable of controlling, processing, circulating or preserving any information, data or electronic information and which if it is damaged or compromised may adversely affect (i) public safety or financial security or public health, (ii) national security or national integrity or sovereignty." In ARTICLE 19's view, the proposed standard in the definition, i.e. that public safety and other interests *may be adversely affected* if those infrastructures are merely *damaged* or *compromised*, is far too low.
  From a comparative perspective, we note that in the USA, for instance, critical infrastructure is defined as "systems and assets, whether physical or virtual, so vital to the USA that the incapacity or destruction of such systems and assets would have a *debilitating* impact on security, national economic security, national public health or safety, or any combination of those matters" (our emphasis).[26] In the EU, Council Directive 2008/114/EC defines critical information infrastructure as ''ICT systems that are Critical Infrastructures

[26]See USA Patriot Act of 2001 (42 U.S.C. §5195c(e)).

for themselves or that are *essential* for the operation of Critical Infrastructures (telecommunications, computers/software, Internet, satellites, etc)"[27] (our emphasis). In other words, information infrastructure can only be 'critical' if the government entirely depends on it to maintain other critical infrastructure and/or guarantee the protection of the various interests listed in the definition. Mere adverse impact is not sufficient.

- **"Digital security"** is defined self-referentially as "the security of any digital device or digital system." In our view, this is clearly insufficient since it fails to define what 'security' means in this context. Instead, the definition should at least make reference to tools or other measures put in place to protect electronic data held in a computer system or other technology against intrusions by outsiders.

- **"Illegal entrance"** is defined as entrance without permission of any person or authority or entrance in violation of the conditions of permission of entrance by the said person or authority into any computer or digital device or digital network system, or by above mentioned entrance create hindrance in the exchange of any data-information suspend or prevent or stop the process of exchange of data-information, or change the data-information or add or deduct the data-information or collect the data-information with the use of a digital device. In ARTICLE 19's view, this definition conflates illegal access to a computer system with data or system interference.[28] This is likely to lead to confusion in relation to any criminal offence based on this definition.

- **"Cognition of Liberation War"** means "those great ideals which inspired our brave public to dedicate themselves to the national liberation struggle and our brave martyrs to lay down their lives for the cause of liberation, the ideals of nationalism, socialism, democracy and secularism" under the 2018 Act. ARTICLE 19 believes that any criminal offence based on this definition is bound to be overbroad. In particular, it is likely to be used to stifle criticism of the government in place or its policies.

- **"Service Provider"** is defined as (i) any person who through computer or digital process enables any user to communicate; or (ii) any such person, entity or institution who or which preserves or process data in favour of the service user. ARTICLE 19 notes that this definition appears excessively broad. For comparative perspective, we note for instance that under the EU Directive, information society services cover "any service normally provided *for remuneration*, at a distance, by means of electronic equipment for the processing (including digital compression) and storage of data, and at the individual request of a recipient of a service"[29] (our emphasis). We are concerned that the current definition in the 2018 Act could be used to hold individuals providing free wifi hotspots, e.g. through their phone, liable for the actions of users on their networks.

Recommendation:

- Several definitions, including data storage, critical information infrastructure, digital security, illegal entrance, cognition of Liberation War and service provider, must be narrowed or clarified in accordance with international standards or best practice.

[27] Council Directive 2008/114/EC of 8 December 2008 on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection, 23 December 2008.
[28] *C.f.* the Cybercrime Convention, *op.cit.*, Articles 2, 4 and 5.
[29] *C.f.* Directive (EU)2015/1535 of the European Parliament and the Council of of 9 September 2015 laying down a procedure for the provision of information in the field of technical regulations and of rules on Information Society services (codification), L 241/1, 17 September 2015.

Chapter 1, section 4 – Extraterritorial application of the Act

Section 4 of Chapter 1 of the 2018 Act provides that it has extra 'judicial' application in certain circumstances, namely "(1) if any person commits an offence within this Act outside of Bangladesh which would be an offense inside Bangladesh; (2) if any person commits an offence under this Act from outside Bangladesh using a computer or computer system; and (3) if any person commits an offence 'outside Bangladesh within this Act from inside Bangladesh, then the provision of this Act will be applicable in such a manner that the whole process of committing the offense occurred in Bangladesh."

ARTICLE 19 notes that the translation of the 2018 Act makes reference to the extra 'judicial' application of the Act. Our understanding, however, is that section 4 deals with the extra*territorial* application of the Act. We further note that these kinds of provisions are not entirely unusual in the criminal law, at least in certain countries such as France. In practice, however, they are subject to the ability of the prosecuting authorities to gather sufficient evidence, including from abroad, following appropriate procedures, and the extent to which a suspect is likely to be extradited under extradition treaties. In any event, ARTICLE 19 is concerned that section 4 is overbroad since it would lead to the extraterritorial application of provisions, which are in breach of international human rights law. In our view, domestic provisions should only apply extraterritorially when a real and substantial connection can be established between the service at issue and the country seeking to apply its laws in this way.

Recommendation:

- Section 4 of Chapter 1 should be amended to clarify that domestic provisions should only apply extraterritorially when a real and substantial connection can be established between the service at issue and the country seeking to apply its laws in this way.

Chapters 2 & 3 - Blocking powers of the Digital Security Agency

Chapter 2 of the 2018 Act establishes the Digital Security Agency (DSA). Its remit is unclear other than the fact that its overarching purpose is to fulfil the objectives of the 2018 Act. Section 6 provides that the government appoints the Managing Director and the Directors.

Under Chapter 3, section 8 of the Act, the DSA is granted powers to order preventive measures. In particular, section 8 (1) provides that the Director General of the DSA can request the Bangladesh Telecommunications and Regulatory Authority ('BTRC') to remove or block 'data-information' that falls within the purview of the DSA and that threatens 'digital security'. Under section 8 (3), the BTRC has to comply and must notify the government. In addition, the BTRC has to comply with requests from law enforcement agencies sent via the DSA to block 'data-information' that 'hampers the nation or any part therein in terms of nations' unity, financial activities, security, defence, religious values, public discipline or incites racism and hatred' (Section 8 (2)).

ARTICLE 19 notes that the 2018 Act grants sweeping powers to the executive to block information it doesn't like. Under international law, any restriction on freedom of expression must be provided by law and be necessary in a democratic society. Section 8 utterly fails this test.

As noted above, the 2018 Act provides an overbroad definition of 'digital security'. In any event, section 8 suggests that digital security is not understood in the sense of information security but rather more broadly in the sense of national security, for which no definition is provided

and therefore leaves enormous discretion to the executive. Section 8 (2) is couched in equally broad and vague terms, including references to the 'nation's unity', 'religious values' and 'public discipline', so that any information taken to get in the way of government action or policy could be the subject of a blocking order. Leaving aside that e.g. 'public discipline' is not a legitimate aim under international law, no reference is made to the need for blocking orders to be necessary and proportionate to the aim sought to be achieved. All of the above is a serious problem, particularly in circumstances where, as noted above, such broad powers are vested in a government agency, the DSA, rather than an independent body or a court. This is also in stark contradiction with international standards in this area.

Recommendation:
- Section 8, Chapter 3 should be repealed in its entirety.

Chapter 6 - Offences

Chapter 6 of the 2018 Act provides for a wide range of offences, including some computer crimes and several speech offences. ARTICLE 19 is concerned that the 2018 Act is duplicating existing speech offences under the criminal law. If so, we believe that the new offences are likely to create legal uncertainty in this area. To the extent that cybercrime laws add anything new to existing speech offences, it often means harsher sentences for the online version of an offline offence. In our view, this is unjustified, as the same crime should be punished in the same way online and offline.

In any event, the new speech offences in the 2018 Act contain several terms that are unduly vague. Legitimate content will inevitably get caught out as a result. We highlight particular points of concern further below.

- **'Propaganda or campaign against the liberation war, cognition of the liberation war, father of the nation, national anthem or national flag':** section 21 effectively punishes with up to 10 years imprisonment and/or one crore taka (nearly £100,000) any online criticism of the liberation war, 'cognition of the liberation war' as well as an emblematic figure of Bangladesh and some national symbols. Re-offending is punishable by life imprisonment and/or a fine of up to 3 crores (nearly £300 000). Neither section 21 nor any other provision in the 2018 Act define what amounts to 'propaganda' or a 'campaign'. As already noted, the definition of the Liberation War is overly broad. In any event, the offence is couched in such broad terms and its purpose is such that it would prevent legitimate debate on matters of public interest, including the country's history and the role of the father of the nation. As such it is clearly incompatible with international human rights law and should be repealed.

- **'Publishing, sending of offensive, false or fear inducing data information':** section 25 (1)(a) criminalises intentionally or knowingly sending information which is offensive or fear-inducing or sending, publishing or disseminating false information despite knowing that it is false with the intention to "annoy, insult, humiliate or denigrate a person." Section 25 (1)(b) further criminalises the publication, or assisting the publication of any information "with the intention of tarnishing the image of the nation or spread confusion or despite knowing it as false, publishing or propagating information in full or in a distorted form for the same intentions." These offences are punishable with up to 3 years imprisonment and/or a fine of 3 lacs taka (nearly £3,000).

In ARTICLE 19's view, section 25 is overbroad and constitutes a disproportionate restriction on freedom of expression. Key terms are undefined such as 'false information' or what constitutes 'offensive' content in section 25 (1)(a). Criminalising the spreading of 'false information' is particularly problematic regardless of intent because facts are not always easily distinguishable from opinions. The offences in section 25 (1)(a) are also made up of elements that are eminently subjective (e.g. offensiveness) and their threshold is very low. For instance, sending false information merely to "annoy" or "denigrate"' someone could lead to imprisonment.

Section 25 (1)(b) is equally overbroad using undefined terms such as "spreading confusion" or "tarnishing the image of the nation." In practice, section 25 (1) (b) could easily be used to prosecute anyone who criticises the country or the government. For all these reasons, we recommend that section 25 be repealed in its entirety. By contrast, we note that some restrictions on freedom of expression may be justified, such as the adoption of provisions criminalising harassment or threats. If such offences do not already exist in the criminal code, the Bangladesh Parliament could consider adopting them. In so doing, it should ensure that any new offences are tightly defined and do not overly restrict freedom of expression.

- **'Publication, Broadcast etc. of information on any website that hampers religious sentiment or values'**: Section 28 criminalises the publication in any format of information with intent to hurt religious feelings or values. The offence is punishable with up to 7 years imprisonment and/or a fine of up to 10 lac taka (nearly £10,000). Re-offending is punishable by up to 10 years imprisonment and up to 20 lac taka (nearly £20,000) fine. In ARTICLE 19's view, this offence is incompatible with the freedom of expression standards under international law since it merely seeks to protect religious feelings or values rather that individual's freedom of religion. The HR Committee has made it clear in General Comment no. 34 on the right to freedom of expression that prohibitions of displays of lack of respect for a religion, including blasphemy laws are incompatible with the ICCPR.[30] For this reason, we would recommend the repeal of section 28 of the 2018 Act.

- **'To publish, broadcast defamation information':** Section 29 extends the criminalisation of defamation as defined under the Penal Code to the online environment. The offence is punishable by up to 3 years imprisonment and/or a 5 lac (nearly £ 5,000) fine. Re-offending is punishable by 5 years imprisonment and/or a fine of 10 lac (nearly £10,000). It is well established that criminal defamation, whether offline or online, is incompatible with international standards on freedom of expression. Accordingly, ARTICLE 19 recommends that section 29 be repealed.

- **Deterioration of public order:** Section 31 criminalises the intentional publication or broadcast online of material that would create "hostility, hatred or adversity among people or destroy any communal harmony or create unrest or disorder or deteriorates or threatens to deteriorate law and order." The offence is punishable with up to 7 years imprisonment and/or a fine of Tk 5 lac (nearly £ 5,000). Re-offending is punishable by 10 years imprisonment and/or a fine of 10 lac (nearly £10,000). In ARTICLE 19's view, section 31 is drafted in excessively broad terms and is incompatible with international standards on freedom of expression (see above). Key terms are undefined, such as 'communal harmony', 'law and order' or 'adversity'. The provision is further unclear about the threshold of likelihood of violence or hostility occurring. Insofar as it seeks to implement the prohibition under Article 20(2) of ICCPR, it fails to make reference to the protection of certain groups

[30] General Comment 34, *op.cit.*, para 48.

from incitement to violence or discrimination on the basis of protected grounds. We believe that this provision could easily be used to prosecute journalists, human rights defenders and others publishing dissenting or critical views of the government. Accordingly, we would recommend that section 31 be repealed.

- **Breaching government secrets:** Section 32 extends the criminalisation of various offences under the Official Secrets Act 1923. The offence is punishable by up to 14 years and/or a fine of up to 25 lac (nearly £25,000). Re-offending is punishable by life imprisonment and up to one crore (nearly £100,000). ARTICLE 19 has not reviewed the Official Secrets Act but we warn against unnecessarily duplicating offences to deal with online criminality. We also take this opportunity to reiterate that the protection of official secrets should not come at the expense of the protection of the right to freedom of expression. In particular, the scope of any legislation in this area should not be so broad as to cover a wide range of information and activities that could be relevant to journalism, academic research and other legitimate activities. In addition, it should include a mental element, i.e. require proof of intent to harm to the state or risk of harm from the disclosure.

- **Hacking related offences:** ARTICLE 19 notes that the 2018 Act contains several computer offences, including section 17 (illegal access to critical information infrastructure), section 18 (illegal access to a computer, digital device or computer system), section 19 (damage to a computer or computer system), section 20 (offences relating to a computer source code changes), section 33 (illegally transferring, saving, etc. of data information) and section 34 ('hacking-related' offence). We do not propose to analyse these provisions in detail but we note that the Cybercrime Convention contains a much narrower range of offences, including illegal access, illegal interception, data interference, system interference and misuse of devices. Furthermore, the Cybercrime Convention makes clear that intent is an important element of computer-related offences but it is not always included in relevant offences in the 2018 Act. Accordingly, ARTICLE 19 believes that these offences should be reviewed and brought more closely in line with international standards in this area.

- **Aiding in commission of offences under the Act:** Section 35 criminalises anyone 'aiding' the commission of an offence under the Act. The punishment for aiding the commission of an offence is the same as that of the original offence. ARTICLE 19 notes that the 2018 Act does not define what actions might count as 'aiding' the commission of an offence. Moreover, section 35 fails to include intent as an element of the commission of any such inchoate offences. As such, we believe that they are overly broad and could be used to criminalise a very wide range of Internet users. For instance, someone re-tweeting an online comment deemed to amount to e.g. deterioration of public order could fall under this provision. If the various speech offences that we have highlighted are repealed, which we recommend, inchoate offences could be kept for some computer crimes, consistent with the standards developed in the Cybercrime Convention. However, section 35 would still need to include 'intent' to comply with those standards.

- **Service providers' liability:** Section 38 provides that any service provider will not be responsible under the 2018 Act for facilitating access to data-information if it can prove that the offence was committed without his knowledge or he took all possible steps to stop the commission of these offences. Although ARTICLE 19 welcomes these defences to a liability for third party content, we remain concerned that service providers may still be held criminally liable for content posted by their users. We further note that Section 38 fails to define the standard of knowledge to be put on notice of illegality, i.e. whether knowledge results from a court order or other type of notice. Furthermore, we believe that service providers should only be required to show that they took all 'reasonable' steps to

prevent the commission of an offence. In our view, 'all possible steps' is too broad, as some steps may not be sufficiently useful and others may lead to an unnecessary interference with users' rights to freedom of expression and privacy (e.g. upload filters).

Recommendations:
- Sections 21, 25, 28, 29, 31 should be repealed
- Computer-related offences in sections 17-20, 33 and 34 should be reviewed and brought more closely in line with relevant international standards in this area.
- If sections 21, 25, 28, 29 and 31 are repealed, section 35 should only be reviewed to include a requirement of intent.
- Section 38 should be repealed. At the very least, it should be amended to require 'actual' knowledge of illegality and the taking of 'reasonable' steps before liability can be imposed.

Chapter 9 - Miscellaneous

Chapter 9 of the 2018 Act sets out various powers to delegate (section 56) to 'remove difficulties' (section 59) and to make rules (section 60).

ARTICLE 19 is very concerned by the scope of these powers for the following reasons:
- **Power to delegate, section 56:** we note that the power to delegate under section 56 is unduly broad. This is especially concerning given the powers of the Director General of the DSA to order website blocking on a massive scale. In our view, it is inappropriate for such power to be delegated to 'any employee' of the agency or 'any person' or to a 'police officer.' The power is so broadly drafted that it could be entrusted to individuals with no knowledge or expertise of the issues at stake. The fact that the power can be entrusted to 'any person' is especially concerning as it suggests that such person may not be bound by the same code of conduct that should normally apply to civil servants.

- **Removal of difficulty, section 59:** ARTICLE 19 notes that section 59 enables the government to take measures to remove 'difficulties' in the implementation of the Act. The Act however does not explain what amounts to a difficulty. In reality, this section gives carte blanche for the government to adopt measures that could well infringe in the rights to free expression and privacy without proper scrutiny from Parliament.

- **Power to make rules, section 60:** Section 60 provides that the government can enact rules for a number of purposes, including establishing the digital forensic lab, supervision of the digital forensic lab, reviewing traffic data or information and the process of its collection and preservation, process of interference, review or decryption and protection, security of compromised information infrastructure, cloud computing and metadata and security of preserved data, among others. ARTICLE 19 notes that section 60 gives unfettered power to the executive to make up rules in areas that ought to be legislated by Parliament: this included the review of traffic data or information and the process of its collection and preservation, process of interference, review or decryption and protection, security of compromised information infrastructure, cloud computing and metadata and security of preserved data. In our view, it is highly improper for the government to make rules in this area without the Bangladesh Parliament having a say in the matter and ensuring that the rights to freedom of expression, privacy and due process are protected.

Recommendations:
- Sections 56, 59 and 60 should be repealed or at the very least drastically limited in their scope.

About ARTICLE 19

ARTICLE 19 advocates for the development of progressive standards on freedom of expression and freedom of information at the international and regional levels, and their implementation in domestic legal systems. The Law Programme has produced a number of standard-setting publications which outline international and comparative law and best practice in areas such as defamation law, freedom of expression and equality, access to information and broadcast regulation.

On the basis of these publications and ARTICLE 19's overall legal expertise, the organisation publishes a number of legal analyses each year, comments on legislative proposals as well as existing laws that affect the right to freedom of expression. This analytical work, carried out since 1998 as a means of supporting positive law reform efforts worldwide, frequently leads to substantial improvements in proposed or existing domestic legislation. All of our analyses are available at http://www.article19.org/resources.php/legal.

If you would like to discuss this analysis further, or if you have a matter you would like to bring to the attention of the ARTICLE 19 Law Programme, you can contact us by e-mail at legal@article19.org.

For more information about the ARTICLE 19's work in Bangladesh, please contact, Faruq Faisel, Regional Director for Bangladesh and South Asia of ARTICLE 19, at faruq@article19.org.