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

Ref.: OL BGD 2/2025
(Please use this reference in your reply)

17 March 2025

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.

I would like to thank your Excellency's Government for its engagement with my mandate and for the constructive meetings I have had with yourself, the Law Adviser, Mr. Asif Nazrul, the former Information Adviser, Mr. Nahid Islam, the Honorable Chief Justice, Syed Refaat Ahmed and the Chairperson and members of the Media Reform Commission.

Following these meetings and consultations with legal experts and civil society leaders, I am writing to share my observations on the draft Cyber Protection Ordinance (CPO) which was disseminated on the website of the Information, Communications and Technology Division for public comments.

I welcome the decision of the Interim Government to repeal the Cyber Security Act (CSA), adopted by the previous government in 2023. The CSA and its predecessor, the Digital Security Act (DSA), were the subject of several communications from my mandate as well as the United Nations High Commissioner for Human Rights (see OL BGD 7/2023, BGD 4/2023, BGD 1/2022, BGD 2/2021, BGD 7/2020, BGD 5/2020, BGD 4/2020, BGD 2/2020, BGD 4/2018).

I am pleased that section 50(1) of the draft Cyber Protection Ordinance, which will repeal the CSA, will also obliterate all criminal cases pending under sections 21, 25, 28, 29 and 31 of the CSA. I encourage your Excellency's government to accelerate the obliteration of the cases and bring an end to the distress of the affected individuals as documented in the above-mentioned communications by UN special procedures experts. In such communications, Special Procedures mandate holders raised concerns about human rights defenders, journalists, social activists, political opponents, artists and intellectuals in Bangladesh that were targeted by the previous government using the DSA and the CSA, threatened, legally harassed, prosecuted, and in many cases, subjected to prolonged pre-trial detention, which led to at least one death in custody.

I am also pleased that sections 21 and 25 of the CSA on criminalization of defamatory content do not appear in the draft CPO. As noted in my communication on the CSA to the previous government (OL BGD 7/2023), the restriction of speech to protect the reputation of others is permitted under international law but it should be done through civil litigation by the aggrieved individuals and not through prosecution by the State under criminal law. While commending the Interim Government for ending online criminal defamation, I encourage it to review the current offence of criminal defamation in the Penal Code and replace it with a clear, narrowly defined provision on civil

defamation, limiting the claim only to those who are directly affected and incorporating public interest in the subject matter and truth as valid defences. Such a change will significantly reduce the possibility of legal harassment of journalists and human rights defenders and strengthen freedom of expression in Bangladesh.

Although the draft CPO introduces some important positive changes, I believe it nevertheless contains some major flaws that call for review and significant revision. The draft Ordinance should not be adopted in its current form.

A major deficiency of the draft CPO is that the same law seeks to regulate both cybercrimes (e.g. hacking) and online content (e.g. gendered harassment), although the two issues are fundamentally different in nature and require different approaches and solutions. The ICT Act, the 2018 DSA and the 2024 CSA also combined cyber security and content regulation in one legislation and under one administrative structure. As their subsequent implementation showed, human rights violations are inevitably high when online content is regulated through a criminal law framework by an agency geared to fight attacks on technology infrastructure.

I have been struck by the absence in the CPO of an explicit commitment by the government to uphold the right to freedom of expression in line with international standards to which the government is legally bound. Although some provisions of the CSA which were contrary to international human rights law do not appear in the draft CPO, other troubling provisions and features of the CSA that caused serious concern to my mandate and to the High Commissioner for Human Rights have been retained. Broad, vaguely defined speech-related offences that are likely to lead to abuse and overreach, harsh punishments that could intimidate users and chill freedom of expression, and a powerful, highly centralized administrative structure controlled by the executive with no judicial oversight or public accountability are troubling features of the draft CPO and reminiscent of past State policies and practices which your Excellency's government has condemned. I strongly encourage the Interim Government to review the draft CPO in light of these problems.

I set out below the international legal standards relating to freedom of expression with which the draft CPO and other digital governance reforms must comply.

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.

Article 19(1) of the ICCPR guarantees that all individuals "shall have the right to hold opinions without interference". Article 19(2) of the International Covenant on Civil and Political Rights 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 online and offline (A/HRC/RES/32/13).

According to article 19(3) States may restrict freedom of expression only if is the restriction is "provided by law" and "necessary" for the legitimate objective of protecting "the rights or reputation of others", "national security, public order, public health and morals". The Human Rights Committee, the authoritative treaty body for the interpretation of the Covenant on civil and political rights has clarified that "provided by law" means not only that the restrictions should be enacted in law but that the language of the law should be clear, precise, accessible to the public and predictable. Furthermore, "necessity" implies that the restrictions must be proportionate to the five objectives set out in article 19(3). 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). The objectives themselves should be clearly and narrowly defined. No restriction should not be such as to jeopardize the right itself.

Article 20(2) requires States to prohibit advocacy of national, racial or religious hatred that constitutes incitement to discrimination, hostility or violence. The Human Rights Committee has stated that the prohibition should be narrowly construed in line with article 19(3). The Rabat Plan of Action (A/HRC/22/17/Add.4), developed by the United Nations High Commissioner for Human Rights, provides useful guidance on measures to address speech that constitutes incitement to discrimination, hostility or violence under international law.

Cyber Protection Ordinance

My observations on the draft CPO focus on three specific aspects:

- overly broad and vague language to define speech related offences;
- disproportionate punishment for speech related offence;
- extensive unfettered executive authority without independent oversight or public accountability.

Overly broad and vaguely defined speech offences

As stated in my report to the Human Rights Council, criminalization of speech is often a disproportionate response, gagging journalism, chilling free speech and damaging democratic discourse and public participation. The criminal law should be used to restrict expression only in the most egregious circumstances (A/HRC/50/29, para 111). The draft CPO contains three offences relating to speech. They are framed in vague, overly broad or undefined terms that are likely to create legal uncertainty and lead to abuse, overreach and arbitrary, inconsistent interpretation by officials, infringing freedom of expression and encouraging self-censorship. I draw attention specifically to four sections of the CPO below.

Section 25 penalises the intentional dissemination or threat to disseminate information, obscene videos, audio visuals, still images, graphics or content produced with Artificial Intelligence which is harmful or intimidating and is

used to blackmail by means of sexual harassment or "revenge porn". It is a new provision, not previously existing in the CSA or DSA.

While the intention to address online sexual and gender-based harassment is good, the offence, as drafted, is problematic. The language is unclear and confusing, which will make enforcement difficult and increase the likelihood of censorship of lawful expression. Nowhere does the draft CPO define "sexual harassment" or "revenge porn". It defines "blackmail" as the threat or intimidation to publish "private information" or cause "harm" to coerce an individual into granting illegal advantages or services, but what constitutes "private information" or "harm" is not clarified. The draft Ordinance criminalises the dissemination of content deemed "obscene", a broad term which is open to subjective interpretation, and could be used unfairly to target women and tarnish their reputation, or seek to suppress legitimate artistic expression and encourage a culture of self-censorship. The failure to define key concepts clearly and the focus only on one element of a much more complex problem of online gender-based threats and violence means that this section is unlikely to have much effect on the latter while increasing the possibility of censorship.

I agree that the growing problem of online gender-based violence, harassment and disinformation must be tackled. However, experience shows that the solutions to these problems are most effective when they are addressed in comprehensive manner and well-grounded in human rights (A/78/288). A hurriedly crafted, piece meal response may aggravate the problem of online gender-based threats rather than resolve it. My advice to the Interim Government is to work in consultation with civil society organizations specialized on women's and children's rights and review and amend existing legislations on protection of women and children to include also digital threats, to strengthen their provisions and ensure effective enforcement through a range of legal and social measures.

Section 26 penalises any person or group for publishing, propagating, or facilitating the propagation of "anything" in cyberspace that is "hateful", "malicious" or "provocative" against any religion or its followers. This section is framed too broadly and vaguely and is not in line with international standards. "Hateful", "malicious" and "provocative" are vague and subjective terms and could potentially be weaponized to silence religious minorities, secular voices and social reformers.

Under article 20(2) of the International Covenant on Civil and Political Rights advocacy of religious hatred must be prohibited only when such advocacy constitutes incitement to discrimination, hostility or violence. In other words, the offence must comprise both advocacy of hatred as well as incitement of harm. I recommend that section 26 of the CPO be revised to bring it in line with the standards set out in article 20(2) of the Covenant.

It must be noted that the right to freedom of expression includes all kinds of information and ideas, including those that may shock, offend or disturb (A/67/357). It is important in democratic societies to allow debate and dissent

and encourage tolerance even on sensitive topics. Religious criticism that does not reach the threshold of incitement to violence, hostility and discrimination should be handled not through prosecution under the criminal law but non-legal means, such as awareness building, information sharing, education and community building programs. The Rabat Plan of Action (A/HRC/22/17/Add.4) provides useful guidance on various measures through which "hate speech" can be tackled without resorting to prosecution. I urge your Excellency's government to consider these non-criminal options while reserving criminal law for the most egregious cases of incitement to violence.

Section 23 on cyber terrorism is very similar to a provision in the Cyber Security Act. Like that provision, section 23 is extremely broad and vague, and likely to chill legitimate freedom of expression of journalists, political activists and human rights defenders. Given the heavy penalty that this offence carries, it is particularly important that the definition be tightened and aligned with international standards and good practice. I strongly suggest that the Interim Government should adopt the international definition on terrorism set out by the Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism.

Section 27 penalizes anyone who "aids" in the commission of an offence in the draft CPO but does not define what constitutes "aiding". This lacuna could lead to overreach by the authorities, unjustifiably implicating a wide group of users in a criminal offence. Vague terminology and the likelihood of such prosecution or threat of it may discourage users from engaging in online debates or disseminating information, and thereby contribute to self-censorship, chilling dissenting voices. The section should be revised to restrict the concept of aiding only to those who intentionally and substantially contribute to a criminal offence.

Disproportionately harsh punishment

International law requires measures to restrict freedom of expression to be strictly necessary and proportionate. When speech offences lead to disproportionately harsh punishment they violate this principle.

Although the draft Cyber Protection Ordinance has reduced the number of speech offences, it provides for stiff fines and prison sentences. The penalty under **section 25** for offences of gender-based blackmail and obscenity entails a maximum of two years' imprisonment and/or a fine of one million (ten lakh) Taka. If the offence involves a child or a woman, the imprisonment is increased to a maximum of three years and/or fines of two million (twenty lakh) Taka. Under Section 26, the penalty for provocative, hateful, or inciting speech is a maximum of two years' imprisonment and/or a fine of one million (ten lakh) Taka. The penalty for cyber terrorism under section 23 is a maximum of ten years' imprisonment (reduced from fourteen years under the CSA) and/or a fine of ten million (one crore) Taka. When such penalties under the draft Ordinance are combined with vaguely defined offences and unfettered powers of law enforcement authorities to search, seize, arrest and block content, they can become a formidable deterrence to freedom of expression, as they are likely to

lead to arbitrary decisions from officials which can intimidate and induce self-censorship by artists, satirists, critics of societal norms and human rights defenders, stifling freedom of expression and media freedom, impacting on reporting and debate on issues of critical public interest.

I encourage the Government to ensure that criminal penalties are proportionate to the offence.

Unfettered executive authority

The broad, unfettered executive power to control communications through a centralized authority without any requirement of transparency, judicial oversight or public accountability is the most worrying aspect of the draft CPO. There is no requirement under the draft CPO for judicial oversight of decisions to take down posts or block websites or shut down the internet, nor Parliamentary accountability for such actions nor any semblance of independence of the cyber protection agency from political and security actors in the government.

In effect, the CPO replicates the institutional arrangements under the CSA and the repealed DSA. As is well known, the unchecked centralized control of information and communications technology system was widely abused by the previous government to intercept data, carry out surveillance and shut down the Internet, with serious consequences for human rights, democratic institutions and the economy. It is deeply disturbing that the Interim Government has chosen to reproduce that same system.

Section 8 of the draft Ordinance gives the Director-General of the Cyber Protection Agency the authority to request the Bangladesh Telecommunication Regulatory Commission (BTRC) or the Information and Communication Technology Division to remove data or restrict website access that threaten “cyber security”, or upon request from law enforcement agencies, on vaguely defined grounds such as "solidarity", "financial activities", "religious values", or "public discipline of the country”. These grounds for requesting content removal do not align with internationally recognised standards for restricting expression. Nor are they defined, circumscribed or justified by any national law or policy. The interpretation and application of these provisions seem to be left to entirely to the discretion of a narrow powerful group of officials in the government.

The **Cyber Protection Agency** under the draft CPO Ordinance will be administratively linked to the Information and Communication Technology Division. Its Director-General (DG)and other directors appointed by the government, will execute their roles according to governmental directions regarding duties and terms of service (section 6 and 7).

The **National Cyber Protection Council**, to be formed under the draft Ordinance and similar to the Councils under the CSA and the DSA in the past, will be chaired by the head of government, and will comprise of members from various governmental and autonomous bodies, including security and

intelligence agencies (section 12). The political and security-orientation of the Council is clear. There is no provision for civil society participation as representatives of the users and consumers of information and communications technology. The Council will guide the Cyber Protection Agency, authorise direct measures for addressing cyber security threats, advise on the development of cyber security infrastructure, formulating inter-institutional policies to ensure cyber security, implementing the draft Ordinance and related Rules, and undertaking other activities as mandated by these Rules (section 13).

This legal framework compromises the ability of the Cyber Protection Agency to operate independently from the government and potentially creates significant scope for political pressure from the Council on the Agency. The absence of any requirement for transparency of decision making, public accountability or judicial oversight, combined with lack of clear and precise definitions, create a serious likelihood of arbitrary and excessive actions by the Director-General (Government appointed official reporting to a Council headed by the Prime Minister), the BTRC (state regulator), and the ICT Division (part of a government ministry). There is significant scope for abuse of power, including exploitative and excessive blocking of content and websites, unlawful electronic surveillance and Internet disruption and shutdowns, as actually happened under the previous government using the similar set up of the CSA and the repealed DSA. Moreover, the overlapping powers given to the BTRC and the ICT Division increase the risks and could create confusion about responsibility and accountability for abuse of power.

These serious problems should be addressed by a total overhaul of the sections in the draft CPO relating to digital governance. The National Protection Agency must be an independent state entity with full functional autonomy, in line with international standards of impartiality and transparency, with robust accountability mechanisms. The Agency must be protected from overt or covert pressure from the government or the private sector. The role of the National Protection Council should be reviewed to ensure that it is not able to exert pressure or undue influence on the Agency and performs its activities in an accountable manner. In line with international guidance and good practice, the Council should be a multistakeholder body, including representatives of civil society and technology experts as well as state officials.

All provisions related to content removal and blocking of information should be clearly defined by law and fully in line with international human rights standards. Given the scope of abuse, all such acts should be carried out only with judicial authorization and oversight (A/66/290, para. 17).

Another worrying provision in the CPO is section 35 which 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 on mere suspicion of a cyberattack on Critical Information Infrastructure (CII), illegal access to any computer, computer system among others, and hacking. Such unfettered discretion of law enforcement authorities, especially given the vagueness of the grounds on which such power may be exercised, could lead to abuse of authority and human rights violations, as the

experience of the CSA, DSA, and section 57 of the ICTA has shown. Independent judicial oversight over the conduct of search, seizure and arrest by law enforcement officials must be affirmed clearly.

The draft CPO, similar to the CSA and the DSA, allows for investigations to continue for a maximum period of 105 days which a Cyber Tribunal can extend for a reasonable period but the grounds on which such extension can be granted is not mentioned. As in the past, it is likely to lead to unnecessary prolongation of investigations as method of harassing, intimidating and leaving journalists, human rights defenders, activists and others in an uncertain situation. I recommend that the relevant section in the CPO be amended to provide specific, clearly defined criteria for the Tribunal to permit the extension of investigations.

Conclusion

Although my communication focuses on the draft CPO, I note that your Excellency's Government has embarked on amendment of the Bangladesh Telecommunications Regulatory Act and on drafting and adopting a Personal Data Protection Order, which are also of relevance to the right to freedom of expression. Without going into a detailed analysis, I would like to make a general observation that the problems of inadequate consultations, lack of transparency in the process and a piece meal approach to digital governance reforms that this communication identifies in the context of the draft CPO are equally applicable to the other two reform initiatives.

The proposed amendment of the Bangladesh Telecommunications Regulation Act has not been open to public consultations, although it covers surveillance, interception and internet shutdowns which are directly relevant to human rights, especially freedom of expression. Internet shutdowns are inherently disproportionate, given the blanket nature of the consequences affecting multiple users. As such, they violate the requirement of necessity and proportionality set out in international human rights law.

The Human Rights Council, of which Bangladesh is currently the Vice-Chair, has strongly condemned the use of Internet shutdowns that intentionally and arbitrarily prevent or disrupt access to information online.

The draft Personal Data Protection Order proposes sweeping exemptions for law enforcement and intelligence agencies to collect, process and store personal data, entrenching the dangerous practice of state surveillance, which has led in the past to major human rights violations and created a climate of intimidation, silencing critical voice and encouraging self-censorship.

The importance of upholding the right to freedom of expression, including access to information, cannot be overstated, especially given the experience of massive human rights violations resulting from repressive cyber safety laws in Bangladesh in the recent past. I urge the Interim Government to adopt a well-coordinated and comprehensive approach to digital governance through a transparent, inclusive multistakeholder process, and to adopt laws that are well-grounded in the international human rights obligations of Bangladesh. The Government should also promote non-legal measures, such as proactive information sharing by State institutions, independent

online fact-checking, and digital and media literacy for users.

As it is our responsibility, under the mandates provided to us by the Human Rights Council, to seek to clarify all matters brought to our attention, we would be grateful for your observations on the following matters:

1. Please provide any additional information and comments on my observations above.

2. Please indicate in particular what measures have been or will be taken to ensure that the proposed Cyber Protection Ordinance complies with the Government's obligations to respect and promote freedom of expression under article 19 of the ICCPR.

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.

I look forward to our continued cooperation and stand ready to meet with officials in your Excellency's government and support them in this important reform initiative.

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