ARTICLE 19

Bangladesh: Analysis of Information Communication Technology Act

April 2016

Legal analysis

Executive summary

In April 2016, ARTICLE 19 analysed the Information and Communication Technology Act, 2006 (ICT Act). The analysis examines the most problematic aspects of both laws from the perspective of international human rights standards, in particular the right to freedom of expression and privacy.

In the analysis, ARTICLE 19 concludes that several provisions of this law are too vague or unnecessarily criminalise legitimate expression. The same is true of provisions granting investigatory powers to the authorities or imposing obligations on service providers for the purposes of assisting the investigation of cybercrimes. Procedural or public interest safeguards are also missing. We therefore recommend that a number of provisions must be either repealed or substantially reviewed to be compatible with international standards in this area.

Key recommendations:

- Clauses 46 and 57 of the ICT Act should be repealed in their entirety;
- Clause 63 which deals with certain violations of privacy should be reviewed and clarified. In particular, a public interest disclosure exemption should be added. Furthermore, the scope of clause 63 should be more clearly limited to public officials.
- The protection of personal data undergoing automated processing should properly be addressed as part of comprehensive data protection legislation.

Table of contents

Introduction

In August 2015, ARTICLE 19 analysed the Information and Communication Technology Act, 2006 (ICT Act).[1] The analysis examines the most problematic aspects of both laws from the perspective of international human rights standards, in particular the right to freedom of expression and privacy.

The ICT Act was passed by the Bangladesh Parliament in 2006[2] with the aim of implementing the National Information and Communication Technology Policy 2002 (The 2002 Policy). The Policy called for legislation to protect against cybercrime[3] and formulate new laws and amend existing ones to ensure security of data and freedom of information.[4] The Cyber-security Bill is being currently considered in the Parliament and it complements, rather than replaces the controversial ICT Act 2006.

ARTICLE 19 is well place to undertake this analysis thanks to our extensive experience of working on freedom of expression issues, including working on issues related to the protection of freedom of expression online. We have analysed several cybercrime laws from around the world including in Kenya[5], Brazil[6], Iran[7], Pakistan[8] and Cambodia.[9] In Bangladesh ARTICLE 19 has been consistently working on different fronts to defend freedom of online expression for the last few years. These include our submissions to the Human Rights Council in 2012 for the second cycle of Universal Periodic Review on Bangladesh. Our report highlighted restrictions on internet expression. In 2013 our Bangladesh Country Report raised concerns on the application of Section 57 especially in view of the amendments made by the ICT Amendment Act 2013. In the same year in collaboration with several civil society organisations we organised a Roundtable on the implications of the amendment on freedom of expression. In our 2014 Report we stressed that criminalisation of online expression has continued with the application of Section 57 of the ICT Act.

The analysis not only highlights concerns and conflicts with international human rights standards within both pieces of legislation but also actively seeks to offer constructive recommendations on how they can be improved. We urge the Bangladesh legislator to consider these recommendations and bring both laws in full compliance with international standards.

[1] ARTICLE 19's analysis is based on English translations of these laws. ARTICLE 19 does not take responsibility for the accuracy of the translation or for comments made on the basis of any inaccuracies in the translation.
[2] Act No. 39 of 2006.
[3] Paragraph 3.7.2.
[4] Paragraph 3.7.4.
[5] ARTICLE 19, Kenya: Cybercrime and Computer Related Crimes Bill, July 2014, available at http://bit.ly/1HOPICH.
[6] ARTICLE 19, Brazil: Draft Cybercrimes Law, January 2012.
[7] ARTICLE 19, Islamic Republic of Iran: Computer Crimes Law, 2012.
[8] ARTICLE 19 and Digital Rights Foundation Pakistan, Pakistan: New Cybercrime Bill Threatens the Rights to Privacy and Free Expression, 2014, available at http://bit.ly/1G1LSrh.
[9] ARTICLE 19, Cambodia: Secret Draft Cybercrime Law seeks to undermine free speech online, April 2014.

International standards on freedom of expression and privacy

The right to freedom of expression

The right to freedom of expression is protected by a number of international human rights instruments that are binding on Bangladesh; in particular, Article 19 of **the Universal Declaration of Human Rights** (UDHR)[10] and Article 19 of **the International Covenant on Civil and Political Rights** (ICCPR)[11] that elaborates upon and gives legal force to many of the rights articulated in the UDHR. Bangladesh acceded to the ICCPR on 06 September 2000 and is therefore legally bound to respect and to ensure the right to freedom of expression as contained in Article 19 of the ICCPR.

In September 2011, the UN Human Rights Committee (HR Committee), as treaty monitoring body for the ICCPR, issued **General Comment No 34** in relation to Article 19.[12] General Comment No.34 constitutes an authoritative interpretation of the minimum standards guaranteed by Article 19 ICCPR. General Comment No 34 states that Article 19 ICCPR protects all forms of expression and the means of their dissemination, including all forms of electronic and Internet-based modes of expression.[13] In other words, the protection of freedom of expression applies online in the same way as it applies offline. At the same time, General Comment No 34 requires States party to the ICCPR 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.[14] In particular, the legal framework regulating the mass media should take into account the differences between the print and broadcast media and the Internet, while also noting the ways in which media converge.[15]

Similarly, the four special mandates for the protection of freedom of expression, including the African Special Rapporteur on Freedom of Expression and Access to Information, have highlighted in the **2011 Joint Declaration on Freedom of Expression and the Internet** that regulatory approaches in the telecommunications and broadcasting sectors cannot simply be transferred to the Internet.[16] In particular, they recommend the development of tailored approaches for responding to illegal content online, while pointing out that specific restrictions for material disseminated over the Internet are unnecessary.[17] They also promote the use of self-regulation as an effective tool in redressing harmful speech.[18]

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 ICCPR as interpreted by the HR Committee and that they are in line with the special mandates' recommendations.

---

[10] UN General Assembly Resolution 217A(III), adopted 10 December 1948. The UDHR is not directly binding on states; however, parts of it, including Article 19, are widely regarded as having acquired legal force as customary international law since its adoption; see, e.g. *Filartiga v. Pena-Irala*, 630 F. 2d 876 (1980) (US Circuit Court of Appeals, 2nd circuit).
[11] GA res. 2200A (XXI), 21 UN GAOR Supp. (No. 16) at 52, UN Doc.
[12] General Comment 34, CCPR/C/GC/3.
[13] *Ibid.*, para. 12.
[14] *Ibid.*, para. 17.
[15] *Ibid.*, para. 39.
[16] Joint Declaration on Freedom of Expression and the Internet, June 2011.
[17] *Ibid.*
[18] *Ibid.*

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. Article 19(3) of the ICCPR permits the right to be restricted in the following respects:

> The exercise of the rights provided for in paragraph 2 of this article carries with it special duties and responsibilities. It may therefore be subject to certain restrictions, but these shall only be such as are provided by law and are necessary:
> (a) For respect of the rights or reputations of others;
> (b) For the protection of national security or of public order, or of public health or morals.

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

- be provided by law, i.e. formulated with sufficient precision to enable an individual to regulate his or her conduct accordingly;[19]
- pursue a legitimate aim as exhaustively enumerated in Article 19(3)(a) and (b) of the ICCPR; and
- conform to the strict tests of necessity and proportionality, i.e. if a less intrusive measure is capable of achieving the same purpose as a more restrictive one, the least restrictive measure must be applied.[20]

The same principles apply to electronic forms of communication or expression disseminated over the Internet. In particular, in General Comment No. 34, the HR Committee has said that:

> 43. Any restrictions on the operation of websites, blogs or any other Internet-based, electronic or other such information dissemination system, including systems to support such communication, such as Internet service providers or search engines, are only permissible to the extent that they are compatible with paragraph 3. Permissible restrictions generally should be content-specific; generic bans on the operation of certain sites and systems are not compatible with paragraph 3. It is also inconsistent with paragraph 3 to prohibit a site or an information dissemination system from publishing material solely on the basis that it may be critical of the government or the political social system espoused by the government.[21]

Further limitations on the right to freedom of expression are stipulated in Article 20 para 2 of the ICCPR which requires states to prohibit "any *advocacy* of national, racial or religious hatred that constitutes *incitement* to discrimination, hostility or violence shall be prohibited by law." Article 20 para 2 of the ICCPR does not require States to prohibit all negative statements towards national groups, races and religions. However, States should be obliged to prohibit the advocacy of hatred that constitutes incitement to discrimination, hostility or violence. "Prohibition" allows three types of sanction: civil, administrative or, as a last resort, criminal. The same principles apply to electronic forms of communication or expression disseminated over the Internet.[22]

---

[19] HR Committee, *L.M. de Groot v. The Netherlands*, No. 578/1994, UN Doc. CCPR/C/54/D/578/1994 (1995).
[20] HR Committee, *Velichkin v. Belarus*, No. 1022/2001, UN Doc. CCPR/C/85/D/1022/2001 (2005).
[21] HR Committee, Concluding Observations on the Syrian Arab Republic (CCPR/CO/84/SYR).
[22] General Comment 34, op.cit., para 43.

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 in two reports in 2011 (in May[23] and August[24]). In the latter, the Special Rapporteur also clarified the scope of legitimate restrictions on different types of expression online.[25] In August 2011 report, 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.[26]

In particular, the Special Rapporteur clarified that the only exceptional 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.

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. [27] In other words, these laws must also comply with the three-part test outlined above. For example, legislation prohibiting the dissemination of child pornography over the Internet through the use of blocking and filtering technologies is not immune from those requirements.

The Special Rapporteur also highlighted his concern that a large number of domestic provisions seeking to outlaw hate speech are unduly vague, in breach of international standards for the protection of freedom of expression. This includes expressions such as combating "incitement to religious unrest", "promoting division between religious believers and non-believers", "defamation of religion," "inciting to violation," "instigating hatred and disrespect against the ruling regime," "inciting subversion of state power" and "offences that damage public tranquility."

The Special Rapporteur further clarified which online restrictions are, in his view, impermissible under international law. In particular, he called upon States to provide full details regarding the necessity and justification for blocking a particular website, stressing that "determination of what content should be blocked should be undertaken by a competent judicial authority or a body which is independent of any political, commercial, or other unwarranted influences to ensure that blocking is not used as a means of censorship." [28]

---

[23] UN Special Rapporteur on Freedom of Expression, May 2011.
[24] Report of the Special Rapporteur on Freedom of Expression, A/66/290, 10 August 2011, para. 16.
[25] *Ibid.*, para.18.
[26] *Ibid.*
[27] *Ibid,* para. 22
[28] *Ibid.*, para. 38

Finally, the Special Rapporteur stressed that all other types of expression, such as defamatory comments, should not be criminalized. Rather, States should promote the use of more speech to combat offensive speech. In this regard, it is worth mentioning that with new Web 2.0 types of applications, including the comment section on newspapers websites, blogs, online chat rooms etc., it is now possible to respond to online derogatory comments almost immediately at no cost. For this reason, the Special Rapporteur remarked that the sanctions available for offline defamation and similar offences may well be unnecessary and disproportionate. [29]

Role of Internet intermediaries and intermediary liability

Intermediaries, such as Internet Service Providers (ISPs), search engines, social media platforms and web hosts, play a crucial role in relation to access to the Internet and transmission of third party content. They have come to be seen as the gatekeepers of the Internet. For Internet activists, they are key enablers of the meaningful exercise of the right to freedom of expression, facilitating the free flow of information and ideas worldwide, while law enforcement agencies view them as central to any strategy to combat online criminal activity.

Given the huge amount of information that is available on the Internet, and that could potentially be unlawful, e.g. copyright law, defamation laws, hate speech laws, criminal laws for the protection of children against child pornography, Internet intermediaries have had a strong interest in seeking immunity from liability on the Internet.

In many western countries, Internet intermediaries have been granted immunity for third-party content.[30] They have also been exempted from monitoring content.[31] However, they have been made subject to 'notice and take-down' procedures, which give them a strong incentive to remove content once they are put on notice by private parties or law enforcement agencies that a particular content is unlawful, lest they face liability for that content. This system can be found for example in the E-commerce directive in the EU and the Digital Copyright Millennium Act 1998 (the so-called 'safe harbours') in the US.

A number of problems have been identified in relation to such 'notice and take-down' procedures, including their lack of clear legal basis [32] and basic fairness. Rather than obtain a court order requiring the intermediary to remove unlawful material (which, in principle at least, would involve an independent judicial determination that the material is indeed

[29] *Ibid.*, para. 28.
[30] See for example, the Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market, the 'E-commerce directive' in the EU. See also the Communications Decency Act 1996 in the US, and in Singapore, the Electronic Transaction Act 2010 which gives strong protection to innocent providers.
[31] See Article 15 of the E-commerce directive. In the case of *SABAM v. Scarlet Extended SA,* the Court of Justice of the European Union (CJEU) considered that an injunction requiring an ISP to install a filtering system to make it absolutely impossible for its customers to send or receive files containing musical works using peer-to-peer software without the permission of the rights holders would oblige it to actively monitor all the data relating to each of its customers, which would be in breach of the right to privacy and the right to freedom to receive or impart information. The court noted that such an injunction could potentially undermine freedom of information since the suggested filtering system might not distinguish adequately between unlawful content and lawful content, with the result that its introduction could lead to the blocking of lawful communications.
[32] OSCE report, Freedom of Expression and the Internet, July 2011, p 30.

unlawful), internet intermediaries are given an incentive to act merely on the say-so of a private party or public body. As the Special Rapporteur on freedom of expression noted:[33]

> 42. [W]hile a notice-and-takedown system is one way to prevent intermediaries from actively engaging in or encouraging unlawful behaviour on their services, it is subject to abuse by both State and private actors. Users who are notified by the service provider that their content has been flagged as unlawful often have little recourse or few resources to challenge the takedown. Moreover, **given that intermediaries may still be held financially or in some cases criminally liable if they do not remove content upon receipt of notification by users regarding unlawful content, they are inclined to err on the side of safety by overcensoring potentially illegal content**. Lack of transparency in the intermediaries' decision-making process also often obscures discriminatory practices or political pressure affecting the companies' decisions. Furthermore, intermediaries, as private entities, are not best placed to make the determination of whether a particular content is illegal, which requires careful balancing of competing interests and consideration of defences. (Emphasis added)

Accordingly, the four special rapporteurs on freedom of expression recommended in their 2011 Joint Declaration on Freedom of Expression and the Internet that:

> (i) No one should be liable for content produced by others when providing technical services, such as providing access, searching for, or transmission or caching of information;[34]
> (ii) Liability should only be incurred if the intermediary has specifically intervened in the content, which is published online;[35]
> (iii) ISPs and other intermediaries should only be required to take down content following a court order, contrary to the practice of notice and takedown.[36]

Surveillance of communications

Guaranteeing the right to privacy in online communications is essential for ensuring that individuals have the confidence to freely exercise their right to freedom of expression. The mass-surveillance of online communications therefore poses significant concerns for both the right to privacy and the right to freedom of expression.

The right of private communications is strongly protected in international law through Article 17 of the ICCPR, which states that:

> 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.

In **General Comment No. 16 on the right to privac**y, the HR Committee clarified that:

---

[33] May 2011 report, *op.cit*, para. 42.
[34] *Ibid.*
[35] *Ibid.*
[36] *Ibid.*

> 3. The term "unlawful" means that no interference can take place except in cases envisaged by the law. Interference authorized by States can only take place on the basis of law, which itself must comply with the provisions, aims and objectives of the Covenant.

The Committee went on to explain that:

> 4. The expression "arbitrary interference" is also relevant to the protection of the right provided for in article 17. In the Committee's view the expression "arbitrary interference" can also extend to interference provided for under the law. The introduction of the concept of arbitrariness is intended to guarantee that even interference provided for by law should be in accordance with the provisions, aims and objectives of the Covenant and should be, in any event, reasonable in the particular circumstances.

The Committee further stated that:

> 8. Even 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 authorized interference must be made only by the authority designated under the law, and on a case-by-case basis.

The UN Special Rapporteur on promotion and protection of human rights and fundamental freedoms while countering terrorism has argued that like restrictions on the right to freedom of expression under Article 19, restrictions of the right to privacy under Article 17 of the ICCPR should be interpreted as subject to the three-part test: [37]

> [A]rticle 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.

The Special Rapporteur further defined the scope of legitimate restrictions on the right to privacy as follows: [38]

> 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 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 there must be "on the basis of a warrant issued by a judge on 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.

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

> 53. [T]he Internet also presents new tools and mechanisms through which both State and private actors can monitor and collect information about individuals'

[37] Report of the Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism, Martin Scheinin, A/HRC/13/37, 28 December 2009.
[38] *Ibid.*, para. 21

> communications and activities on the Internet. Such practices can constitute a violation of the Internet users' right to privacy, and, by undermining people's confidence and security on the Internet, impede the free flow of information and ideas online.

He also further noted that:

> 59. [T]he right to privacy can be subject to restrictions or limitations under certain exceptional circumstances. This may include State surveillance measures for the purposes of administration of criminal justice, prevention of crime or combating 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.

In particular, the Special Rapporteur recommended that States should ensure that individuals can express themselves anonymously online and to refrain from adopting real-name registration systems.[39]

Cybercrime

The Council of Europe Convention on Cybercrime CETS No. 185 (also known as the Budapest Convention) is the only binding international instrument in this area.[40] It was adopted in 2001 and has been ratified by 42 countries, including the United States, Australia and Panama, and signed by another 11 countries. The Convention provides helpful guidance on how to draft cybercrime legislation in accordance with human rights standards. In particular, it contains basic definitions, including a definition of computer data, computer system, traffic data and service provider.

The Convention further requires its signatory parties to create offences against the confidentiality, integrity and availability of computer systems and computer data, computer-related offences such as forgery and content-related offences such as the criminalisation of child pornography. In addition, the Convention mandates the adoption of a number of procedural measures to investigate and prosecute cybercrimes, including preservation orders, production orders and search and seizure of computer data.

Finally, and importantly, the Convention makes clear that the above measures must respect the conditions and safeguards for the protection of human rights consistent with the Contracting parties' obligations under ICCPR and the European Convention on Human Rights.

---

[39] *Ibid.*, para 84.

[40] The Council of Europe Convention on Cybercrime, CETS No. 185. 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 ICT Act 2006

Introduction

The ICT Act is divided into nine chapters:

- Chapters I to VII and IX of the ICT Act are largely definitional, laying down the basic rules governing e-commerce and online transactions, including the legal recognition of digital signatures (chapters II-IV, Sections 5-17) and the regulation of certification authorities (chapter V, Sections 18-40). In this respect, the ICT Act largely follows the UN Commission on International Trade (the UNCITRAL) Model Law on Electronic Commerce, 1996 and the UNCITRAL Model Law on Electronic Signatures, 2001.

- In addition, Chapter VIII of the ICT Act provides for a number of offences as well as the way in which these offences should be prosecuted and tried. These include:
  - **computer misuse**, including damage to computer/ computer systems (Section 54), tampering with computer source codes (Section 55), hacking a computer system (Section 56) and unauthorised access to protected systems (Section 61)
  - **regulatory offences** for failing to comply with licensing or other requirements under the Act, including failure to surrender a licence (Section 58), failure to comply with orders made by the controller in an emergency (Section 60) ; and
  - **online speech-offences** adapted from offline 'crimes' such as the publication of fake, obscene or defamatory information in electronic form (Section 57), the disclosure of private information in breach of privacy (Section 63) or using computers for committing an offence (Section 66).

In 2013, the ICT Act was amended by the Information and Communication Technology (Amendment) Act 2013.[41] Among other things, the 2013 Act lifted a number of procedural restrictions on the ability of the authorities to arrest individuals suspected of having committed an offence under the 2006 ICT Act without a warrant during the investigation of those crimes.[42] In other words, the 2013 Act facilitated the prosecution of offences under the 2006 Act and made it more prone to abuse, particularly as regards the prosecution of speech offences.[43]

In this analysis, however, ARTICLE 19 focuses on Chapter VIII of the ICT Act. Specifically, we examine Sections 57 and 63 of the Act, which are primarily concerned with speech offences. We also analyse Section 46 of the Act, which seems to have provided the basis for website blocking in Bangladesh. We conclude that, as a minimum, Sections 46 and 57 should be repealed on the basis that they are incompatible with international standards on freedom of expression. Section 63 should be clarified in order to meet the standards of legal clarity required international law.

[41] The Information and Communication Technology (Amendment) Act 2013 (Act No. 42 of 2013).
[42] Section 8(b).
[43] Sections 6 and 7.

Lack of clarity over the powers of the controller

Section 46 of the Act provides for the power of a controller to give directions in an emergency. Under Section 19, 'controllers' are defined by reference to their functions, which essentially consist in overseeing the activities of certifying authorities, which are themselves tasked with issuing digital signature certificates. Controllers are appointed by and accountable to the government.[44]

Section 46 of the Act provides that:

> (1) If the controller is satisfied that it is necessary or expedient so to do in the interest of the sovereignty, integrity, or security of Bangladesh, friendly relations of Bangladesh with other States, public order or for preventing incitement to commission of any cognisable offence, for reasons to be recorded in writing, by order, direct any agency of the Government to restrict transmission of any information through any computer resource.
>
> (2) The subscriber or any person in charge of a computer resource shall, when called upon by any agency to which direction has been issued under sub-section (1) of this section, extend all facilities and technical assistance to decrypt the information.

ARTICLE 19 notes that Section 46 has apparently been relied upon in Bangladesh to justify the legality of website blocking in the country.[45] In our view, this provision is deeply problematic for several reasons, in particular:

- **Overly broad discretionary powers of the controller**: in any event, these powers are couched in inappropriately broad language. While the title of Section 46 suggests that the power is only to be exercised in an emergency, it fails to define what constitutes "emergency." Instead, it refers to a number of broad purposes, some of which are not recognised as legitimate under Article 19 (3) ICCPR, such as maintaining "friendly relations"' with other States or the "prevention of incitement to the commission of cognizable offences." In other words, Section 46 confers an unfettered power on a public authority (the controller) to conduct surveillance or block access to information in an incredibly wide range of circumstances. The potential for abuse is obvious.

- **Inappropriate authority**: in addition to the above, it is hard to understand why the authority supervising certification authorities should be granted surveillance powers or powers to block access to websites. The former should be exercised by law enforcement agencies under the supervision of the courts and the latter should be ordered by the courts.

In short, the provisions of Section 46 fail to meet the requirement of legality under international law. In our view, it is so broad and confusing that it should be repealed in its entirety. If the Bangladeshi government were inclined to grant any additional surveillance powers to law enforcement or intelligence agencies, it should do so by way of separate legislation in strict compliance with the requirements of international law. Equally, any blocking powers should be clearly provided by law and comply with the international standards on freedom of expression outlined in the 'international standards' clause of this report.

---

[44] Section 18(1).
[45] See e.g. Arafat Hosen Khan, Speak No Evil, Dhaka Tribune, 13 October 2013.

Recommendation:

- Section 46 of the ICT Act should be repealed in its entirety.

Criminalisation of online expression

Section 57 of the ICT Act criminalises several forms of online expression, including:

- false information;
- obscene material;
- defamatory statements;
- expression likely to cause deterioration of law and order;
- expression which tarnishes the image of the state or of an individual;
- statements hurting religious sentiments;
- statements provoking individuals or organisations.

Under the original version of the Act, punishment for offences under Section 57 included imprisonment for a term not exceeding 10 years and a fine not exceeding Tk.1 crore. Following the 2013 Amendment, offences under Section 57 are now punishable by imprisonment for a term ranging from 7 to 14 years.[46]

In ARTICLE 19's view, this Section is both unnecessarily broad and criminalises legitimate forms of expression in breach of international standards on freedom of expression. Furthermore, the sanctions available under Section 57 are clearly disproportionate. We therefore recommend that it should be repealed in its entirely.

False information

In ARTICLE 19's view, the prohibition of "fake material" or "false information" falls short of international standards of freedom of expression for the following reasons:

- First, in the digital environment where news travels at an incredible pace, facts may be difficult to check. If journalists, or indeed bloggers and other social media users, are faced with the prospect of a prosecution for publishing false information, they are much less likely to share information, including news that is clearly in the public interest. Ultimately, therefore, criminalising the dissemination of false information can have a serious chilling effect on the free flow of information.

- Secondly, facts are not always easily separated from opinions. It would therefore be unfair to criminalise individuals for failing to differentiate between the two. Moreover, it is easy enough to see how a ban on false news could be used as a cover for shunning opinions not favoured by the authorities. Equally, whether something is true or false cannot always be confidently established because it may depend on prevailing social views or scientific progress. To convict an individual on the back of such vague a notion as 'truth' is therefore unlikely to comply with the requirement of legal certainty under international law.

- Thirdly, the criminal law, and especially imprisonment, cannot be a proportionate response to the harm caused, if any, by the circulation of fake/false information. In this

[46] The Information and Communication Technology (Amendment) Act 2013 (Act No. 42 of 2013), Section 4.

regard, the Human Rights Committee stated that "the prosecution and punishment of journalists for the crime of publication of false news merely on the ground, without more, that the news was false, [is a] clear violation of Article 19 of the Covenant."[47] Similarly, the UN Special Rapporteur has said that "In the case of offences such as … publishing or broadcasting "false" or "alarmist" information, prison terms are both reprehensible and out of proportion to the harm suffered by the victim. In all such cases, imprisonment as punishment for the peaceful expression of an opinion constitutes a serious violation of human rights."[48]

- Finally, and in any event, criminalising the dissemination of false information online would be both highly impractical and counter-productive, given the vast amount of potentially inaccurate information that circulates online and the number of individuals disseminating it via social media platforms such as Twitter or Facebook. In our view, the prosecution of potentially millions of Bangladeshi for innocuous – yet inaccurate - tweets would be a clear waste of public resources, which would be much better spent investigating serious crimes (e.g. the recent murders of a number of bloggers in Bangladesh).

Publication or transmission of obscene materials

Section 57 further criminalises the online publication or electronic transmission of 'obscene' material, which tends to 'deprave and corrupt' those who read it.

ARTICLE 19 recalls that while Article 19(3) of the ICCPR allows for limits on freedom of expression for materials in order to protect public morals, this does not provide for an open-ended ability to ban all materials which officials might find offensive.[49] The UN Siracusa Principles on the Limitation and Derogation of Provisions in the ICCPR also place 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.[50]

In ARTICLE 19's view, Section 57 falls well below these standards. In particular, the absence of any definition or at least interpretative guidance of key terms of the offence – such as "obscene," "material" "depravity" and "corruption"– is in clear breach of the requirement of legality under international human rights law. As currently drafted, the offence is so broad as to criminalise virtually any form of expression, from mundane gestures to artistic expression, which is merely offensive or contains the most oblique sexual overtones. Whilst we recognise that defining "obscenity" may be challenging, it is by no means impossible. We note, for

[47] Concluding Observations of the HR

[48] Annual Report to the UN Commission on Human Rights, Promotion and protection of the right to freedom of opinion and expression, 18 January 2000, UN Doc. E/CN.4/2000/63, para. 205.

[49] See also, e.g., European Court, *Murphy v. Ireland*, Application No. 44179/98, 10 July 2003.

[50] UN Economic and Social Council, UN 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.

instance, that a number of jurisdictions have adopted far more detailed guidelines on what constitutes obscenity.[51]

Section 57 is not only in breach of the requirement of legality under international law but is also disproportionate. In particular, it prohibits the publication of all obscene material merely by reference to vague notions of "depravity" and "corruption." In our view, however, the publication of obscene material should only be restricted if it can be shown to be necessary to prevent real harm – rather than 'harm to public morals' - or for the protection of children. For this reason, we believe that the criminalisation of the publication of all manners of 'obscene' material regardless of any demonstrable harm is both disproportionate and cannot be justified in a democratic society.

Online defamation

ARTICLE 19 further considers that the "online defamation" provision of Section 57 of the ICT Act violates international standards on freedom of expression.

International human rights law strongly favours the decriminalisation of defamation on the basis that civil defamation laws already provide adequate protection for reputation. Moreover, the use of criminal penalties in relation to defamation is a disproportionate restriction on freedom of expression.

ARTICLE 19 has long advocated against criminal defamation. In our view, defamation is typically a private matter between two individuals, one which does not warrant the use of criminal penalties such as imprisonment. This can obviously have a serious chilling effect on the peaceful exercise of freedom of expression. Our position therefore is that all criminal defamation laws are in breach of international guarantees for the protection of freedom of expression and must be abolished.

The same obviously applies to the Bangladesh provisions on criminal defamation in relation to digital technologies. ARTICLE 19 therefore recommends that the criminal defamation provision in the ICT law should be repealed and replaced with appropriate civil law remedies. Pending their abolition, law enforcement agencies should refrain from prosecuting defamation cases and the judiciary should quash convictions for defamation. Equally, the courts should refrain from imposing disproportionate sanctions in such cases.

Causing the deterioration of law and order

Sections 57 of the ICT Act also criminalises the deliberate online publication or transmission of any material that 'causes or is likely to cause deterioration of law and order'.

ARTICLE 19 notes that whilst it is legitimate to limit freedom of speech to protect public order, such limitations must comply with the requirements of legality, necessity and proportionality under Article 19 (3) of the ICCPR. However, this part of Section 57 falls well below those standards. In particular:

- The phrase "deteriorate law and order" is extremely vague. We remind the Bangladeshi government that the principle of legality demands that laws are sufficiently clear to

[51] This is the case, for instance, in the United States, Canada and South Africa: see ARTICLE 19, *Obscenity Laws and Freedom of Expression: A South African Perspective*, 12 January 2000

enable individuals to regulate their conduct as well as to prevent abuse by the authorities in the application of those laws. Whether or not material is likely to cause deterioration of law and order is impossible to know in advance.

- Moreover, it is highly unclear what constitutes "deterioration" of law and order. In the absence of any clear definition, it could include the publication of material that merely causes a public outcry in the news or riots. In any event, rather than punishing those who publish material which is likely to cause deterioration of law and order, even if done deliberately, the law should punish those who actively incite others to violence.

Moreover, given that criminal sanctions attach to such an impermissibly broad range of conduct, this part of Section 57 cannot be considered necessary and proportionate in a democratic society.

Image of the state or individual

Under Section 57 of the ICT Act, tarnishing 'the image of the state or individual' is also criminalised. For all intents and purposes, they are tantamount to the criminalisation of defamation of public figures or state institutions.

ARTICLE 19 notes that there is no reason in principle why public figures should benefit from special protection against defamation. Indeed, under international law, all public officials are required to tolerate a higher degree of criticism than other individuals. By virtue of their public position, they must be subject to closer public scrutiny. The more senior the position, the more tolerance a public servant ought to display. This also applies to foreign officials. Moreover, as already noted above, it is not appropriate to apply criminal penalties to disputes of this nature. More generally, the protection of the "state" (and, by extension, public officials) from defamation is entirely prohibited as state institutions do not benefit from the protection of reputation.

Sections 57 dealing with the tarnishing of the 'image of the state or individual' is therefore in clear breach of international standards on freedom of expression and should be abolished.

Hurting religious sentiments

The deliberate publication or transmission online of any material, which "hurts or is likely to hurt religious sentiments," is an offence under Section 57 of the ICT Act. In defining a similar offence relating to religion, the Penal Code 1860 specifies that a person to be criminally liable must have "deliberate and malicious intention of outraging the religious feelings of any class of the citizens of Bangladesh."[52] Therefore an accused can plead "absence of deliberate and malicious intention" as a legitimate defence when charged under the Penal Code, but not when charged under Section 57 of the ICT Act.

ARTICLE 19 is concerned that these prohibitions fall short of the requirements of international law, for the following reasons:

- Firstly, under international law, freedom of expression protects not only the views and information that are favourably received, but precisely those that some people might find

[52] Section 295A.

controversial, shocking, offensive or insulting.[53] That also includes information and ideas that might hurt some people's 'religious beliefs'.

- Secondly, to the extent that international law requires the prohibition of advocacy of religious hatred, under Article (2) ICCPR, it must be confined to "any *advocacy* of national, racial or religious hatred that constitutes *incitement* to discrimination, hostility or violence" (emphasis added). The term "advocacy" and "incitement" imply that negligence or recklessness are not sufficient to impose sanctions and that something more than intentional distribution or circulation is required. The words "causing hurt or may hurt religious belief," included in the provisions of Section 57 are broader in scope than what is permitted under Article 20 (2). They are also too vague to comply with the legality requirement under Article 19 (3) ICCPR.

- Thirdly, and in any event, while international law protects the rights of individual persons and, in some instances, of groups and persons, it does not protect abstract entities such as values, religions, beliefs, ideas or symbols. Although criticising and mocking religions, religious objects or deity may be considered by some to be blasphemous or an insult to their religious beliefs and feelings, under international human rights law, this is not a valid ground for banning or otherwise censoring them. In particular attempts to protect religions or beliefs from criticism in international law through the United Nations have ultimately failed. In April 2011, for instance, the UN Human Rights Council rejected the concept of so-called "defamation of religions" in a resolution on combatting discrimination of persons based on their religion or belief.[54].

- Finally, prohibitions of blasphemy/defamation of religions and protection of symbols and beliefs are not only contrary to guarantees of freedom of expression, but are also counterproductive and prone to being abused against the religious minorities that they purport to protect. They can also be contrary to the promotion of tolerance and protection against discrimination of any kind, including on religious grounds.

Provocation

Under Section 57 of the ICT Act, provoking any person or organisation by the information contained in any material deliberately published or transmitted in the website or in any electronic form is punishable by a term of between 7 to 14 years. In our view, this is a perfect example of unprincipled criminalisation.

In ARTICLE 19's view, this provision is both unnecessarily vague and disproportionate. In particular, the provision entirely fails to define provocation by reference to any further act that may be proscribed by law (e.g. provocation to commit murder). Nor does it link provocation to any aim that may legitimately be used to limit freedom of expression (e.g. public order). In those circumstances, the availability of sanctions as harsh as 14 years imprisonment for such highly undefined criminal acts is disproportionate.

Recommendation:

[53] European Court, *Handyside v the UK*, no. 5493/72 [1976] ECHR 5, 7 December 1976.
[54] Combating intolerance, negative stereotyping and stigmatization of, and discrimination, incitement to violence, and violence against persons, A/HRC/RES/16/18.

- Section 57 of the ICT Act should be repealed in its entirety.

Criminalisation of unauthorised disclosure of information

Section 63 of the ICT Act criminalises the unauthorised disclosure of information obtained pursuant to the powers conferred under the Act or "rules and regulations made thereunder."

To the extent that this provision is restricted only to public officials exercising statutory powers, ARTICLE 19 agrees that this is, on its face, a permissible restriction given that it safeguards private information from being unlawfully disclosed. However, we are concerned that there is no exemption provided for disclosure in the public interest, e.g. in the case of whistleblowers wishing to disclose information relating to corruption or other serious wrongdoing.

On a separate note, it is unclear whether a person who obtains information "in pursuance of any of the powers conferred under this Act or rules and regulations made thereunder" could include one or more private individuals. If this were the case, we would conclude that any such provision must be plainly disproportionate. We would therefore welcome clarification that this provision only applies to public officials. To the extent that this provision seeks to protect personal data undergoing automated processing, it should properly be addressed as part of comprehensive data protection legislation and not in a law relating to ICT.

Recommendations:

- Section 63 should be reviewed and clarified. In particular, a public interest disclosure exemption should be added. Furthermore, the scope of Section 63 should be more clearly limited to public officials;
- The protection of personal data undergoing automated processing should properly be addressed as part of comprehensive data protection legislation.

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.