

Mandate of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression

Ref.: OL BGD 7/2023
(Please use this reference in your reply)

28 August 2023

Excellency,

I have the honour to address you in my capacity as Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, pursuant to Human Rights Council resolution 52/9.

In this connection, I am writing to your Excellency regarding the **draft Cyber Security Act which was approved by the Cabinet on 7 August 2023** in order to share my observations and comments on the draft law with a view to engaging constructively with your Excellency's Government and supporting it through this process to ensure that the proposed law is in line with international human rights standards.

I understand that the draft Cyber Security Act is intended as an amendment to the current Digital Security Act (DSA). In light of the numerous concerns regarding the Digital Security Act raised by the High Commissioner for Human Rights, by Member States during the Universal Periodic Review and by the Special Procedures of the Human Rights Council, including my own mandate, I am encouraged by the Government's decision to amend the DSA. However, it is disappointing that the proposed new draft Act has retained many of the serious deficiencies of the DSA.

The Office of the High Commissioner on Human Rights provided your Excellency's Government with a technical note in June 2022. That note contained clear, precise recommendations, most of which have not been included in the proposed draft law.

I would like to highlight the following comments relating to the draft Cyber Security Act:

- a) The draft Act contains vague and overly broad provisions which criminalize a large variety of legitimate forms of expression. These provisions have been reproduced from the Digital Security Act, although they contravene international human rights law, have been used wrongly against journalists, human rights defenders and scholars, and have led to severe negative human rights consequences, including prolonged detention, deaths in custody and attacks on media freedom, as raised in previous communications sent to your Excellency's Government (e.g. BGD 4/2023, BGD 1/2022, BGD 2/2021, BGD 7/2020, BGD 5/2020, BGD 4/2020, BGD 2/2020, BGD 4/2018).
- b) The punishments remain disproportionately harsh under the draft Act. Although the Government has sought to reduce the maximum period of imprisonment or remove it in some cases and to expand the bail provision to a wider number of offences, the proposed changes would not be significant enough to be meaningful, and in some cases, such as

criminal defamation, the reduction of the prison sentence has been offset by higher fines.

- c) Law enforcement agencies and the telecommunications regulatory authority enjoy extensive, unfettered power under the draft Act. That could create serious risks to human rights in the absence of adequate judicial oversight.

I strongly urge your Excellency's Government to bring the proposed draft Cyber Security Act in line with international legal standards so that the new legislation can be a truly momentous step forward in safeguarding freedom of opinion and expression in Bangladesh. It would send a strong message about the Government's commitment to human rights and the rule of law as the country embarks on its sixth decade since independence.

In the hope that the Bangladesh government will take the opportunity to make further changes to the draft law prior to submitting it to Parliament, I set out below the international legal standards and areas where the proposed draft could be improved to meet those standards.

International legal standards on freedom of opinion and expression

The obligation of Bangladesh to respect and protect the right to freedom of opinion and expression is derived from article 19 of the International Covenant on Civil and Political Rights (ICCPR) to which Bangladesh acceded on 6 September 2000 under the leadership of her Excellency, Prime Minister Sheikh Hasina.

Article 19(1) of the ICCPR guarantees that all individuals "shall have the right to hold opinions without interference". Article 19(2) of the ICCPR provides that "[everyone] shall have the right to freedom of expression; this right shall include the freedom to seek, receive and impart information and ideas of all kinds, regardless of frontiers, either orally, in writing or in print, in the form of art, or through any other media of his choice". It is well established that all provisions regarding freedom of opinion and expression, including the permissible restrictions, apply equally on the internet as well as offline (A/HRC/RES/32/13).

According to article 19(3) any restriction of the right to freedom of expression must be a) "provided by law"; b) "necessary" and c) for the purpose of protecting "the rights or reputation of others", "national security, public order, public health and morals". The Human Rights Committee has clarified that not only should the restrictions be enacted in law but that the language of the law should be clear, precise, accessible and predictable. Furthermore, "necessity" implies that the restrictions must be proportionate to the objectives to be achieved. In other words, the restrictions must be "the least intrusive instrument among those which might achieve the desired result." (Human Rights Committee, general comment no. 34, CCPR/C/GC/34).

Article 20(2) requires States to prohibit advocacy of national, racial or religious hatred that constitutes incitement to discrimination, hostility or violence. The prohibition should be narrowly construed in line with article 19(3).

Cyber Security Act

Drawing heavily on the DSA, the Cyber Security Act criminalizes a wide range of expressions, imposes disproportionate, harsh punishment for the offences and uses vague, broad and imprecise language that could lead to arbitrary and unpredictable decisions by officials. In its current form, the draft Act would not meet the requirements of legality, necessity and legitimate objectives set out in the International Covenant on Civil and Political Rights, as mentioned above. Therefore, it must be revised, and some elements of it removed, if it is to meet international legal standards and comply with the international obligations of Bangladesh.

1. Political expression

Section 21 criminalizes “any kind of propaganda or campaign against liberation war, spirit of liberation war, father of the nation, national anthem or national flag.” According to section 2(u) the “spirit of liberation war” refers to “the high ideals of nationalism, socialism, democracy and secularism which inspired our heroic people to dedicate themselves to, and our brave martyrs to sacrifice their lives in, the national liberation struggle”.

According to the Human Rights Committee, criticism of state authorities, including the Head of the State, and diverse views relating to a State’s flag, national symbols or historical events are legitimate expressions, protected by international law.

While appreciating the Government’s desire to protect the distinct national historical legacy of Bangladesh, the vague and broadly framed nature of this provision could lead to unlawful restriction of political expression and is not **consistent with international law**. Instead of criminalization of criticism of the past, I encourage the government to **promote respect for the liberation struggle, the martyrs, and national symbols and values through enhanced public education, awareness programs and community based activities, instead of pursuing criminalization**.

2. Religious hatred

Section 28 punishes publication of information that “hurts the religious values or sentiment” while **section 31** criminalizes the publication of material that “creates enmity, hatred or hostility among different classes or communities”.

International human rights law protects individuals from intolerance, violence and discrimination based on their religion or belief, but it does not allow restriction or prohibition of criticism of religious belief or sentiment or lack of respect for religion.

Furthermore, the imprecise language of the provisions would risk encouraging human rights abuses by State and non-State actors in the name of religion and would be inconsistent with the requirements of legal certainty under international law. Your Excellency’s government will recall that these concerns were expressed by the Committee against Torture, in its observations on Bangladesh. (Committee against Torture, Concluding observations on the initial report of Bangladesh, 26 August 2019 (CAT/C/BGD/CO/1)).

Section 28 appears to be inconsistent with international law and should be removed, while section 31 should be tightened and brought into line with

article 20(2) of the International Covenant on Civil and Political Rights which requires States to prohibit “advocacy of national, racial or religious hatred that constitutes incitement to discrimination, hostility or violence”.

3. Criminal defamation and false information

Section 29 on criminal defamation and **section 25** on “offensive, false or threatening data-information” of the DSA have been used frequently to detain those criticizing the government, as raised in numerous communications previously sent to your Excellency’s Government. It is deeply disturbing to find that they have both been retained in the draft Cyber Security Act.

While international law permits the restriction of speech to protect the reputation of others, it should be done through civil litigation by individuals, and not through prosecution by the State under criminal law. As I mentioned in my report to the Human Rights Council, “criminalization of speech (other than in the most egregious cases of incitement to violence and hatred) is disproportionate, gags journalism and damages democratic discourse and public participation.” (A/HRC/50/29, para 111).

I urge the government to heed the recommendation of the High Commissioner to **replace criminal defamation in the Cyber Security Act and in the Penal Code with a clear, narrowly defined provision on civil defamation**, to limit the claim only to those who are directly affected, and to include public interest in the subject matter and truth as valid defences.

The criminalization of “offensive or false information” (section 25) is both contrary to international law standards and ineffective in combating disinformation and misinformation. The right to freedom of expression applies to all kinds of information and ideas, including those that may shock, offend or disturb (A/67/357). International law does not allow information to be prohibited merely because it is false as that could lead to the suppression of views with which the government does not agree. Access to plural, diverse sources of information, including independent, diverse and pluralistic media, and digital and media literacy of the public have proven to be more effective against false information than criminalization and censorship (A/HRC/47/25, para. 38).

4. “Cyber terrorism”

Section 27 on cyber terrorism in the DSA has been reproduced in the draft Cyber Security Act. That definition of cyber terrorism is extremely broad and vague, and does not refer to the elements in the international definition of terrorism. The penalty of up fourteen years in prison makes it particularly important that this provision should be tightened and brought into line with international standards.

I urge you to accept the recommendation of the High Commissioner for Human Rights that the government should **adopt the international definition on terrorism** set out by Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism.

5. Disproportionate punishment

International law requires measures to restrict freedom of expression to be strictly necessary and proportionate. The UN human rights bodies, including myself, have called for the decriminalization of all offences related to freedom of expression (except in highly egregious cases of advocacy of national, religious or ethnic hatred that constitutes incitement to discrimination, violence or hostility).

The Cyber Security Act not only retains the long list of criminal offences of the DSA but also incorporates the same harsh punishments, except for some small changes. For instance, the penalty under section 21 has been reduced from ten to seven years imprisonment, and under section 25 from three to two years. While the government has removed imprisonment as a penalty for criminal defamation, it has increased by five times the financial penalty for criminal defamation (from BDT 500,000 to a maximum of BDT 2,500,000). The punishment for cyberterrorism is up to 14 years.

The heavy penalties under the draft Act, coupled with a long list of vaguely defined offences, could be a major threat to freedom of expression, as they are likely to lead to arbitrary decisions from officials or self-censorship by journalists, human rights defenders and political activists, stifling democracy as well as media freedom, including reporting on issues of critical interest to the public, such as corruption.

I encourage the Government **to consider reducing the number of criminal offences and the penalties** under the draft Act to bring it in line with international standards.

6. Power of regulatory and law enforcement authorities

Section 8 of the draft Act empowers the Bangladesh Telecommunication Regulatory Commission (BTRC) to remove data or restrict access to websites that threaten “digital security”, or when asked by law enforcement authorities on a wide range of vaguely drafted grounds, including “solidarity”, “financial activities”, “religious values” or “public discipline of the country” which are not recognized grounds for restricted expression under international law. The vagueness of this section would leave considerable room for arbitrary and excessive action by the Regulatory Commission, and could infringe unlawfully on freedom of expression.

Content removal and blocking of information should be carried out under provisions that are clearly defined by law and in line with international human rights obligations, and such acts **should be carried out only upon the decision of an independent, preferably judicial, body** (A/66/290, para. 17).

Section 42 affords police officers very wide authority to search and seize computers, computer systems, computer networks, data-information or other materials and arrest any person without a warrant. I have grave concerns about such unfettered discretion of law enforcement authorities, especially given the vagueness and vast scope of the draft Act. Such unfettered discretion of law enforcement authorities may lead to abuse of authority and human rights violations. The experience of the DSA suggests strongly that **independent judicial oversight over the conduct of search, seizure and arrest by law enforcement officials must be strengthened.**

Conclusion

Allow me to conclude by expressing appreciation for the stated intention of the Government to amend the Digital Security Act in line with international standards. However, I note that most of the problematic provisions of the Digital Security Act are retained in the draft Cyber Security Act, including sections 21, 25, 27, 28, 29, 31 and 32.

In particular, it is unfortunate, and in my view a missed opportunity for the Government, that the recommendations of the OHCHR technical review of the Digital Security Act,¹ including the proposal to repeal of the sections 21 and 28, have not been reflected in the draft Cyber Security Act.

I recognize both the complexity of the issues and the engagement of the Government with the United Nations. Notwithstanding the stated calendar for adoption of the new law, I strongly urge the Government to take the window created by this reform process to reconsider the draft and take into account the recommendations from the United Nations.

For my part, I stand ready to engage with your Excellency's Government on this matter. I look forward to receiving any additional information and any comment you may have on my observations above, in particular how the proposed Cyber Security Act complies with your Excellency's Government's obligations to respect and promote freedom of expression under article 19 of the ICCPR.

I am available to meet with you and his Excellency, the Minister for Law, Justice and Parliamentary Affairs at your convenience.

This communication, as a comment on pending or recently adopted legislation, regulations or policies, and any response received from your Excellency's Government will be made public via the communications reporting [website](#) after 48 hours. They will also subsequently be made available in the usual report to be presented to the Human Rights Council.

Please accept, Excellency, the assurances of my highest consideration.

Irene Khan
Special Rapporteur on the promotion and protection of the right to freedom of opinion
and expression

¹ [Microsoft Word - OHCHR note on review of Digital Security Act June 2022.docx](#)