ARTICLE 19

Bangladesh: Draft Digital Security Act

April 2016

Legal analysis

Executive summary

In this legal analysis, ARTICLE 19 reviews the draft Digital Security Act of Bangladesh (Draft Act), currently being discussed in the country, for its compliance with international freedom of expression standards.

As a state party to the International Covenant on Civil and Political Rights (ICCPR), Bangladesh must ensure that any of its laws attempting to regulate electronic and Internet-based modes of expression comply with international standards on freedom of expression. Hence, this analysis highlights concerns about possible conflicts with international human rights standards within the Draft Act; it also actively seeks to offer constructive recommendations on how the Draft Act can be improved.

In particular, this analysis shows that the Draft Act contains several broadly defined speech offences with harsh sentences, that could have a serious chilling effect on the right to freedom of expression online in Bangladesh. The provisions dealing with 'content-related' offences in the Draft Act fall well below international standards. The Draft Act also establishes unduly broad offences against computers and other computer-related offences. Moreover, we note that the procedural powers to investigate and prosecute cybercrimes are dangerously overbroad; we also emphasise that, under international human rights standards, all powers conferred upon the police should also be made subject to a court order.

We recommend entirely omitting several offences that are so broadly defined as to expose them to abuse for less legitimate ends. We also recommend including more precise intent and harm requirements for existing offences. Further, public interest needs to be considered in various areas of this Act; this defence offers an opportunity for the accused to establish that there was no harm or risk of harm to a legitimate interest in engaging in the proscribed activity, or that the public benefit in the activity outweighed the harm. Finally, we strongly suggest eliminating the heading of "terrorism" and categorizing these offences separately.

ARTICLE 19 hopes that the final version of the Draft Act will reflect our comments and that the Bangladesh Government and legislators will ensure that the freedom of expression online is fully protected in their national legislation.

Summary of recommendations:

- The Draft Act should provide sufficient safeguards for the protection of human rights and specifically reference international human rights standards;
- The definition of "unlawful access" in Section 2(2) of the Draft Act should explicitly require both "dishonest" intent and "infringement of security features" for access to be "unlawful;"
- In Section 2(3) the Draft Act's "may have an adverse effect on the matters relating to the" should be replaced with "seriously harm;"
- Section 2(3)(b) should be deleted;
- The definition of "forgery" in Section 2(15) should require intent for "inauthentic" data to become actionable, and the language "incorrect and inappropriate work or procedure" should be removed;
- The definitions of terms "digital pornography" in Section 2(16) and "obscene" in Section 2(36) should be struck out in their entirety;

- Section 9 should require "dishonest" intent, and its sanctions should be reduced;
- Section 10 should require "dishonest intent," "serious" harm to property; and the words "suppress" and "distort" should be eliminated;
- Section 10 should require intent for "inauthentic data" to be acted upon for legal purposes;
- The term "publishing" should be removed from the offences stipulated in Section 10;
- Section 11(1) should be amended to require "dishonest intent;"
- Section 11(2) should include a requirement for "interference with the functioning of a computer system" as well as intent to procure "economic benefit for oneself or for another person;"
- Section 12 should be struck out in its entirety. Should Section 12 be retained, it must be amended to specify that the conduct must be intentional and dishonest and that serious harm must result from it. Both reasonableness and public interest defences must be made available;
- Sections 13(1)(a)(I)-(III), as well as aiding and abetting, should not be terrorism offenses. These offenses should be placed outside of the heading of "terrorism." After Sections 13(1)(a)(I)-(III) are moved, all three should be amended to require "dishonest" intent. Similarly, after Section 13(1)(a)(I) is moved it should require "serious harm" to result from the offence, and contain provisions for a public interest defence. The remaining offences under Section 13 should be omitted as they are properly addressed under already existing offences. Section 13(1)(g), especially, should be struck out entirely;
- The word "rigorous" should be struck out from the sanctions in subsection 13(2). Sanctions for this section should be reduced by at least half;
- Sections 14, 15(1) and 16 should be omitted in their entirety;
- Section 18 should also be struck out entirely. Any investigative police search powers must be properly defined, proportionate and, where they impact upon the rights and property of individuals, include strict requirements for judicial review;
- Section 24 as written should be struck out. Any compulsion should be in accordance with other portions of the criminal code of Bangladesh, and, at the least, stipulate minimum judicial review and warrant requirements.

Table of contents

Introduction

In April 2016, ARTICLE 19 analysed the Draft Digital Security Act 2016 (Draft Act)[1] for its compliance with international human rights standards.

The Draft Act is intended to address demands from the public and the growing ICT sector for dedicated cyber-crime legislation, since this is not sufficiently covered in the Information Communications Technology (ICT) Act, which has been in operation since 2006. In response to these demands, in early 2015, the Government of Bangladesh published a draft Cyber Security Act, 2015, for public consultation and feedback. Subsequently, the draft was renamed as the Digital Security Act 2016 (Draft Act).

ARTICLE 19's analysis first sets out in detail applicable international human rights standards, in particular on the right to freedom of expression and the right to privacy, together with guidance on how these provisions are interpreted in relation to information and communication technologies. The analysis then goes on to make a number of general recommendations regarding the Draft Act as a whole, before highlighting human rights issues within particular sections of the Act.[2]

The analysis not only highlights concerns about possible conflicts with international human rights standards within the Draft Act; it also actively seeks to offer constructive recommendations on how the Act can be improved. We explain the ways in which problematic provisions in the Act can be made compatible with international standards on freedom of expression and privacy and set out key recommendations at the end of each section.

ARTICLE 19 urges the drafters of the Act and the Parliamentary committees in charge of scrutinising it to address the shortcomings identified above in order to ensure the compatibility of the Act with international standards of freedom of expression. We stand ready to provide further assistance in this process.

[1] The analysis is based on the English translation of the Draft Act, which is available upon request from ARTICLE 19. ARTICLE 19 takes no responsibility for the accuracy of the translation or for comments made on the basis of any inaccuracies in the translation.

[2] ARTICLE 19's analysis focuses only on specific sections that raise key freedom of expression concerns. The fact that there are no comments on certain sections does not constitute an automatic endorsement of those sections by ARTICLE 19.

International human rights standards

The protection of freedom of expression under international law

The right to freedom of expression is protected by a number of international human rights instruments that bind states, including Bangladesh; particularly pertinent are Article 19 of the **Universal Declaration of Human Rights (UDHR)**[3] and Article 19 of the **International Covenant on Civil and Political Rights** (ICCPR).[4]

Additionally, **General Comment No 34**,[5] adopted by the UN Human Rights Committee (HR Committee) in September 2011, explicitly recognises that Article 19 of the ICCPR protects all forms of expression and means of dissemination, including all forms of electronic and Internet-based expression.[6] In other words, the protection of freedom of expression applies online in the same way that it applies offline. States parties to the ICCPR are also required to consider the extent to which developments in information technology, such as Internet and mobile-based electronic information dissemination systems, have dramatically changed communication practices around the world.[7] The legal framework regulating the mass media should take into account the differences between print and broadcast media and the Internet, while also noting the ways in which media converge.[8]

Similarly, the four special mandates for the protection of freedom of expression have highlighted, in their **Joint Declaration on Freedom of Expression and the Internet** of June 2011, that regulatory approaches appropriate to the telecommunications and broadcasting sectors cannot simply be transferred to the Internet.[9] In particular, they recommend the development of regulatory approaches tailored to illegal content online, while pointing out that specific restrictions for material disseminated over the Internet are unnecessary. They also promote the use of self-regulation as an effective tool in redressing harmful speech.

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 HR Committee, and that they are in line with the special mandates' recommendations.

Limitations on the right to freedom of expression

While the right to freedom of expression is a fundamental right, it is not guaranteed in absolute terms. Restrictions on the right to freedom of expression must, however, be strictly and narrowly tailored and may not put in jeopardy the right itself. The determination of whether a restriction is narrowly tailored is often articulated as a three-part test. Restrictions must:

- **Be prescribed by law**: this means that a norm must be formulated with sufficient precision to enable an individual to regulate his or her conduct accordingly.[10] Ambiguous,

[3] UN General Assembly Resolution 217A(III), adopted 10 December 1948.
[4] GA res. 2200A (XXI), 21 UN GAOR Supp. (No. 16) at 52, UN Doc.
[5] CCPR/C/GC/3, adopted on 12 September 2011, available at http://bit.ly/1xmySgV.
[6] *Ibid*, para 12.
[7] *Ibid*, para 17.
[8] *Ibid*, para 39.
[9] Joint Declaration on Freedom of Expression and the Internet, June 2011, available at http://bit.ly/1CUwVap.
[10] HR Committee, *L.J.M de Groot v. The Netherlands,* No. 578/1994, UN Doc. CCPR/C/54/D/578/1994 (1995).

vague or overly broad restrictions on freedom of expression are therefore impermissible;

- **Pursue a legitimate aim:** these legitimate aims are exhaustively enumerated in Article 19(3)(a) and (b) of the ICCPR as: respect of the rights or reputations of others; protection of national security; public order; public health or morals. As such, it would be impermissible to prohibit expression or information solely on the grounds that it casts a critical light on the government or the political social system espoused by the government;

- **Be necessary and proportionate**. Necessity requires that there must be a pressing social need for the restriction. The party invoking the restriction must show a direct and immediate connection between the expression and the protected interest. Proportionality requires that a restriction on expression is not over-broad and that it is appropriate to achieve its protective function. It must be shown that the restriction is specific to attaining that protective outcome and is no more intrusive than other instruments capable of achieving the same limited result.[11]

The same principles apply to electronic forms of communication or expression disseminated over the Internet.[12]

Prohibiting incitement to discrimination, hostility or violence

It is also important to note that 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. At the same time, "inciting violence" means more than just expressing views that people disapprove of or find offensive:[13] it is speech that encourages or solicits other people to engage in violence through vehemently discriminatory rhetoric. At the international level, the UN has developed the Rabat Plan of Action, an inter-regional, multi-stakeholder process involving UN human rights bodies, NGOs and academia - which provides the closest definition of what constitutes incitement law under Article 20 (2) of the ICCPR.[14]

Terrorism and incitement to acts of terrorism

There is no universally agreed definition of terrorism under international law.[15] At the same time, UN human rights bodies have highlighted the tension between freedom of expression and counter-terrorism measures. In particular, General Comment no. 34 clearly provides:

> 46. States parties should ensure that counter-terrorism measures are compatible with paragraph 3. Such offences as "encouragement of terrorism" and "extremist activity" as well as offences of "praising", "glorifying", or "justifying" terrorism, should be clearly defined to ensure that they do not lead to unnecessary or disproportionate interference with freedom of expression. Excessive restrictions on access to information must also be

[11] HR Committee, *Velichkin v. Belarus*, No. 1022/2001, UN Doc. CCPR/C/85/D/1022/2001 (2005).
[12] General Comment 34, *op.cit.*, para 43.
[13] *C.f.* European Court, *Handyside v the UK*, judgment of 6 July 1976, para 56.
[14] See UN Rabat Plan of Action (2012), available at http://bit.ly/1T2efOV. It clarifies that regard should be given to six factors in assessing whether speech should can be considered as incitement, including the general context, the speaker, intent, content, the extent of the speech and the likelihood of harm occurring, including its imminence.
[15] See e.g. UNODC, Frequently Asked Questions on International Law Aspects of Countering Terrorism, 2009, p. 4, available at http://bit.ly/1PQeTiC. See also UNODC, The Use of the Internet for Terrorist Purposes, 2012, para 49, available at http://bit.ly/1X1yiTo.

> avoided. The media plays a crucial role in informing the public about acts of terrorism and its capacity to operate should not be unduly restricted. In this regard, journalists should not be penalized for carrying out their legitimate activities.

Moreover, the **Johannesburg Principles on National Security, Freedom of Expression and Access to Information**[16] (Johannesburg Principles), a set of international standards developed by ARTICLE 19 and international freedom of expression experts, are instructive on restrictions on freedom of expression that seek to protect national security. Principle 2 of the Johannesburg Principles states that restrictions justified on the ground of national security are illegitimate unless their genuine purpose and demonstrable effect is to protect the country's existence or its territorial integrity against the use or threat of force, or its capacity to respond to the use or threat of force. The restriction cannot be a pretext for protecting the government from embarrassment or exposure of wrongdoing, to conceal information about the functioning of its public institutions, or to entrench a particular ideology. Principle 15 states that a person may not be punished on national security grounds for disclosure of information if

- the disclosure does not actually harm and is not likely to harm a legitimate national security interest, or
- the public interest in knowing the information outweighs the harm from disclosure.

Further, the **Tschwane Principles on National Security and the Right to Information**[17] also consider extensively the types of restrictions that can be imposed on access to information.

Online content regulation

The above principles have been endorsed and further explained by the UN Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression (Special Rapporteur on FOE) in two reports in 2011.[18]

In the September 2011 report, the Special Rapporteur also clarified the scope of legitimate restrictions on different types of expression online.[19] 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.[20]

In particular, the Special Rapporteur on FOE clarified that the only types of expression that States are required to prohibit under international law are:

- child pornography;
- direct and public incitement to commit genocide;
- hate speech; and
- incitement to terrorism.

---

[16] Adopted on 1 October 1995. The Principles have been endorsed by the UN Special Rapporteur on FOE and have been referred to by the UN Commission on Human Rights in their annual resolutions.
[17] The Tschwane Principles, available at http://osf.to/1jag6nW.
[18] Report of the UN Special Rapporteur on FOE, A17/27, 17 May 2011 and Report of the UN Special Rapporteur on FOE, A/66/290, 10 August 2011.
[19] *Ibid*, para 18.
[20] *Ibid*.

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.[21] 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.

Surveillance of communications

The right to privacy complements and reinforces the right to freedom of expression. The right to privacy is essential for ensuring that individuals are able to freely express themselves, including anonymously,[22] should they so choose. The mass-surveillance of online communications therefore poses significant concerns for both the right to privacy and the right to freedom of expression.

The right to private communications is strongly protected in international law through Article 17 of the ICCPR[23,] which states, *inter alia*, that no one should be subjected to arbitrary or unlawful interference with his privacy, family or correspondence. In **General Comment no. 16** on the right to privacy,[24] the HR Committee clarified that the term "unlawful" means that no interference can take place except in cases envisaged by the law. Interference authorised by States can only take place on the basis of law, which itself must comply with the provisions, aims and objectives the ICCPR. The General Comment further stated that:

> [E]ven with regard to interferences that conform to the Covenant, relevant legislation must specify in detail the precise circumstances in which such interferences may be permitted. A decision to make use of such authorised interference must be made only by that authority designated under the law, and on a case-by-case basis.[25]

The UN Special Rapporteur on the 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:

> Article 17 of the Covenant should also be interpreted as containing the said elements of a permissible limitations test. Restrictions that are not prescribed by law are "unlawful" in the meaning of Article 17, and restrictions that fall short of being necessary or do not serve a legitimate aim constitute "arbitrary" interference with the rights provided under Article 17.[26]

In terms of surveillance (within the context of terrorism, in this instance), he defined the parameters of legitimate restrictions on the right to privacy in the following terms:

---

[21] *Ibid*, para 22.
[22] *Ibid*, para 84.
[23] Article 17 states: "1) 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. 2) Everyone has the right to the protection of the law against such interference or attacks."
[24] HR Committee, General Comment 16, 23rd session, 1988, U.N. Doc. HRI/GEN/1/Rev.1 at 21 (1994).
[25] *Ibid.*, para 8.
[26] Report of the Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism, A/HRC/13/37, 28 December 2009, para 17.

> States may make use of targeted surveillance measures, provided that it is case-specific interference, on the basis of a warrant issued by a judge on the showing of probable cause or reasonable grounds. There must be some factual basis, related to the behaviour of an individual, which justifies the suspicion that he or she may be engaged in preparing a terrorist attack.[27]

The Special Rapporteur on FOE has also observed that:

> The right to privacy can be subject to restrictions or limitations under certain exceptional circumstances. This may include State surveillance measures for the purposes of the administration of criminal justice, prevention of crime or combatting terrorism. However, such interference is permissible only if the criteria for permissible limitations under international human rights law are met. Hence, there must be a law that clearly outlines the conditions whereby individuals' right to privacy can be restricted under exceptional circumstances, and measures encroaching upon this right must be taken on the basis of a specific decision by a State authority expressly empowered by law to do so, usually the judiciary, for the purpose of protecting the rights of others, for example to secure evidence to prevent the commission of a crime, and must respect the principle of proportionality.[28]

Anonymity and encryption

The protection of anonymity is a vital component in protecting the right to freedom of expression as well as other human rights, in particular the right to privacy. A fundamental technology enabling anonymity online is encryption - a mathematical "process of converting messages, information, or data into a form unreadable by anyone except the intended recipient" that protects the confidentiality of content against third-party access or manipulation.[29] Without the authentication techniques derived from encryption, secure online transactions and communication would be impossible.

The right to online anonymity has so far received limited recognition under international law. Traditionally, the protection of anonymity online has been linked to the protection of the right to privacy and personal data. In May 2015, the Special Rapporteur on FOE published his report on encryption and anonymity in the digital age.[30] The report highlighted the following issues in particular:

- Encryption and anonymity must be strongly protected and promoted because they provide the privacy and security necessary for the meaningful exercise of the right to freedom of expression and opinion in the digital age;[31]

- Anonymous speech is necessary for human rights defenders, journalists, and protestors. He noted that any attempt to ban or intercept anonymous communications during protests was an unjustified restriction to the right to freedom of peaceful assembly under the UDHR and the ICCPR.[32] Legislation and regulations protecting human rights defenders and journalists should include provisions that enable access to and provide support for using technologies that would secure their communications;

[27] *Ibid.*, para 21.
[28] Report of the UN Special Rapporteur on FOE, A17/27, 17 May 2011, para 59.
[29] SANS Institute, History of encryption, 2001.
[30] Report of the Special Rapporteur on FOE, A/HRC/29/32, 22 May 2015.
[31] *Ibid,* paras 12,16 and 56.
[32] *Ibid,* para 53.

- Restrictions on encryption and anonymity must meet the three-part test of limitations to the right to freedom of expression under international law.[33] Laws and policies providing for restrictions to encryption or anonymity should be subject to public comment and only be adopted following a regular – rather than fast-track – legislative process. Strong procedural and judicial safeguards should be applied to guarantee the right to due process of any individual whose use of encryption or anonymity is subject to such restriction.[34]

The Special Rapporteur's report also addressed compulsory 'key disclosure' or 'decryption' orders whereby a government may "force corporations to cooperate with Governments, creating serious challenges that implicate individual users online."[35] The report stipulated that such orders should be

- based on publicly accessible law;
- clearly limited in scope and focused on a specific target;
- implemented under independent and impartial judicial authority, in order to preserve the due process rights of targets; and
- only adopted when necessary and when less intrusive means of investigation are not available.[36]

Cybercrime

There is no international standard on cybercrime. Among the regional standards, the 2001 Council of Europe Convention on Cybercrime (the Cybercrime Convention) has become the most recognised and relevant.[37] Although Bangladesh is not a signatory to this Convention, it provides a helpful model for states seeking to develop cybercrime legislation.

The Cybercrime Convention provides definitions for relevant terms, including: computer data, computer systems, traffic data and service providers. It requires States parties to create offences against the confidentiality, integrity and availability of computer systems and computer data; computer-related offences including forgery and fraud; and content-related offences such as the criminalisation of child pornography. The Cybercrime Convention then sets out a number of procedural requirements for the investigation and prosecution of cybercrimes, including preservation orders, production orders and the search and seizure of computer data.

Finally, and importantly, the Convention makes clear that the above measures must respect all conditions and safeguards for the protection of human rights and liberties, consistent with the ICCPR and other applicable international human rights instruments.

[33] *Ibid*, para 56.
[34] *Ibid*, paras 31-35.
[35] *Ibid*, para 45.
[36] *Ibid*.
[37] The Council of Europe Convention on Cybercrime, CETS No. 185, in force since July 2004. As of May 2015, 46 states have ratified the Convention and a further eight states have signed the Convention but have not ratified it.

Analysis of the Draft Act

General Comments

Before laying down our specific concerns, ARTICLE 19 would like to make several general comments about the Draft Act. In particular, we are concerned about

- **High number of offences, including a high number of offences unnecessarily categorized as "terrorism":** We note that the Draft Act introduces an unusually high number of computer-related offences and we question the necessity of this approach. For a comparative perspective, the Bangladesh legislators should consider that the Cybercrime Convention contains only five such offences. The UK Computer Misuse Act 1990, meanwhile, contains just four such offences and to our knowledge there have been no concerns raised that the UK is not properly equipped to deal with cybercrime.[38] In our view, and as detailed further below, all the offences provided for under the Draft Act could be either regrouped and simplified or entirely removed. Further, the Draft Act contains a "terrorism" section which is unnecessary. In general, we believe that the issue of cybercrime could be address as an amendment to the general criminal law rather than in the specific legislation;

- **Disproportionate sanctions:** We are concerned that the offences contained in the Draft Act provide for unduly harsh sentences, including lengthy imprisonment. Moreover, most of the offences do not articulate a significant *mens rea* requirement of "dishonest" intent or the need for "serious" harm to flow from the offence before criminal liability attaches. We would therefore recommend that the sentences available for offences against the confidentiality, integrity and availability of computer data and systems should be reduced to a one-year maximum.[39] In addition, a harm test or 'public interest defence' should be provided for in the Draft Act where appropriate.

- **Lack of procedural safeguards for human rights protections:** Procedural safeguards for human rights protections are markedly absent throughout the Draft Act. There is no reference to Bangladesh's obligations to uphold and protect the right to freedom of expression and other human rights enshrined in international law. The absence of any such provisions could threaten the entire Act's compatibility with international standards and the enforcement of human rights in this area.

- **Excessive police powers:** While ARTICLE 19 does not conduct an exhaustive analysis of all the procedural guarantees afforded in the Draft Act, we observe that it confers excessive discretionary power to relatively low-ranking police officers without judicial oversight. The breadth of these provisions allows officers to bypass any obligation to obtain a court order to conduct search and seizure operations that seriously infringe individual privacy rights. Further, the Draft Act gives investigators broad powers to compel individuals and service providers to not only provide records and access to systems, but, disturbingly, to "assist" in any way asked. These provisions run grossly counter to international standards stipulating that a law may not confer unfettered discretion on any authority for the restriction of freedom of expression.

[38] The UK Computer Misuse Act 1990 (1990 Act) proscribes unauthorised access to computer material, unauthorised access with intent to commit an offence, unauthorised access with intent to impair a computer, and making or supplying articles to commit one of the aforementioned offences.
[39] *C.f.* 1990 Act 3(6).

Recommendations

- Offences should clearly include requirements for "dishonest" intent in their commission as well as for "serious" harm to result before criminal liability attaches;
- The offences punishing "terrorism" should be reorganized into separate sections;
- The Draft Act should provide sufficient safeguards for the protection of human rights and specifically reference international standards;
- All powers conferred upon the police should also be made subject to a court order;
- Public interest defences should be made available to ensure that legitimate whistleblowers acting in good faith are not prosecuted under the Act.

Definitions

In general, ARTICLE 19 welcomes that the Definitions section aims to shed some light upon key operative terms of the Draft Act. In particular, we note that the definition of traffic data is consistent with the definition contained in the Cybercrime Convention. Part I of the Draft Act contains several important definitions, including "lawful access," "digital communication," "traffic data," "computer or digital device," "computer or digital network," "unlawful interception" and "programme."

However, ARTICLE 19 is concerned about the broad definitions of several key terms connected to the prosecution of computer-related crimes, in particular:

- With respect to Section 2(1), the Draft Act does not define what it means for someone to be "entitled to hold full control" to access a "programme or data;"

- In Section 2(2) (defining "unlawful" access), there is no reference to the need for security features to be infringed or for any "dishonest" intent to access data. For this reason "unlawful access" may include forms of access that expose wrongdoing, such as in the case of whistleblowers, without any opportunity for a public interest defence;

- The definition of "critical information infrastructure" in Section 2(3) is concerning for two reasons:
    - *First*, such infrastructures are defined to include those where "immobility or collapse may have an adverse effect on matters relating to the national security, the integrity and sovereignty of the state, economy, and public health." We find the definition of "adverse effect" is overly broad and may catch minor disruptions or losses to information systems. We believe that the definition of damage for the purposes of cybercrime legislation should reflect the fact that only "serious" impairment or losses should attract a criminal sanction. Similarly, we believe that the reference to "adverse effect" on matters relating to "public health" or "public safety" is unduly broad;

    - *Second*, Section 2(3) contains a sub-provision allowing what is deemed "critical information infrastructure" to be "declared by the government." By nature this means it is not defined in law and therefore the sub-provision should be omitted entirely.

- The definition of "damage" in Section 2(5) is too broad and would catch minor disruptions or losses to information systems. In our view, the definition should reflect the fact that only "serious" impairment or losses should attract criminal sanctions;

- The definition of "computer or digital device" in Section 2(9) does not appear intrinsically problematic; we note that it fails to include a reference to "automatic processing of data" which is a key component of the definition of computer systems in the Cybercrime Convention (mentioned here for comparative perspective. It is true that other definitions contained in the Act make reference to "data processing." However, we believe that the definition of "computer system" should make it clear that data processing in this context is "automatic;"

- The definition of "digital or electronic forgery" in Section 2(15) is difficult to understand, especially as "incorrect" and "inappropriate" as used are nowhere defined. We suggest that the Bangladesh legislator could consider the definition of forgery in the Cybercrime Convention[40] and to require some intent that the "inauthentic" data will be acted upon;

- The definition of "digital pornography" in Section 2(16)(a) is problematic. The term "artistic or educational value" is vague and undefined; the prohibition of acting, or even "partially unclothed dance," could conceivably apply to many forms of expression, including dance, film, depictions of music performances, music videos, among others. Moreover, we are concerned that Section 2(16)(b) may unduly limit freedom of expression, and suggest striking it out from the law in its entirety;

- The definition of "obscene" in Section 2(36) is similarly broad.We note that Article 19(3) of the ICCPR allows for limits on freedom of expression for materials in order to protect public morals. However, as noted by the HR Committee in General Comment No 34:

  > [T]he concept of morals derives from many social, philosophical and religious traditions; consequently, limitations ... for the purpose of protecting morals must be based on principles not deriving exclusively from a single tradition. Any such limitations must be understood in the light of universality of human rights and the principle of non-discrimination.[41]

  Also, the UN Siracusa Principles on the Limitation and Derogation of Provisions in the International Covenant on Civil and Political Rights also places limitations on the application of public morality as grounds for limiting expression:

  > Since public morality varies over time and from one culture to another, a state which invokes public morality as a ground for restricting human rights, while enjoying a certain margin of discretion, shall demonstrate that the limitation in question is essential to the maintenance of respect for fundamental values of the community. The margin of discretion left to states does not apply to the rule of non-discrimination as defined in the Covenant.[42]

- We also suggest that the definition of "unlawful interception" in Section 2(22)(b) is more closely aligned with Article 3 of the Cybercrime Convention, which requires "the interception without right, made by technical means, of non-public transmissions of

[40] Council of Europe, Convention on Cybercrime, Nov. 23, 2001, ETS No. 185, Article 7. The Cybercrimes Convention defines "forgery" as "the input, alteration, deletion, or suppression of computer data, resulting in inauthentic data with the intent that it be considered or acted upon for legal purposes as if it were authentic, regardless whether or not the data is directly readable and intelligible."
[41] General Comment No. 34, *op.cit.,* para 32.
[42] UN, Economic and Social Council, U.N. Sub-Commission on Prevention of Discrimination and Protection of Minorities, Siracusa Principles on the Limitation and Derogation of Provisions in the International Covenant on Civil and Political Rights, Annex, U.N. Doc E/CN.4/1984/4 (1984), pp. 17-18.

computer data." Key to the Cybercrime Convention definition is that the interception be made "without right", and that the transmissions are "non-public." The definition as drafted contains no requirement for impediments to information flow to be "serious."

Recommendations:

- The definition of "unlawful access" in Section 2(2) should explicitly require both "dishonest" intent and "infringement of security features" for access to be "unlawful;"
- In Section 2(3) the text "may have an adverse effect on the matters relating to the" should be replaced with "seriously harm;"
- Section 2(3)(b) should be deleted because it allows "critical information infrastructure" to be "declared by the government;"
- Section 2(5), which defines "damage," should include the word "serious" before the words "alteration", "loss" and "obstruction;"
- The definition of "computer system" in Section 2(9) should be revised; in particular, it should make explicit reference to "automatic processing of data;"
- The definition of "forgery" in Section 2(15) should require intent for "inauthentic" data to be acted upon, and the language "incorrect and inappropriate work or procedure" should be removed;
- The definitions of "digital pornography" in Section 2(16) and "obscene" in Section 2(36) should be struck out in their entirety;
- The phrase "creating impediments to the flow of information" in 2(22)(b) should be removed. Alternatively, the word "serious" should be inserted to require "creating serious impediments."

Offences against the critical information structure

Section 9 of the Draft Act criminalizes "any offence against critical information infrastructure." For the reasons stated previously, the definitions of "critical information infrastructure" in Sections 2 and 9 are not formulated with sufficient precision to enable an individual to regulate his or her conduct according to its terms. Article 9 further fails to define what an "offence" entails, nor the nature of the interest the law seeks to protect. There is also no requisite mental state for finding culpability, and the sanctions are unduly harsh.

Recommendations:

- Since Section 9 relies on the underlying definitions in Section 2(3) of critical information infrastructure, those definitions should be amended as recommended above;
- Section 9 should require "dishonest" intent, and its sanctions should be reduced.

Crimes of computer or digital device related forgery

ARTICLE 19 is concerned that Section 10 of the Draft Act is vague, overbroad and restricts freedom of expression beyond what is permissible under international freedom of expression standards. In particular:

- Section 10 makes it a crime to "suppress any information, or publish, or add any new information, or distort information with the intention of harming property." The term "information" as used in Section 10 is nowhere defined. Similarly "harming property" is unduly broad and could apply to minor disruptions. For these reasons, Section 10 does not meet the requirement of legal certainty under Article 19(3) of the ICCPR.

- We are also concerned that vague terms "suppress" or "distort" could proscribe the use

of encryption, which is a necessary tool for secure online transactions, anonymity, and freedom of expression.[43] Criminalising encryption would have a broad chilling effect on legitimate expression.

- In addition to vague wording of Section 10, we are concerned that – given the inclusion of the word "publish" – it could be abused to sanction journalistic activity, security research, and other legitimate expression without legitimate reason. Here, we reiterate that the legislators should consider the wording of Article 7 of the Cybercrime Convention, and in particular the requirement for "dishonest" intent. Noteworthy in the Convention's definition is the requirement of intent for the "inauthentic data" to be acted upon for legal purposes.

Recommendations:
- Section 10 should require "dishonest intent," "serious" harm to property, and eliminate the words "suppress" and "distort;"
- It should require intent for "inauthentic data" to be acted upon for legal purposes;
- The term "publishing" should be removed from offences stipulated in Section 10.

Computer-related fraud

Section 11(1) of the Draft Act punishes the same conduct as Section 10; hence ARTICLE 19 refers to the concerns articulated above.

Section 11(2) punishes with up to five years' imprisonment the sending of an electronic message while "intending to defraud" and "materially misrepresenting any fact", where the recipient "is caused to suffer any damage or loss." We note that these terms are vague and do not meet the requirement of legal certainty stipulated under the three-part test of permitted restrictions under Article 19(3) of the ICCPR.

We observe that – for comparative purposes - Article 8(b) of the Cybercrime Convention, defining fraud, requires there to be "interference" with a computer system and intent to procure "economic benefit for oneself or for another person."[44] These elements are not present in Section 11(2). We recommend that Section 11(2) include this requirement. While Section 11(2) prohibits the misrepresentation of facts, misrepresentation does not require disruption of the function of a computer. Therefore this provision could be used to proscribe conduct that occurs outside cyberspace.

Recommendations:
- Section 11(1) should be amended to require "dishonest intent;"
- Section 11(2) should more closely track Article 8 of the Cybercrime Convention by including a requirement for "interference with the functioning of a computer system" as well as intent to procure "economic benefit for oneself or for another person."

[43] *C.f.* Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, David Kaye A/HRC/29/32, 22 May 2015.

[44] For comparative purposes, Article 8 of the Cybercrime Convention defines "computer-related fraud" as "the causing of a loss of property to another person by: a) any input, alteration, deletion or suppression of computer data; b) any interference with the functioning of a computer system, with fraudulent or dishonest intent of procuring, without right, an economic benefit for oneself or for another person."

Crimes of identity theft and impersonation

Section 12 of the Draft Act punishes any individual who with "intent to deceive or defraud" obtains identity or information or "by intentional forgery impersonates another entity or person" with intent to "gain advantage," "obtain any property" or "cause disadvantage to the entity or person being impersonated." ARTICLE 19 first of all notes that the Cybercrime Convention does not contain a provision for identity theft, and that the conduct proscribed by Section 12 need not occur in cyberspace. The offence of fraud (formulated in Section 11) would seem to adequately cover digital identity theft.

ARTICLE 19 also notes that while these provisions require intent to "deceive or defraud" and "intentional forgery," they do not have any requirement of intent to commit "serious" harm. Absent also is any requirement that the identity information is obtained "unlawfully." As a result, the current formulation of this subsection may be broadly interpreted to achieve less legitimate ends, such as punishing a comedian for impersonating a public figure. This would have a chilling effect on freedom of expression, causing individuals to fear sharing information via digital means.

Recommendations:

- Section 12 should be struck out in its entirety. Should Section 12 be retained, it must at minimum be amended to specify that the conduct must be both intentional and dishonest and that serious harm must result from it. Both reasonableness and public interest defences must be made available.

Crime of digital or cyber terrorism

ARTICLE 19 is concerned that Section 13 of the Draft Act contains several unnecessary offences of broad scope that raise significant issues for freedom of expression. Many offenses that can be punished by other provisions are nevertheless placed under the category of "terrorism." For example, computer access offences are listed under the heading of "terrorism," but the terrorism section is the only section in which "access" offenses appear.

Generally, prohibitions under Section 13(1)(a) require "intent to threaten the unity, integrity or sovereignty of Bangladesh, striking terror into the mind of the people or any section of the people." While there is no internationally agreed definition for terrorism, here the offence of "terrorism" is circularly defined to include the phrase "striking terror" which provides no legal certainty as to the scope of its application. These provisions - which attach severe criminal penalties of up to fourteen years' imprisonment without any requirement of intent to cause actual serious harm - could be used to curtail legitimate public discussion or dissent. In particular:

- Section 13(1)(a)(II) – which criminalizes access to a computer "illegally or without authorization" – does not require circumvention of security measures. Neither does it require "dishonest" intent. As a result this section could be used to punish whistleblowers for exposing information in the public interest.[45] Hypothetically, a

[45] A whistleblower is an individual, who exposes information that he/she reasonably believes, at the time of disclosure, to be true and to constitute a threat or harm to a specified public interest, such as a violation of national or international law, abuse of authority, waste, fraud, or harm to the environment, public health or public safety (see e.g., Report of the Special Rapporteur on FOE, UN Doc. A /70/361, 8 September 2015, para28). Numerous international bodies recognize the importance of protections for whistleblowers who disclose information in the public interest, including the 2015 Report of the Special Rapporteur on FOE (*op.cit,)*, the case law of the European Court (see e.g. *Guja v. Moldova*, App. No. 14277/04, 12 February 2008), the Parliamentary Assembly of the Council of Europe (Parliamentary Assembly of the Council of Europe, Improving the protection of whistle-

whistleblower may be a government employee with initial authorization to access a computer system; the supervisors, however, may determine after-the-fact that the whistleblower was not "authorized" to access a computer system with the intent to disclose information to the public. We reiterate the requirements of Principle 15 of the Johannesburg Principles (see section on international standards). Additionally, this provision might punish the accessing of computer data without authorization for the purposes of testing whether the data kept in a computer system is stored securely. For both these reasons a harm test or 'public interest defence' should be provided.

- Section 13(1)(a)(III) – which criminalizes those who "aid or induce" others to deny access to a computer or "penetrate" a computer - contains no intentionality requirement. As a result the provision could conceivably be used to punish a journalist for his or her relationship with a source who obtained journalistic materials via unauthorized access to a computer system. It is important that the receipt of data, even where initially obtained by unauthorized means, is not an offence. The provision must therefore include a requirement for "dishonest" intent.

- Section 13(1)(g) broadly punishes any person who "spearheads or backs any kind of propaganda campaign against the Liberation War of Bangladesh, spirit of the Liberation War or the Father of the Nation" and deems that person (which can include a foreign citizen) commits a "digital terrorist act." In ARTICLE 19's view, these provisions suffer from the same weaknesses as the rest of the provisions we have already analysed above. The lack of precise definitions of terms employed is a fatal flaw, and mean that this section of the Act does not constitute legitimate restrictions under ICCPR Article 19(3). Section 13(1)(g) is framed broadly enough to punish politically expressive conduct that has no digital component.

Recommendations:

- The Draft Act should not contain a "terrorism" section;
- Sections 13(1)(a)(I)-(III), as well as aiding and abetting, should not be terrorism offenses. These offenses should be placed outside of the heading of "terrorism;"
- After Sections 13(1)(a)(I)-(III) are moved, all three should be amended to require "dishonest" intent;
- After Section 13(1)(a)(I) is moved it should require "serious harm" to result from the offence, and make available a public interest defence;
- The remaining offences under Section 13 should be omitted as they are properly addressed under existing offences. Section 13(1)(g), especially, should be struck out entirely.

Crimes related to violation of privacy

Section 14(1) of the Draft Law punishes any person who with "malicious" intent "captures, publishes or transmits or distorts or keeps the private image of any person without his or her consent." These provisions do not seem to us to be aimed solely at preventing the harassment or intimidation of individuals. The lack of any defence of reasonableness or public interest means that the proposed offence could easily be used to punish individuals engaged in entirely legitimate activities.

---

blowers, document No. 13791, 19 May 2015) or the Organization of American States (see, e.g. Model Law to Facilitate and Encourage the Reporting of Acts of Corruption and to Protect Whistle -blowers and Witnesses, 2013).

Moreover, the provisions punishes not only the capturing of "private images" but also their publication and possession. This would criminalize a reporter receiving private photos or publishing them, which would have a direct chilling effect on freedom of expression. It would also criminalize the possession or publication of private images that were originally obtained with the consent of an individual, such as an individual's former intimate partner. As such, this Section is so vague and overbroad that it is incompatible with the permitted restrictions of freedom of expression under Article 19(3) of the ICCPR.

Recommendations:

- Section 14 should be omitted in its entirety.

Pornography, "child pornography" and related offences

Section 15 of the Draft Act punishes any person who visits, publishes, produces, or preserves "pornographic or obscene material" as well as any person who "publishes or causes to be published an advertisement likely to be understood as conveying that the advertiser distributes or shows pornographic or obscene material."

ARTICLE 19 suggests that all of Section 15(1) be struck out. The definitions of the terms "pornography" and "obscene" as outlined in the Section 2 analysis above are unduly broad, restrictive, and open to subjective interpretation and abuse. Further, Section 15(1) provides no intent requirement at all while proscribing publication, possession, and even visiting content. The provisions in this part of the Act are not limited to the digital context. Pornography is not a form of expression that may be restricted under international law. As noted above, the HR Committee has affirmed that restrictions on freedom of expression for the protection of public morals must be based on a broad understanding of what 'public morals' means.

With respect to Section 15(2), we note that the prevention and prosecution of "child pornography" is an important and legitimate objective, and child sexual abuse images are a type of expression that States are required to prohibit under international law.[46] In this regard, we observe that the provisions of Section 15(2) sufficiently overlap with the definitions contained in Article 9 of the Cybercrime Convention which lays down a commonly agreed definition of offences related child pornography.

Recommendations:

- Section 15(1) should be struck out in its entirety.

Commission of offence by company

Section 16 of the Draft Act imposes broad liability on organizations which commit "any offence under this Act", making "every owner, chief executive, director, manager, secretary, and any other officials … who have direct involvement" liable. Problematically, every individual who is determined to "have direct involvement" shoulders the burden of proof for negating the presumption of guilt: liability attaches "unless it is proved that such offence was committed without his knowledge or he tried his level best to prevent such offence from commission."

[46] *C.f.* the May 2011 Report of the Special Rapporteur, *op.cit.*; and the Cybercrime Convention, Article 9.

ARTICLE 19 considers that this Section threatens to have a profound chilling effect on organizations, which could include media organizations and others who exercise their right to freedom of expression and information. The punishment of individuals for "knowledge" requires significantly looser intentionality than underlying offences. By broadly punishing all members of an organization, this will deter organizations from engaging in legitimate expressive activity.

The Cybercrime Convention in Article 12 contemplates liability for companies in the form of sanctions on the company, where the offence is committed for the company's benefit by an individual exercising "power of representation" or "authority." Those sanctions are not necessarily criminal, and may be "civil" or "administrative."

Recommendations:

- Section 16 should be struck out entirely.

Procedures and investigations

The remaining sections of the Draft Act set out investigatory powers and procedures, including powers of access, search and seizure preservation order, expedited preservation, disclosure of data, production of data, collection of traffic data, interception and forensic tools. ARTICLE 19 does not propose to conduct an exhaustive analysis of this part of the Draft Act, but we do seek to make several important observations for the protection of the rights to privacy and freedom of expression.

Power to enter and examine by Director General and police officer

Section 18(1) grants extraordinarily broad powers to the Director General or any police officer to: "take possession of or access a computer" or "digital network, or any programme" and content on a "removable drive;" to "require any person or organization to disclose traffic information data;" and to "do such other things reasonably which are required for the purpose of this Act." The section is justified for the purpose of "inspection or investigation" of any offence under the Act.

ARTICLE 19 is concerned that this Section grants alarming, sweepingly broad, search powers to potentially any police officer. There is no requirement for the police officer to obtain a warrant or judicial review. The compelled disclosure in Section 18(1)(b) can be used to force providers to disclose associational information such as the senders and recipients of e-mail and SMS messages. Indeed, "traffic data" is defined in Section 2(14) to include any data related to communications, or 'metadata', which includes the "origin, destination, route, time, date, size, duration, or type of underlying service." The provision in Section 18(1)(c),granting authority "to do such other things reasonably which are required for the purpose of this Act", confers a loose, undefined power which could be interpreted to mean almost anything. The ability to solicit outside experts under Section 18(2) threatens to further strip the due process and privacy rights of individuals under investigation.

The compelled disclosure powers in Section 18(1)(b) do not offer adequate safeguards for the protection of sources and journalistic material. In his 2015 report to the General Assembly, the Special Rapporteur on FOE set forth the international standards on protection of sources, observing that compelled disclosure of journalistic source materials must adhere to the three-

part test under Article 19(3).[47] Specifically, he noted that in "the light of the importance attached to source confidentiality, any restrictions must be genuinely exceptional and subject to the highest standards, implemented by judicial authorities only."

Recommendations:

- Section 18 should be struck out entirely. Any investigative police powers of search must be defined, proportionate and, where they implicate the rights and property of individuals, include strict requirements for judicial review.

Duty to assist inspection or investigation

Section 24(1) problematically grants a broad, unrestricted authority to compel individuals and entities to assist with investigations. It requires "any person, entity or service provider … to disclose any information or to assist the investigation officer in investigation." The punishment for non-compliance with any order of an investigating officer is imprisonment for up to two years.

The provision does not provide any definition of or limitation on this stipulated "assistance." Section 24 therefore could be used to circumvent judicial warrant requirements by allowing investigators to simply compel any individual to disclose information they seek. The vagueness of "assist" is especially problematic because it could mean anything from the forced disclosure of records to requiring service providers to become extensions of law enforcement. The latter might involve forcing providers to re-write computer code to insert security 'back doors' into their products or to engage in active surveillance of users.

The 2015 report of the Special Rapporteur on FOE stipulated, in the case of orders for compelled assistance to decrypt communications, that such orders should be: necessary and the least intrusive means available; based on publicly accessible law; clearly limited in scope; focused on a specific target; and implemented under independent and impartial judicial authority.

The HR Committee has held that interceptions of private communications by Governments must be provided for by law, be in accordance with the provisions, aims and objectives of the Covenant and be reasonable in the particular circumstances of the case.[48]

Recommendations:

- Section 24 as written should be struck out. Any orders or compulsion should be in accordance with other portions of the criminal code of Bangladesh, and at a minimum, stipulate minimum judicial review and warrant requirements.

[47] Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, A/70/361, 8 September 2015, para 21.
[48] HR Committee, General Comment 16, 23rd session, 1988, U.N. Doc. HRI/GEN/1/Rev.1 at 21 (1994).

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, 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 Tahmina Rahman, Director of ARTICLE 19 Bangladesh, at tahmina@article19.org.