Bangladesh

Analysis of the Draft Digital Security Bill

May 2018

Centre for Law and Democracy
info@law-democracy.org
+1 902 431-3688
www.law-democracy.org

Table of Contents

Annotated List of Key References

Council of Europe: *Declaration on freedom of communication on the Internet*
The Council of Europe is the key body within the wider European region (i.e. not just the European Union but all of Europe, comprising 47 States) that, among other things, is responsible for promoting human rights. It has a large and complicated system for doing this, of which the European Court of Human Rights (see below) is a key component. Another is the Declarations adopted by the Committee of Ministers, which is comprised of Ministers for Foreign Affairs of member States. Declarations are not binding but are seen as authoritative statements of the standards that flow from binding obligations.

European Court of Human Rights
The European Court of Human Rights was created by the European Convention on Human Rights (adopted 4 November 1950, in force 3 September 1953). It has the power to make binding legal decisions regarding whether States Parties have respected their Convention obligations, including where cases are brought by private individuals (or companies). States are legally obliged to respect its decisions and it has various ways of enforcing compliance.

General Comment No. 34
The UN Human Rights Committee (see below) adopts general comments from time-to-time highlighting its jurisprudence in a specific area in one easily accessible and comprehensive document. General Comment No. 34, adopted in 2011, is its most recent general comment on freedom of expression.

***International Covenant on Civil and Political Rights* (ICCPR)**
The ICCPR[1] is a treaty promulgated by the United Nations General Assembly which is formally legally binding on the 170 States (as of April 2018) that have ratified it (this includes Bangladesh, which ratified the treaty on 6 September 2000). It is the key international human rights treaty setting out civil and political rights.

Special International Mandates on Freedom of Expression: Joint Declarations
Globally, there are four special international mandates on freedom of expression, namely the United Nations (UN) Special Rapporteur on Freedom of Opinion and Expression, 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. Each year, they adopt a Joint Declaration on a freedom of expression issue. While not formally binding, these provide authoritative evidence of the scope and meaning of international guarantees of freedom of expression.

[1] UN General Assembly Resolution 2200A(XXI), adopted 16 December 1966, in force 23 March 1976.

UN Human Rights Committee

The UN Human Rights Committee is the official body which is responsible for overseeing compliance with the ICCPR. When States ratify the ICCPR, they accept this oversight power of the Committee. A key part of this is that they are obliged to submit a report to the Committee every five years on what they have done to implement the treaty and the Committee then adopts its own views on their performance, which are in turn made public. States which have ratified the (first) Optional Protocol to the ICCPR, which does not include Bangladesh, also accept the jurisdiction of the Committee to hear individual complaints about their failure to respect the provisions of the ICCPR.[2]

[2] More information about the Committee is available at: http://www.ohchr.org/EN/HRBodies/CCPR/Pages/CCPRIndex.aspx.

Executive Summary

Earlier this year, the government of Bangladesh approved a Digital Security Bill, 2017 (Bill), which has now been sent to parliament for its review and consideration. The current government, led by the Bangladesh Awami League, has placed considerable emphasis on the role of digital technologies to deliver Vision 2021, the party's political manifesto that, among other things, promises to eradicate poverty in Bangladesh by 2021, 50 years after attaining independence.

However, it has at the same time been supporting legislation that seeks to undue limit freedom to use digital communications technologies. Amendments in 2013 to section 57 of the Information & Communication Technology Act, 2006 significantly exacerbated the problems with this provision, leading to a rash of prosecutions under it. However, the current Bill contains far more and far more problematical provisions which introduce unduly limiting restrictions on digital content, create a number of vastly overbroad other criminal offences relating to digital technologies and give government controlled bodies extensive power over digital communications. The Bill in its current form would have a significant negative impact on journalists and the media, as well as other citizens.

This Analysis assesses the Bill against international human rights standards, in particular relating to freedom of expression, finding that it fails to respect those standards in a number of key respects. International standards dictate, among other things, that content restrictions and other criminal measures should not be vague, overbroad or unnecessary, that parallel regimes for online activities are warranted only where the activity is either completely or substantially different online, that penalties should not be greater simply because an activity is carried out online, and that regulatory systems should be protected against political interference. The Bill fails in important ways to respect all of these standards.

An initial problem is that the Bill employs extremely broad definitions for key terms, including the very central notion of "digital security", which covers all types of security and not just external threats to security, and then grants regulators very broad powers in relation to digital security. Other notions which are defined too broadly include "unlawful access", which covers not only unlawful access but also any access, even if lawful, that prevents a system from sending information, which happens every time someone shuts down a computer. Similarly, "malware" is defined as any programme that changes the tasks performed by a computer, whether or not this is done with intent to harm the computer, which would, as a result, include a user tweaking his or her own settings. Although we presume that these are mistakes, and that individuals will not be charged for shutting down their own computers, the fact that the Bill allows for this means that it could easily be abused.

Another serious problem with the Bill is that, instead of setting out clearly the functions and powers of the bodies it creates, and the procedures for applying the powers it grants, much of this is left to be determined by rules, which will be adopted later by the responsible minister. This includes the "[p]ower, duty and activities" of the Digital Security Agency, the key implementing body for the Bill, which are almost entirely left to be determined by the rules. This not only fails to give citizens appropriate notice of what these powers will be, but it also grants enormous

discretion to the minister to determine how very intrusive powers over online communications will work. It is also inconsistent with established practice in Bangladesh, as well as other democracies, whereby the powers of regulatory bodies are set out in the primary legislation.

The above problem is seriously exacerbated by the fact that the Agency, and its oversight body, the National Digital Security Council, are controlled by government instead of being independent, as international law requires regulatory bodies which have powers in the area of freedom of expression to be. The Bill fails to indicate who will sit on the Council, but it does stipulate that the Chair will be the Prime Minister. The government also constitutes the Agency, appoints its Director General and approves its organigram. The Bill even appears to give law enforcement agencies the power to order the Bangladesh Telecommunications Regulatory Commission to block a range of types of content, instead of granting this power to an independent body.

When it comes to the content restrictions, three general problems keep coming up, with some provisions exhibiting more than one problem at the same time. First, a number of content restrictions are simply not legitimate according to international standards because they prohibit expression that is protected under international law. Obviously these should be removed from the Bill. Second, several content restrictions duplicate restrictions which are already found in existing laws of general application, such as the Penal Code, often with heavier penalties being provided for in the Bill. There have already been amendments to various laws, including the Penal Code, to ensure that it applies to digital means of disseminating content. There is, therefore, no need to duplicate these offences in a specific digital law. There is also no warrant for imposing harsher penalties on digital content than on its offline equivalent. Third, a number of content restrictions are worded too broadly, giving undue discretion to the authorities in how they are applied.

Crossing cutting this is the fact that most of the offences in the Bill, namely 14 out of the 18 separate sections providing for offences, are cognizable and non-bailable. For cognizable offences, the police can make arrests without a judicial warrant, with the result that these rules are far more open to being abused to harass journalists and citizens. For non-bailable offences, once charged an accused will normally be held in detention unless a court, in its discretion, agrees to grant bail. Given that almost all of these offences already fail to conform to international standards, these features are extremely problematical.

The following content restrictions limit forms of expression that are protected under international law:

- Information which “hampers unity, economic activity … religious sentiment” (section 8(2))
- Propaganda “against the Liberation War of Bangladesh or the ideals of the Liberation War or against the Father of the Nation” (section 21) (cognizable and non-bailable)
- “Offensive” information (section 25(1)(a))
- Information that “can make a man corrupt or degraded” (section 25(1)(b))
- Information one knows to be false to “annoy, humiliate … someone” (section 25(1)(c))
- Knowing it to be false or propaganda, publishing information, “either in full or partially distorted to tarnish the image or the good name of the State” (section 25(1)(d))

- Publishing information with the intention and result of hurting "religious values or sentiments" (section 28) (cognizable and non-bailable)

The following content restrictions provide for unduly broad limits on expression:

- Information which "hampers … security, defense … or public order or promote hatred towards a community in the entire country or in part of it" (section 8(2)), because "hamper" and "promote" represent standards which are too low to restrict expression
- Publishing or broadcasting "intimidating" information (section 25(1)(a)), because this does not contain the limits that a prohibition on issuing a threat would have
- Information one knows to be false to "insult someone" (section 25(1)(c)), because this does not contain the defences needed for defamation
- Intentionally publish information that "creates tension or chaos or deteriorate law and order or pose a threat to that effect" (section 31), because the standards associated with these offences are too low (cognizable and non-bailable)

The following content restrictions duplicate provisions that already exist:

- Information which "hampers … security, defense … or public order or promote hatred towards a community in the entire country or in part of it" (section 8(2))
- Commits a crime, as set out in section 499 of the Penal Code, via a website or electronic platform (section 29), which explicitly refers to the Penal Code although this already covers digital defamation
- Intentionally publish information that "creates enmity, hatred amongst related different classes or community or destroy communal harmony or creates tension or chaos or deteriorate law and order or pose a threat to that effect" (section 31) (cognizable and non-bailable)

In some cases the offences described above provide for harsher penalties for crimes committed online. This is particularly evident with the section 29 offence, which is exactly the same offence as under the Penal Code. While the Penal Code only provides for imprisonment for up to two years for defamation, section 29 envisages imprisonment for up to three years, 50% longer. Similarly, section 28, dealing with hurting religious sentiments, provides for seven years' imprisonment, whereas the analogous provisions in the Penal Code provide for only one or two years' imprisonment.

The Bill also includes a large number of offences – in sections 17, 18, 19, 20, 22, 23, 24, 26, 27, 30, 32, 33 and 34 – that are not essentially content related, almost all of which are cognizable and non-bailable. A general problem with most of these provisions is that they fail to stipulate a clear and strong intent requirement, which should therefore, be added to all of them.

Section 38 is essentially positive in nature, providing for protection for service providers as long as they can prove that there were "not aware of the offence or tried its best to prevent the commission of offence". However, this standard is too limited because it is likely to lead to takedowns whenever someone claims content breaches the law. This is because service providers will not be able to verify all of the claims and so will simply take down the content rather than risk taking on liability. Better practice is to protect service providers unless they adopt or intervene in the content, or are ordered by a court to take it down.

Sections 22-24 deal, respectively, with forgery, fraud and fraudulent impersonation and appear to unnecessarily duplicate provisions in the Penal Code, which has extensive provisions dealing with these issues which already appear to cover the commission of these crimes using digital tools.

Sections 17, 18, 32, 33 and 34 all deal with access issues, whether to information or computer systems. While it is legitimate to prohibit intentionally illegal access gained for purposes of causing harm, many of these provisions go beyond this. Clear requirements of intent to cause harm should be added to all of them (or they should simply be removed). In some cases, such as section 34(a), dealing with hacking, the access does not even need to be unlawful, so that changing information in your own computer would be deemed to be hacking. Section 32 deserves special mention because it addresses accessing confidential government information. Better practice in this regard is to impose sanctions only on officials who are under a primary obligation to protect the information, and not to sanction third parties, including journalists, to whom information is leaked. These sorts of rules should also exempt whistleblowers – individuals who expose wrongdoing – from their scope.

Some of the other particularly problematical provisions in this group include:

- Section 20(1), which makes it a crime to change a computer source code, even if one is the owner of the computer
- Section 27(1)(c), which makes it a crime to damage the supply of essential goods, even if one's action is otherwise perfectly legal
- Section 27(1)(d), which makes it a crime intentionally to access a computer which can be used for an act against a friendly foreign country, even though such an act is not in fact committed, which would cover access to almost any computer
- Section 30(1)(a), which makes it a crime to perform an e-transaction, thus apparently ruling out all e-commerce

These problems with both the content and other offences in the Bill are exacerbated by the fact that the penalties for breach of its provisions are, in most cases, very harsh indeed, providing for long prison sentences for content and actions that should not be criminalised in the first place.

The combined effect of the criminal prohibitions in the Bill is very serious indeed. Some provisions appear to have been included by mistake, given how broad and unnecessary they are. Others appear to have been included intentionally, with the goal of giving the government broad grounds to charge individuals with crimes, even though there is no victim and the activity is otherwise perfectly normal. Yet others prohibit types of expression that are protected under international law. These flaws are exacerbated by the lack of independence of the regulators, the power of the government to largely define the mandate and powers of the regulators (which they control), the very harsh penalties for breach of most of the provisions and the fact that most of the offences are cognizable and non-bailable. It is clear that major changes need to be made in the Bill if it is not to become a tool for seriously undermining respect for freedom of expression in Bangladesh.

Introduction

On 29 January 2018, the cabinet of Bangladesh approved the draft Digital Security Bill, 2017 (Bill). The Bill has since been placed before Parliament and then sent to the Parliamentary Standing Committee for scrutiny. The Bill contains a large number of content restrictions and other measures which could be used to limit freedom of expression, and there is some concern that it will indeed be used in this way.[3] This Analysis reviews the Bill based on international standards relating to freedom of expression and better practice in this area by other States, making recommendations for reform of the Bill where this is deemed appropriate.

The Analysis starts with a brief analysis of some of the recent experiences of Bangladesh in this area and in particular with section 57 of the Information & Communication Technology Act, 2006 (ICT Act),[4] which has been used numerous times in recent years to restrict the dissemination of content using digital tools. It then provides a general analysis of the extent to which (new forms of) regulation, and in particular criminal offences, are needed to address digital behaviours. The following parts focus on the specific provisions of the Bill. The first looks at the issue of scope and precision, including what has been left to be clarified in subsequent rules. The next two look at the offences established by the Bill, which take up 21 separate sections, first addressing content restrictions and then other types of offences. The following part focuses on the institutional structures created by the Bill and the extent to which they are independent of government, while the final part looks at a collection of other issues.

The Analysis is based on an unofficial English language translation of the Bill. It seems likely from the language that there are mistakes in this translation. The author takes no responsibility for errors in the Analysis that are based on underlying translation errors.

History of Similar Legislation in Bangladesh

The current government of Bangladesh, led by the Bangladesh Awami League, places considerable emphasis on digital technologies to lead the development process for the nation. This harkens back to Vision 2021, the political manifesto of that party during the 2008 National Elections. Vision 2021 promises that, by 2021, 50 years after attaining independence, Bangladesh will become a middle income country where poverty has been completely eradicated. An important part of this is "Digital Bangladesh", a digital strategy to help transform the nation into a modern economy.[5]

---

[3] See, for example, Mafuz Anam, "Commentary: 'Analogue Law' for 'Digital Bangladesh'", 31 January 2018, *The Daily Star*. Available at: http://www.thedailystar.net/commentary/commentary-analogue-law-digital-bangladesh-1527565.

[4] Act No. 39 of 2006. Available at: http://www.icnl.org/research/library/files/Bangladesh/comm2006.pdf.

[5] See Lutfar Rahman, "Digital Bangladesh: Dreams and reality", *The Daily Star*, 10 March 2015. Available at: https://www.thedailystar.net/supplements/24th-anniversary-the-daily-star-part-1/digital-bangladesh-dreams-and-reality-73118.

However, repressive legislation governing expressive activities online have hindered progress towards this goal. The most important single provision in this regard is section 57 of the ICT Act, which provides, in part:

> **57. Punishment for publishing fake, obscene or defaming information in electronic form.-**
> (1) If any person deliberately publishes or transmits or causes to be published or transmitted in the website or in electronic form any material which is fake and obscene or its effect is such as to tend to deprave and corrupt persons who are likely, having regard to all relevant circumstances, to read, see or hear the matter contained or embodied in it, or causes to deteriorate or creates possibility to deteriorate law and order, prejudice the image of the State or person or causes to hurt or may hurt religious belief or instigate against any person or organization, then this activity of his will be regarded as an offence.

In the original version of the Act, as adopted in 2006, this was a bailable offence (i.e. bail would normally be granted pending trial) and non-congnizable (the police could not act on a complaint without getting approval from the Licensing Authority as defined in the Act). The maximum penalty was ten years' imprisonment and/or a fine of BDT 10,000,000 (approximately USD 120,000). Amendments introduced in 2013 made this offence non-bailable so that, once charged and taken into custody, an accused will be held in detention until and unless a court, in its discretion, agrees to grant bail. Furthermore, the offence was rendered cognizable, so that the police can accept complaints (FIRs or First Information Reports) and arrest the accused without a judicial warrant. This means that it is far more open to being abused to harass citizens. Finally, the system of penalties was substantially revised, with a minimum sentence of seven years' imprisonment being established, alongside a maximum of 14 years, while the fines were retained. These key features – and especially non-bailable status and minimum terms of imprisonment – are normally reserved for the very most serious crimes.

According to a 2017 report by Global Voices Advox, more than 700 cases were filed under the ICT between when it was amended in 2013 and the date of the study, of which 60% were under section 57. Many of the cases seem completely inappropriate as candidates to be dealt with by a provision with a minimum imprisonment sentence of seven years, including one case where a husband and wife both filed cases against each other.[6] According to The Daily Star, 21 journalists were charged under this provision in four months in 2017. Many of the plaintiffs in these cases were officials.[7]

Legitimate and Unnecessary Regulatory Needs

[6] "Bangladesh's ICT Act paved the way for hundreds of lawsuits over online speech", 21 July 2017. Available at: https://www.ifex.org/bangladesh/2017/07/21/ict-act-lawsuits/.
[7] Tuhin Shubhra Adhikary, "The trap of Section 57: 21 journos sued under the controversial section of ICT Act in 4 months; chances of misuse remain" 7 July 2017. Available at: http://www.thedailystar.net/frontpage/bangladesh-ict-act-the-trap-section-of-57-1429336.

The advent of digital communications – whether carried over the Internet, mobile phone networks or other systems – and digital devices – whether computers, phones, tablets or other devices – has fundamentally altered the communications landscape, as well as almost every other aspect of life. The pace of change varies among countries and Bangladesh is rated relatively low in terms of the percentage of the population that has access to the Internet.[8] However, the impact of digital communications in every country in the world is enormously significant.

This, along with the undoubted presence of a vast amount of harmful content online and the Internet being used to commit new and innovative crimes, has naturally raised questions about the need to regulate this 'new' frontier. This is very much an evolving issue even in the most developed countries, with much legislative and regulatory attention being devoted to it, as well as much criticism and even striking down of legislation by courts. Indeed, even the very nature of digital communications tools is in a rapid state of flux. The largest social platform, Facebook, was only founded in 2004, making it a young teenager, while more recent platforms – for example, Snapchat and Instagram were founded in 2010 – are relatively young children.

As a result, it is not possible to give a remotely definitive answer to the question of what needs to be regulated and how. This is rendered significantly more complicated by the fact that most of the main platforms are based in the United States and, despite their global operations, have no physical operational touch in most countries. This, along with the possibility on most platforms of operating under an alias, means that there is often very little countries can do to address problematical behaviour on these platforms beyond cutting them off entirely, which is an extremely intrusive measure.[9]

As a very preliminary point it may be noted that international guarantees of freedom of expression apply online just as they do offline. The UN Human Rights Committee, the official body which is responsible for overseeing compliance with the *International Covenant on Civil and Political Rights* (ICCPR), a treaty ratified by 170 States, adopted General Comment No. 34 on freedom of expression in 2011. In it, the Committee stated:

> Paragraph 2 protects all forms of expression and the means of their dissemination. … They include all forms of audio-visual as well as electronic and internet-based modes of expression.[10]

Despite the evolving debate about regulation of online speech, we can draw some general conclusions about this issue. First, where a wrong that may be committed online is already

[8] For example, this was assessed at 13.2% of the population in 2016, albeit increasing by a rapid 10.4% per year. See http://www.internetlivestats.com/internet-users-by-country/. Much higher figures, of 48.4% by the end of 2017, were given by the Bangladesh Telecommunications Regulatory Commission (BTRC). However, this is cast in some doubt by the fairly reliable figure of only 12.7% Facebook penetration by June 2017, since it seems unlikely that only 25% of those online were using Facebook. See https://www.internetworldstats.com/asia.htm#bd.

[9] Pakistan, for example, banned YouTube for several years until January 2016, in a move that was widely derided in the country and beyond. See, for example, BBC News, "Pakistan unblocks access to YouTube", 18 January 2016. Available at: http://www.bbc.com/news/world-asia-35345872.

[10] General Comment No. 34, 12 September 2011, CCPR/C/GC/34, paragraph 12.

covered by an existing legal provision and the nature of the online wrong is not materially different from its offline manifestation – such as harm to reputation online which is covered by a general law on defamation – there is clearly no warrant for creating a new, specially tailored offence for the online version. Certainly there is no warrant for imposing more stringent limitations on online content. As the Council of Europe's *Declaration on freedom of communication on the Internet* states, in Principle 1:

> Member States should not subject content on the Internet to restrictions which go further than those applied to other means of content delivery.[11]

Penalties normally vary depending on the context and in practice online defamation, such as via a tweet or Facebook post, is often less damaging than offline forms of defamation, such as in a newspaper article or broadcast programme. In many cases, and again defamation serves as a good example, sophisticated regimes for wrongs have been created through both evolved legal provisions and their interpretation by courts over time. This sophistication is normally lacking in a new provision, which can be highly problematical from a freedom of expression perspective. Despite this, States often feel tempted to create these 'duplicate' prohibitions.

Second, where, due to a technicality, the law governing an offline wrong does not apply to its online version, although the nature of the wrong is essentially the same – for example where a rule on defamation refers to writing, speaking, broadcasting and publishing in a way that would not cover emailing – the better approach is normally to amend the original rule rather than to create a new offence. This is, once again, because in many cases established rules, even if not perfect, have been relatively carefully tailored over time to create a reasonable balance between protecting a social value, in this case reputation, and respecting freedom of expression, something new provisions often lack.

Third, there are a small number of online activities which are harmful and which simply do not have offline equivalents, so that the creation of new crimes is necessary. For example, offences like trespass and breaking and entering are simply not analogous to hacking into or illegally accessing a computer system. Spamming and distributed denial-of-service (DDoS) attacks are other examples of uniquely online wrongs. You do need dedicated criminal provisions for these sorts of wrongs.

Fourth, there may also be some cases where we tolerate an offline activity, even though it does cause some harm, but it does need to be regulated online because its nature somehow changes or intensifies when it goes online. There is in some countries a current debate about rules against cyberbullying, although traditional (offline) bullying has been largely tolerated legally, even if there have been social campaigns against it. This is because the scale (number of people that may be involved), persistence (over time, because digital communications can be fairly continuous) and reach (you cannot find a location which is safe from digital communications) of cyberbullying is, at least potentially, much greater than for traditional bullying.

[11] Adopted 28 May 2003. Available at: https://rm.coe.int/16805dfbd5.

Caution in regulating online activities is especially important in relation to the creation of criminal offences, given how intrusive they are. An especial problem here is the chilling effect of a potential penalty of imprisonment, since people will take care to avoid any chance of falling foul of the rule, which may result in them not disseminating even legitimate statements.

Scope and Precision

In many cases, the language used in the Bill is very broad in scope, eschewing more precise, narrow terms. This becomes particularly problematical where powers are granted to regulatory bodies or offences are created. Under international law, and in particular Article 19(3) of the ICCPR, restrictions on freedom of expression are legitimate only if they are "provided by law" which implies not only that a law has been passed by also that it is clear. As the Human Rights Committee noted in General Comment No. 34:

> For the purposes of paragraph 3, a norm, to be characterized as a "law", must be formulated with sufficient precision to enable an individual to regulate his or her conduct accordingly and it must be made accessible to the public. [references omitted][12]

For example, "digital security", clearly a very important concept, which forms the name of the entire law, is defined as the "security of any digital device or digital system". While that may seem like a natural definition, in fact it is extremely broad. Placing a computer near water may represent a threat to digital security, since getting these devices wet normally renders them useless. Creating a poor password for a computer may also be deemed to be a digital security threat.

Operationally, this becomes very important, for example in section 8(1), which gives the Director General of the Digital Security Agency, the key implementing body for the legislation, created by section 5 of the Bill (see below under Institutional Structures and Independence), the power to request the Bangladesh Telecommunication Regulatory Commission (BTRC) to remove or block any information or data that "poses a risk to digital security". As the basis for such a draconian power, a far narrower definition which is only engaged by a more serious threat is needed. Similarly, section 9 establishes a National Computer Emergency Response Team, a group of experts on digital security and law working under the Agency. According to section 9(5)(b), this Team can take "necessary steps to protect the information infrastructure" if digital security is at risk. And again, the National Digital Security Council, an oversight body created by section 12 of the Bill (again, see below under Institutional Structures and Independence), can issue "necessary directives if digital security is at risk" (section 13(2)). In all of these cases, a far narrower definition, with higher minimum thresholds, is needed.

In other cases, careless, often over-inclusive, drafting leads to illogical results. Thus, "unlawful access" includes accessing a computer "without permission", which is fine, but also where "access prevent[s] that information system from sending or receiving information and data or

[12] Note 10, paragraph 25.

suspending or disrupting or stopping its processing" (section 3(q)), without any conditions on the nature of access (i.e. it could even be by the owner of the computer). As such, every time someone closes down their own computer, they fall within the scope of unlawful access. Similarly, "malware" is any programme that "changes … any task performed by a computer or digital device" or "facilitate[s] … automatic access to any digital device". This would include any adjustment to the settings on a digital device (say the speed of a double click to activate a programme or even the toolbars shown at the top of a word processing programme) or setting up automatic sharing of emails between two devices. Clearly these definitions should not go this far.

Other cases of unfortunately broad language are pointed out throughout the analysis below.

Another source of serious imprecision in the Bill is that a wide range of very important issues are left to be set out in the rules which, according to section 61 of the Bill, are formulated by the government via notification in the Gazette.[13] Rules are a form of subordinate legislation which is normally understood as meaning that they should, indeed, be subordinate to the main legislation. Thus, while they may clarify minor issues or set matters that vary over time, such as the fee for an administrative service, important powers and regulatory issues should not be left to the rules. Giving very broad rule-making power to government circumvents the rigorous scrutiny and representation of the people through the members of Parliament which apply to adoption of primary legislation.

In contrast to this, extremely important issues in the Bill are left entirely to the rules. Thus, the draft says very little about the general powers and functions of the Digital Security Agency and, instead, according to section 5(3), the "[p]ower, duty and activities" this body are to be determined by the rules. This is wholly inappropriate; the main powers and responsibilities of such an important body as the Agency should at least be outlined in the primary legislation.

Section 8 grants enormously wide powers to block or remove content, which is a very intrusive power (see below), but says almost nothing about how this will work. Instead, section 8(4) provides: "To fulfill the objective of this section, other relevant matters will be determined by the Rules." Once again, at least a framework of procedures governing the exercise of this power should be set out in the primary legislation.

The National Computer Emergency Response Team is allocated it a number of very general powers, such as to take "necessary measures to prevent possible or upcoming cyber or digital attack". Once again, a catch-all is provided, with section 9(5)(e) providing that the Team shall undertake "[a]ny other activity directed by the Rule." Similarly, important matters relating to the Digital Forensic Lab[14] (sections 10(4) and 11(1)) and the National Digital Security Council (section 13(2)(e)) are left to be determined by the rules.

[13] In practice, rules are normally adopted by the minister who is responsible for an act.

[14] Another body created by the Bill which is described in more detail in the section of this Analysis on Institutional Structures and Independence.

In contrast to this, a review of other laws in Bangladesh covering similar areas which create an authority or agency stipulates the powers and functions of that authority or agency. For example, other specialist agencies working on technical matters, such as the Bangladesh Computer Council, established by section 3 of the Bangladesh Computer Council Act, 1990, have their functions set out clearly in the primary legislation (in that case in section 5 of the Act). Similarly, section 6 of the Bangladesh Telecommunication Act, 2001 establishes the Bangladesh Telecommunication Regulatory Commission, and its objectives, functions and powers are described in great detail respectively in sections 29, 30 and 31. Thus, the Bill deviates from established practice in Bangladesh by failing to define properly the functions and powers of the bodies it creates and, instead, leaving this to be determined by the government.

Recommendations:

- The whole of the Bill should be reviewed and edited so that its definitions and terms are as clear, precise and narrow as possible, especially where they serve as the basis for offences or the grant of power to a regulatory body.
- Rules should be reserved for matters which are properly subordinate to the main legislation, rather than leaving important matters – such as the primary powers and responsibilities of administrative agencies and how these powers are to be exercised – to the rules.

Offences – Content Related

The Bill contains a number of offences governing content which is distributed digitally. In many cases, these duplicate offences already found in the Penal Code, rendering them unnecessary. Furthermore, in some cases, the very nature of the offence is not in line with international standards.

Section 8(2) provides that, if it is "evident to law enforcing agencies" that information published digitally "hampers unity, economic activity, security, defense, religious sentiment or public order or promote hatred towards a community in the entire country or in part of it", then the law enforcing agency can request BTRC to remove or block that information, while section 8(3) provides that BTRC shall either block or remove the content. The removal or blocking of information represents one of the more extreme actions that might be taken in relation to content, analogous to censorship of a newspaper.

Every year, the special international mandates on freedom of expression adopt a Joint Declaration on a freedom of expression issue.[15] Although not formally binding, these

[15] All of the Joint Declarations are available at: http://www.osce.org/fom/66176.

Declarations are highly respected as an authoritative statement of the meaning of international law in the area covered. In their 2017 Joint Declaration on Freedom of Expression and "Fake News", Disinformation and Propaganda, the mandates stated:

> State mandated blocking of entire websites, IP addresses, ports or network protocols is an extreme measure which can only be justified where it is provided by law and is necessary to protect a human right or other legitimate public interest, including in the sense of that it is proportionate, there are no less intrusive alternative measures which would protect the interest and it respects minimum due process guarantees.[16]

There are several problems with section 8(2), including that law enforcement agencies, which presumably includes the police, should not have the power to order content to be taken down. Its exact scope is not clear but section 8(3) suggests that, where it receives a request under section 8(1), BTRC is required ("will") to remove or block the information immediately. If this is correct, it means that law enforcing agency are proposed to be made the sole judge for determining whether information shall be blocked under section 8(2), which is clearly inappropriate. It is not clear how this would be enforced in practice and, in particular, whether BTRC can block just specific information or only whole websites. If the latter, then, at least in theory, the police could claim media content breached section 8(2) with the result that the whole website of a media outlet might be taken down.

To concentrate on content aspects of section 8(2), we note that it is not legitimate to censor content simply because it hampers unity, economic activity or religious sentiment. As generally understood, these are issues about which free public debate, subject to inciting to other crimes, such as violence, should be permitted. Furthermore, as a basis for restricting free speech, these terms are too unclear. For example, if someone posts a story about air pollution leading to a drop in tourism, does that qualify as hampering economic activity? What about a story that suggests that national resources are unduly focused on Dhaka, which may fuel discontent in other parts of the country (hampering unity)? In addition, the threshold for triggering these rules is unduly very low. While blasphemy laws are generally not appropriate as restrictions on freedom of expression under international law (see below), this is all the more so where all that is required is hampering religious sentiment, which seems to reduce the threshold to a case where someone gets upset.

The other restrictions here – namely security, defence, public order and hatred – are legitimate as grounds for restricting expression but we again note that the standard (i.e. "hamper" or "promote") is unduly low. For example, hate speech is addressed directly in Article 20(2) of the ICCPR, which calls on States to ban "incitement" to hatred, and not merely the promotion of it. More generally, Article 19(3) of the ICCPR only allows restrictions on freedom of expression which are necessary, which the term "hamper" would not meet.

Furthermore, all of these issues are already addressed in the Penal Code. Some of the relevant provisions in the Penal Code include the following:

[16] Adopted 3 March 2017, paragraph 1(f).

- Section 123A, addressing defence and security
- Section 336, addressing safety
- Section 505, addressing racial hatred and public order
- Section 505A, addressing public order, security and foreign relations

Section 21 makes it a crime, punishable by up to 14 years' imprisonment and/or BDT 10,000,000 (approximately USD 120,000), through any digital platform, to run or support a campaign or distribute propaganda "against the Liberation War of Bangladesh or the ideals of the Liberation War or against the Father of the Nation".

Article 19(3) of the ICCPR only permits freedom of expression to be restricted in order to protect a limited number of interests, namely for "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". It will immediately be clear that the Liberation War, its ideals and the Father of the Nation do not fall within the scope of these permissible grounds for restriction. As strongly as many Bangladeshis may feel about these issues, it is simply not legitimate to prohibit others from expressing themselves freely about them.

Pursuant to section 54(a) of the Bill, section 21 is a cognizable and non-bailable offence, which significantly exacerbates its already problematical status. In effect, it means that charges can easily be laid, even if there is only scant evidence that an offence has been committed, and that someone would normally be held in detention once charged with the offence, even if the breach of the rules was minor and would be unlikely to lead to the imposition of imprisonment upon conviction.

Section 25 creates a number of offences committed via websites or other digital platforms, including:

- purposefully publishing or broadcasting "offensive or intimidating" information (section 25(1)(a));
- publishing information that "can make a man corrupt or degraded" (section 25(1)(b));
- publishing or broadcasting information one knows to be false to "annoy, humiliate, insult someone" (section 25(1)(c)); or
- knowing it to be false or propaganda, publishing information, "either in full or partially distorted to tarnish the image or the good name of the State" (section 25(1)(d)).

While many of these rules contain legitimate elements, all fall foul of international law rules on freedom of expression. Furthermore, they are already covered by similar provisions in the Penal Code including section 503, dealing with treats, and section 504, dealing with insults and provocation.

Even though this is a bailable offence, so that presumably it is unlikely that someone would be held in detention pending trial, having to defend against a charge like this, even if the accused

eventually wins the case, is still very costly and time consuming. Indeed, one of the problems with overbroad offences is that they may be abused by the powerful to bring cases to harass the media. Even if the cases fail (i.e. are won by the media), they still have a very negative impact on the ability of the media to do its work.

Regarding section 25(1)(a), the European Court of Human Rights has repeatedly made it clear that:

> [F]reedom of expression … is applicable not only to "information" or "ideas" that are favourably received … but also to those which offend, shock or disturb the State or any other sector of the population. Such are the demands of pluralism, tolerance and broadmindedness without which there is no "democratic society".[17]

If States actually banned all speech which offended someone, the scope of freedom of expression would be very limited indeed. It is a little bit more complicated regarding "intimidating" information, because at some point it is legitimate to ban the making of threats against individuals. However, mere intimidation is too low a standard and also lacks the attributes of a true threat, such as that they are made *mala fides*, are directed at specific individuals, and have an illegitimate aim.

Section 25(1)(b) again contains kernels of legitimacy but simply fails to meet international standards. It is not immediately clear what sort of information might make a man corrupt but ultimately this is too vague and general a reference to fit within any of the protected interests under Article 19(3) of the ICCPR. Corruption is a crime, so prohibiting people from inciting others to corruption would be a legitimate restriction, but that is very different (and much narrower in scope). Similarly, every country (including Bangladesh) has a defamation law, but the reference to making a man degraded in section 25(1)(b) is, once again, too general to pass the necessity test in Article 19(3) of the ICCPR.

International law is quite clear as to the issue of whether it is legitimate to ban 'false' information or news. As the special international mandates on freedom of expression stated in their 2017 Joint Declaration on Freedom of Expression and "Fake News", Disinformation and Propaganda:

> General prohibitions on the dissemination of information based on vague and ambiguous ideas, including "false news" or "non-objective information", are incompatible with international standards for restrictions on freedom of expression, as set out in paragraph 1(a), and should be abolished.[18]

Section 25(1)(c) does not prohibit all false information, adding the additional condition that it be sent with the goal of annoying, humiliating or insulting someone. As already noted above, free speech cannot be restricted simply because it is "annoying", which is far less stringent a term even than offensive, let alone shocking or disturbing, all of which the European Court of Human

[17] *Handyside v. the United Kingdom*, 7 December 1976, Application no. 5493/72, para. 49.
[18] Adopted 3 March 2017, paragraph 2(a).

Rights has made clear are protected. Humiliating or insulting are a bit closer to the idea of protection of reputation, which is allowed under international law. However, these terms are not clear and precise enough to meet the standard of "provided by law" in Article 19(3) of the ICCPR, pursuant to which, as noted above, any restriction on freedom of expression must be set out in clear terms. Furthermore, not everything which is humiliating or insulting would fall within the scope of harming reputation. In any case, Bangladesh already has a defamation regime, so that these provisions are unnecessary.

The comment above on "false news" also applies to section 25(1)(d). Like section 25(1)(c), however, this additionally requires the information to be published with the aim of tarnishing "the image or the good name of the State". Article 19(3) does protect the reputations "of others" but this is limited to private actors. As the special international mandates on freedom of expression stated in their 2000 Joint Declaration:

> [T]he State, objects such as flags or symbols, government bodies, and public authorities of all kinds should be prevented from bringing defamation actions.[19]

Similarly, the UN Human Rights Committee stated, in General Comment No. 34: "States parties should not prohibit criticism of institutions, such as the army or the administration."[20]

Section 28 is a typical blasphemy provision, making it an offence to publish information, with the intention and result of hurting "religious values or sentiments". This is again a cognizable and non-bailable offence. It may be noted that an entire chapter, namely Chapter XV, of the Penal Code is dedicated to offences relating to religion. Section 295 makes it an offense to injure or defile a place of worship with intent to insult religion. Section 295A provides for punishment for deliberate and malicious acts intended to outrage religious feelings. Section 296 addresses the issue of disturbing religious assembly and section 298 creates the offence of uttering words, etc., with deliberate intent to wound religious feelings. The punishment for these offences range from one to two years' imprisonment or fine or both, whereas section 28 of the Bill provides for up to seven years' imprisonment.

In its 2011 General Comment No. 34, the UN Human Rights Committee made it clear that blasphemy laws are not, *per se*, legitimate, stating:

> Prohibitions of displays of lack of respect for a religion or other belief system, including blasphemy laws, are incompatible with the Covenant, except in the specific circumstances envisaged in article 20, paragraph 2, of the Covenant. … Nor would it be permissible for such prohibitions to be used to prevent or punish criticism of religious leaders or commentary on religious doctrine and tenets of faith. [references omitted][21]

[19] Adopted 30 November 2000.

[20] Note 10, paragraph 38.

[21] Note 10, paragraph 48.

Article 20(2) of the ICCPR is limited in scope to prohibiting incitement to hatred, discrimination and violence against someone on the basis of, among others, religion. Hurting someone's religious sentiments or values clearly fails to meet this standard.

Section 29 provides that where anyone commits a crime, as set out in section 499 of the Penal Code,[22] via a website or electronic platform, they may be imprisoned for up to three years and/or fined BDT 500,000 (approximately USD 6,000), increasing to five years and BDT 1,000,000 (approximately USD 12,000) for subsequent offences. Section 499 of the Penal Code is a defamation provision which covers statements made by "words either spoken or intended to be read, or by signs or by visible representations". This seems quite broad enough to cover statements made via digital means, raising a question as to why it was felt to be necessary to include section 29 in the Bill at all. It may be noted that pursuant to section 87(a) of the ICT Act, the definition of "document" in the Penal Code was amended to include any "document generated or prepared by electronic machine or technology". While section 499 of the Penal Code does not specifically use the word "document", it should be clear to judges that the broader intention of section 87(a) of the ICT Act was to extend coverage of the Penal Code generally to digital content.

Furthermore, pursuant to section 500 of the Penal Code, defamation attracts a maximum period of imprisonment of two years, quite a bit shorter than section 29 of the Bill. There is no apparent justification for providing for a more severe penalty for defamation committed online than offline. Instead, penalties should be conditioned on all of the circumstances. In addition, under the Bill this is a non-bailable offence, whereas this does not appear to be the case under the Penal Code.

We note that, according to international standards, defamation should not in any case be criminal in nature. As the special international mandates on freedom of expression stated in their 2002 Joint Declaration:

> Criminal defamation is not a justifiable restriction on freedom of expression; all criminal defamation laws should be abolished and replaced, where necessary, with appropriate civil defamation laws.[23]

The UN Human Rights Committee's General Comment 34 did not entirely rule out criminal defamation laws, although it did express concern about them, but it did rule out penal sanctions for defamation, stating:

> States parties should consider the decriminalization of defamation and, in any case, the application of the criminal law should only be countenanced in the most serious of cases and imprisonment is never an appropriate penalty. [references omitted][24]

[22] Act XLV of 1860.
[23] Adopted 10 December 2002.
[24] Note 10, paragraph 47.

Section 31 creates a number of offences within one provision. Specifically, it makes it an offence, intentionally, to publish, digitally, information that "creates enmity, hatred amongst related different classes or community or destroy communal harmony or creates tension or chaos or deteriorate law and order or pose a threat to that effect". It is perhaps appropriate to address the hate speech and public order parts of this separately.

The first relates to the part of this section covering the creation of "enmity, hatred amongst related different classes or community or destroy communal harmony or creates tension". Article 20(2) of the ICCPR deals with this issue as follows:

> Any advocacy of national, racial or religious hatred that constitutes incitement to discrimination, hostility or violence shall be prohibited by law.

This imposes a number of limitations on what should be captured by hate speech rules, as follows:

- It must represent advocacy of hatred, which has been interpreted as meaning that the person needed to have the intention of creating hatred.
- It is limited to national, racial or religious hatred, although in practice many countries do go further than this.
- Only incitement is covered, so that lesser forms of nexus between the speech and the result (such as promoting or encouraging) are not covered.
- Only incitement to the specific results of "discrimination, hostility or violence" is covered, so that other results, such as prejudice, dislike or stereotyping, are not included.

The relevant parts of section 31 of the Bill do require intention, the first condition above. They do not refer to any particular targets of the hatred or enmity, apart from different classes or communities, which is quite broad but, as noted, practice on this varies around the world. Whereas Article 20(2) uses the term "incitement", section 31 refers to creating. It is not immediately clear what the difference is, although creating would appear to be the more stringent term. The results referred to in section 31 are "enmity", "hatred", destroying "communal harmony" and creating "tension". Enmity is often understood as a less intense result than hatred, but there is perhaps there is not a lot of difference between them. Destroying communal harmony is a different sort of notion, but it seems to refer to quite a significant result, and so is perhaps analogous to hatred. The last result, creating tension, is, however, a much less significant result and to this extent section 31 is broader than what is permitted under international law.

Significantly, this sort of wrong is already addressed by section 153(A) of the Penal Code,[25] which makes it an offence to "promote feelings of enmity or hatred between different classes of the citizens". Section 153(A) may be triggered by an even broader set of types of communications than section 499, namely "by words either spoken or written, or by signs, or by visible representations, or otherwise", so that it almost certainly includes online statements. Like section 499, it provides for a less harsh penalty than its Bill counterpart (two years' versus five

[25] See also section 505(d).

years' imprisonment) and again is bailable, unlike section 31 of the Bill. As with defamation, there is no reason to provide for a harsher regime of penalties for online as opposed to offline hate speech.

Recommendations:

- Section 8(2) should not be applied at the request of law enforcement agencies. Instead, only by an independent oversight body, such as the courts.
- The references to unity, economic activity and religious sentiment should be removed from section 8(2), while a higher standard – such as posing a serious risk of substantial harm or inciting – should be applied to the other protected interests, such as national security.
- Section 21 should be removed.
- Section 25 should be removed.
- Section 28 should be removed.
- Section 29 should be removed.
- Section 31 should either be removed or the language should be narrowed in line with the comments above and the sanctions should be brought into line with their counterparts in the Penal Code.

Offences – Other

In addition to content related offences, the Bill creates a large number of other offences, in sections 17, 18, 19, 20, 22, 23, 24, 26, 27, 30, 32, 33 and 34, along with rules about offences in sections 35-38.

Section 38 is essentially a positive provision, inasmuch as it provides protection to a service providers as long as it can prove that it was "not aware of the offence or tried its best to prevent the commission of offence". Unfortunately, the conditions upon which responsibility arises are too broad. For example, if someone complains to a service provider that content in relation to which they provide services is defamatory, are they deemed to be "aware of the offence" if it should ultimately prove that the material is in fact defamatory? The problem with this is that service providers are not legal experts or in a position, unlike traditional publishers, to stand up for the (often vast numbers of) information transactions that run through their services. If they bear a potential risk of liability, then they will simply take action to block or remove the content so as to meet the condition of doing their "best to prevent the commission of offence". In effect, this turns everyone into a censor because all one has to do is make an allegation of illegality in relation to content to have it taken down.

Taking action in the context of a mere allegation of wrongdoing can lead to abusive results. For example, in the United States, in one case someone claiming to have psychic powers objected to YouTube when someone else uploaded a clip from a television programme showing how the actions performed by the psychic could easily be done without any special powers. YouTube not only took the post down but also suspended the person's account for two weeks, until their counter-claim was processed.[26] Fortunately in this case there was at least some sort of reasonably quick remedy, pursuant to YouTube's policies, but the negative impact on freedom of expression was still serious.

To limit this risk, the United States' Communications Decency Act, 1996 provides that what it defines as an "interactive computer service" is not considered to be a publisher when providing services in relation to material produced by third parties, with the result that service providers essentially enjoy broad immunity from legal prosecution in relation to that content.[27] Similarly, in their 2011 Joint Declaration on Freedom of Expression and the Internet, the special international mandates on freedom of expression stated:

> 2. Intermediary Liability
>
> a. No one who simply provides technical Internet services such as providing access, or searching for, or transmission or caching of information, should be liable for content generated by others, which is disseminated using those services, as long as they do not specifically intervene in that content or refuse to obey a court order to remove that content, where they have the capacity to do so ('mere conduit principle').
> b. Consideration should be given to insulating fully other intermediaries, including those mentioned in the preamble, from liability for content generated by others under the same conditions as in paragraph 2(a). At a minimum, intermediaries should not be required to monitor user-generated content and should not be subject to extrajudicial content takedown rules which fail to provide sufficient protection for freedom of expression (which is the case with many of the 'notice and takedown' rules currently being applied).[28]

A second problem with section 38 is that it places the obligation on the service provider to prove that it was not aware of the offence. This reverses the normal criminal law presumption of innocence, which holds that it is for the party bringing a criminal prosecution, normally the State, to prove all of the elements of the offence (including, in this case, that the service provider was aware of the offence).

Three of the offences in this section – namely those found at sections 22-24 – run in parallel to offences that are already found in the Penal Code. These deal, respectively, with forgery, fraud and fraudulent impersonation. Although we have not been able to study it fully, the Penal Code has extensive provisions dealing with these issues and we believe that it is likely that they would already cover the commission of these crimes using digital tools. To the extent that they do not, a

[26] See Jacqui Cheng, "Five examples of lame DMCA takedowns", 16 May 2010. Available at: https://arstechnica.com/tech-policy/2010/05/five-examples-of-lame-dmca-takedowns/.
[27] 47 U.S.C. § 230. Available at: https://www.law.cornell.edu/uscode/text/47/230.
[28] Adopted 1 June 2011.

better approach than creating parallel criminal regimes for online activities, as noted above, would be to tweak the Penal Code provisions so that they do cover online activities.

A number of the other offences in this section – namely those found at sections 17, 18, 32, 33 and 34 – essentially deal with issues relating to accessing digital systems. As noted above, this is an area where the digital world is fundamentally different from the offline world, so that it is necessary to create specialised offences here. The problem with these offences is, then, not that they are illegitimate in their underlying aims and approach, but that they are, in many cases, drafted in a significantly overbroad manner.

The delicacy around unlawful access is that, in the modern digital environment, it can be done innocently and without causing any harm, either by mistake or through automated processes. It is therefore important to have a clear intent requirement and ideally a requirement of causing harm.

Section 17(1)(a) makes it a crime simply to gain unlawful access to "essential information infrastructure", while section 17(1)(b) adds a requirement that the access "damages, or destroys or renders it ineffective". The latter is sufficient and consideration should be given to dropping section 17(1)(a). Alternatively, adding a requirement of intent and/or harm to this section would considerably narrow its scope and still provide effective protection to essential information infrastructure. Section 18 is similar in approach, with section 18(1)(a) applying to any unlawful access to a computer and section 18(1)(b) being limited to cases where that unlawful access was for purposes of committing a crime. Broadening the type of harm in section 18(1)(b) and removing section 18(1)(a), or adding intent and harm requirements to section 18(1)(a) would appropriately narrow the scope of this offence.

Section 32 makes it a crime, while illegally accessing a record, to send or preserve any confidential government information. The problem with this is that it would also cover a journalist or other third party who (otherwise innocently) received leaked information. Under international law, the right balance between openness and secrecy is deemed to be achieved where government is responsible for keeping its own secrets, while third parties should not be held responsible for leaks. In other words, officials may be punished for leaking information but not third parties who receive this information. Of course this does not apply where the third party committed a wrong – such as trespass, breaking and entering or theft – to get the information in the first place.

These sorts of rules can easily be abused. The case of Wa Lone and Kyaw Soe Oo, seasoned Reuters reporters working in Myanmar, illustrates this clearly. The two were known for their hard-hitting stories on the Rakhine crisis. They have been detained since 12 December 2017 under an analogous rule to section 32 in the 1923 Official Secrets Act for possessing confidential information relating to Rakhine state and the work of security forces there. A verified version of the facts is not available , but according to relatives the two had met with previously unknown police officers in a restaurant in Yangon, where they were given some documents. They were

arrested almost immediately afterwards, before they had had a chance even to review the documents.[29] Although the case is perhaps a bit extreme, it does still highlight the risks with this sort of rule.

The special international mandates on freedom of expression clarified the relevant international standards on this in their 2004 Joint Declaration:

> Public authorities and their staff bear sole responsibility for protecting the confidentiality of legitimately secret information under their control. Other individuals, including journalists and civil society representatives, should never be subject to liability for publishing or further disseminating this information, regardless of whether or not it has been leaked to them, unless they committed fraud or another crime to obtain the information.[30]

To avoid this, section 32 should be limited to officials who are under a primary obligation to respect the confidentiality of this information or to third parties who directly, intentionally and illegally access the information.

Section 32 also fails to include a public interest override, whereby officials who leak information in the public interest (whistleblowers), would not be liable. As such, it may be inconsistent with the Public-interest Information Disclosure Act (Provide Protection), 2011.[31] Section 4(1) of that Act provides that whistleblowers can make public interest disclosures, if considered reasonable, to a competent authority. Section 5(2) provides that when making a disclosure of public interest information, no criminal or civil or, where applicable, departmental suit can be filed against the whistleblower.

Protection of whistleblowers is also be consistent with international standards, for example as reflected in the 2015 Joint Declaration on Freedom of Expression and Responses to Conflict Situations of the special international mandates on freedom of expression:

> Individuals who expose wrongdoing, serious maladministration, a breach of human rights, humanitarian law violations or other threats to the overall public interest, for example in terms of safety or the environment, should be protected against legal, administrative or employment-related sanction, even if they have otherwise acted in breach of a binding rule or contract, as long as at the time of the disclosure they had reasonable grounds to believe that the information disclosed was substantially true and exposed wrongdoing or the other threats noted above.[32]

Section 33 is relatively narrow in scope, applying to those who illegally access a computer to preserve, add, deduct, transfer or hand over government information. Once again, however, the

[29] Reuters, "Facts on the arrest of Reuters reporters Wa Lone and Kyaw Soe Oo", 9 January 2018. Available at: https://www.reuters.com/article/us-myanmar-journalists-explainer/facts-on-the-arrest-of-reuters-reporters-wa-lone-and-kyaw-soe-oo-idUSKBN1EY2S4.
[30] Adopted 6 December 2004.
[31] Act No. 7 of 2011. Available at: http://www.mrdibd.org/downloads/Whistleblower_protection_act_2011_English.pdf.
[32] Adopted 15 May 2015, paragraph 5(b).

provision would be improved by adding in a requirement of intent and protection for whistleblowers.

Section 34 deals with hacking into a computer, defined in section 34(a)[33] as destroying, cancelling or changing information in a computer and in section 34(b) as illegally accessing any computer and damaging it. It may be noted that section 34(a) does not even require illegality, so that every single person working on a computer that saved any edited document would be considered to be a hacker. This appears to be an unintentional omission. Section 34(b) does require illegality and also has a harm requirement, which is positive, but, as always, it would be useful to add in a requirement of intent.

The rest of the offences in this section – namely those found at sections 19, 20, 26, 27 and 30 – deal with other issues. Once again, many of these provisions are unduly broad. Section 19 addresses a range of generally harmful activities, but in most cases it does not specify that the computer must not belong to the person in question or that the activity is otherwise unauthorised. If an individual wants to damage their own computer or hire someone else to do so, they have the right to do that. Section 19(1)(a) makes it a crime to collect any data from a computer, which would effectively criminalise the very use of the Internet. Section 19(1)(e) makes it a crime, punishable by up to seven years' imprisonment, to send an unwanted email without the permission of the sender. While this may appear reasonable, in fact it is very common for people to forward, without at least the express consent of the sender, emails to other people who may or may not want to receive them. More limiting conditions are needed here. Spamming, or the indiscriminate dissemination of emails en masse, which blocks up the Internet and is overwhelmingly unwanted, is banned in many countries. Forwarding emails which the sender has explicitly, or clearly implicitly, tagged as confidential could be subject to the recovery of civil damages, for example on the theory of breach of confidence. Section 19(1)(f) makes it a crime to deposit funds in someone else's account by illegally interfering with a computer. This is not *per se* problematical, but it seems odd given that a more serious issue would seem to be the removal of funds from someone's account.

Section 20(1) applies to cases where a person intentionally hides, destroys or changes a computer source code. Once again, this should be limited to cases where the person does not own the computer or otherwise have lawful access to it. It would also be preferable to add in a harm requirement here, so that it would only apply where the change caused damage of some sort.

Section 26 deals with what is commonly known as identity theft. It is not immediately clear why it has been included, since it does not appear to require the use of a digital device to commit the crime. Otherwise, it would, once again, be useful to add in a requirement of intent to this provision.

Section 27 deals with "terrorist activity". Given the very high penalties for breach of its provisions – namely up to 14 years' imprisonment – it is essential that strict intent requirements

[33] There is no primary sub-section number for this provision (i.e. as in 34(1)(a)).

are applied, whether by adding them specifically or through reading them in, to each provision. Section 27(1)(c) includes a rule against damaging or destroying the supply of essential goods and services (which is not defined), but does not appear to be restricted to digital activities, so it is not clear why it has been included in the Bill. It also lacks any requirement that the action was illegal in the first place, so that perfectly legal behaviour which happens to damage the supply of an essential good becomes criminalised. Section 27(1)(d) refers to intentionally or unlawfully accessing a computer or information "which can be used for an act against a friendly relationship with a foreign country or public order or in favor of any foreign country or person or quarter". As a first point here it may be noted that many items "can be used" against public order – such as a kitchen knife – but they should only attract criminal sanction when they are in fact used in that way. A second point is that there is nothing wrong with undertaking acts against friendly States or in favour of a foreign State or person. Indeed, a newspaper article criticising (or praising) a foreign State could be deemed to fall within this and yet it would (normally) be protected by the right to freedom of expression and could easily even be in the public interest.

Section 30(1)(a) makes it a crime to perform any e-transaction, while section 30(1)(b) prohibits e-transactions which the government or Bangladesh Bank have declared to be illegal. Assuming the government and Bangladesh Bank have a separate legal power to declare these transactions to be illegal, the latter is appropriate but the former, i.e. banning any e-transaction, appears to make no sense at all.

Recommendations:

- Section 38 should be amended to provide simply that service providers are not responsible for content as long as they have not intervened in the content or been ordered by a court to remove it. At a minimum, the burden should rest on the party bringing a criminal prosecution against a service provider to show that they were aware of the offence.
- Sections 22-24 should be removed. The provisions on forgery, fraud and fraudulent impersonation in the Penal Code should be reviewed and, if they fail to cover the commission of these crimes online, they should be amended to address that lacunae.
- Sections 17(1)(a) and 18(1)(a) should either be removed (with the types of harm in section 18(1)(b) being expanded) or have intent and harm requirements added.
- Section 32 should be limited in scope to those who are under a primary obligation to respect government confidentiality (i.e. normally officials) and those who directly, illegally and intentionally access it, and it should also include a public interest override to protect whistleblowers.
- An intent requirement should be added to section 33 and it should include protection for whistleblowers.
- Section 34(a) should be removed and an intent requirement should be added to section 34(b).
- Section 19 should apply only where the person does not own the computer in question or have lawful access to it. Section 19(1)(a) should be removed, section 19(1)(e) should be limited in scope along the lines suggested above and consideration should be given to the purpose of section 19(1)(f) and whether or not it is needed.
- Section 20 should be limited in scope to cases where the person does not have lawful access to the computer and where the action causes harm or damage of some sort.
- Consideration should be given to whether section 26 belongs in the Bill at all and, if it is retained, a requirement of intent should be added.
- A clear intent requirement should be added to section 27. Consideration should be given to whether section 27(1)(c) should be included in the Bill. Section 27(1)(d) should either be removed or fundamentally revised so that it focuses on illegitimate activities which should in fact be prohibited.
- Section 30(1)(a) should be removed.

Institutional Structures and Independence

Section 5 of the Bill establishes the Digital Security Agency (Agency) as the key institutional structure for implementing the law and the DSA is, in turn, overseen by the National Digital Security Council (Council), established by section 12. The Bill does not indicate who most of the members of the Council will be or even how they are appointed but it is clear that it is not independent of government because the Chair is the Prime Minister ((section 12(2)). The government also constitutes the Agency, appoints the Director General and approves its organigram (sections 5(1), 6(2) and 7(1)). Two key institutions operate under the Agency, namely the National Computer Emergency Response Team, established by section 9, and the system of digital forensic labs, set out in section 10.

It is difficult to say with precision exactly what these various bodies do because, as noted above, while some general functions and powers are set out in the Bill, important parts of their powers and functions are to be included in the Rules. However, it is clear that these bodies will exercise important regulatory powers over digital communications tools. For example, pursuant to section 8(1), the Director General of the Agency can request BTRC to remove or block digital information if it poses a risk to "digital security", a notion which, as noted above, is defined very broadly. This is a very significant regulatory power. Its exact scope is not clear but, as with section 8(2), noted above, section 8(3) suggests that, where it receives a request under section 8(1), BTRC is required ("will") to remove or block the information immediately.

The Emergency Response Team will, among other things, take "necessary steps to protect the information infrastructure" and "necessary measures to prevent possible or upcoming cyber or digital attack" (sections 9(5)(b) and (c). The digital forensic labs will, among other things, ensure "facilities relating to physical infrastructure" (section 11(2)(b)). The Council will, in addition to adopting directives and setting policy, take "necessary measures to ensure appropriate implementation of this Act and Rules formulated under this Act" (section 13(2)(d)).

While government can legitimately lead on policy issues, advice and protection measures, when it comes to regulatory powers that impact on freedom of expression, the situation is very different. International standards make it quite clear that regulatory activities should always be undertaken by bodies which are independent of government. In their 2015 Joint Declaration on Freedom of Expression and Responses to Conflict Situations, the special international mandates on freedom of expression stated:

> Administrative measures which directly limit freedom of expression … should always be applied by an independent body. This should also normally be the case for administrative measures which indirectly limit freedom of expression and, where this is impossible, for example for security reasons, application of the measures should be overseen by an independent body.[34]

[34] Adopted 15 May 2015, paragraph 4(a).

Recommendation:

- The institutional bodies established by the Bill should either be rendered independent of government or their powers and functions should be limited so as to exclude any regulatory functions.

Other Issues

Section 4 of the Bill seeks to assert broad extra-territorial jurisdiction for Bangladesh regarding its offences over both persons (section 4(1)) and computer systems (section 4(2)). Section 4(1) claims jurisdiction in Bangladesh over any person who commits an offence for which he or she may be convicted under the act. Many of the offences are cast in broad language and do not require any jurisdictional connection to Bangladesh. It is not clear whether other legal rules in Bangladesh may be deemed to limit the scope of this but, otherwise, with this provision Bangladesh would seem to be claiming a right to police the world. It would be useful to make it clear that jurisdiction over persons outside of Bangladesh would be asserted only where the wrong in question was itself linked to Bangladesh. In their 2011 Joint Declaration on Freedom of Expression and the Internet, the special international mandates on freedom of expression stated:

> Jurisdiction in legal cases relating to Internet content should be restricted to States to which those cases have a real and substantial connection, normally because the author is established there, the content is uploaded there and/or the content is specifically directed at that State. Private parties should only be able to bring a case in a given jurisdiction where they can establish that they have suffered substantial harm in that jurisdiction (rule against 'libel tourism').[35]

Chapter 7 (sections 39-55) introduces a detailed regime for investigating and trying offences under the act. These include rules about who shall investigation, time limits for this, powers, search and seizure, trials and so on. In some cases – such as section 50, which provides that trials and appeals shall be conducted by the Cyber Tribunals and Cyber Appellate Tribunals established, respectively, under sections 68 and 82 of the ICT Act – these provisions are clearly needed to establish special systems under the act. However, in other cases, it is not clear why special rules are needed and why the general rules which are normally applicable to criminial investigations would not suffice. It is beyond the scope of this Analysis to go through all of these provisions in detail to assess their relevance, but it does seem that many may not be needed. For example, section 40(1)(a) states that the investigation officer will complete his or her investigation within 60 days, but it is not immediately apparent why the normal rules regarding investigations would not suffice here.

The provisions on penalties for the various offences created by sections 17-34 represent an important part of the whole length of the Bill. In many cases the provisions are identical, such as

[35] Adopted 1 June 2011, paragraph 4(a).

for sections 22, 23, 24, 26, 30 and 31 so that, at a minimum, these could be brought together. Consideration could also be given to consolidating the number of different penalties into two or three different options, again leading to significant reductions in complexity and length.

Consideration should also be given to reducing the often very lengthy maximum sentences provided for in these rules. One (section 18(1)(a)) has a maximum of just one year but the rest range from three to five to seven to 14 years for a first offence. These are very heavy penalties for what are in many cases relatively minor wrongs. While we recognise that judges have the discretion to levy lighter sentences, the very possibility of a longer sentence is likely to exert a chilling effect.

Recommendations:

- Section 4(1) should be amended to make it clear that it only applies to offences where the wrong is itself linked to Bangladesh.
- The provisions in Chapter 7 should be reviewed to establish that special systems really are needed to ensure respect for the act and, where this is not the case, the provisions should be removed.
- Consideration should be given to simplifying and consolidating the provisions on penalties, which currently take up a lot of space in the Bill.
- Consideration should also be given to moving towards shorter maximum imprisonment penalties for all but the most serious crimes.