Defending freedom of expression
and information

ARTICLE 19 Calls for Meaningful Consultation on Draft Cyber Protection Ordinance 2025

Dhaka, 03 February 2025: ARTICLE 19, an international human rights organization, dedicated to promoting freedom of expression and the right to information, has called for meaningful and effective consultations with relevant stakeholders before the enactment of the Draft Cyber Protection Ordinance 2025. The interim government's advisory council approved the draft of the **Cyber Surokkha Adhyadesh 2024 (Draft Cyber Protection Ordinance 2025)** on 24 December 2024. Prior to drafting the ordinance, the interim government failed to conduct meaningful consultations with relevant stakeholders. The draft ordinance in its present form could severely undermine independent journalism, as well as the rights to freedom of expression, in the country. ARTICLE 19 is calling for the Cyber Protection Ordinance 2025 to:

- comply with **international human rights standards**, particularly those related to freedom of expression, privacy.
- should provide **clear and precise definitions** for terms like "cyberbullying," "aiding," and "spreading hate," ensuring they are narrowly tailored to target only harmful, illegal activities like incitement to violence
- that government bodies including law enforcement should operate with greater **transparency and be subject to independent oversight**, ensuring that these bodies' actions are publicly accountable and that decisions, particularly those affecting citizens' rights, are subject to review.
- must integrate robust safeguards to protect **privacy and personal data as well as against safeguards against mass surveillance**, ensuring that cybersecurity measures do not compromise individuals' fundamental rights.

The draft ordinance has faced harsh criticism in Bangladesh. Journalists, lawyers, teachers, human rights defenders, and activists have severely criticized it, as the proposed law uses many terms that lack clear definitions, creating opportunities for misuse due to their vagueness. Many terms in the law lack clear definitions, creating opportunities for misuse due to ambiguity. Civil society members have questioned the drafting process, noting the lack of an inclusive and meaningful consultation process. Initially, the interim government allowed only three days for comments on the draft law. Amid widespread criticism, the government has uploaded an amended version of the draft ordinance on the ICT Division website and reopened the opportunity for comments from 22 January 2025 to 06 February 2025.

The newly approved draft retains several provisions from its predecessors, which had been widely criticized for suppressing freedom of expression. Initially, Section 57 of the Informaton and Communication Technology Act, 2006 (ICT Act), was frequently utilized by the government to curtail freedom of expression, dissent, and political opposition. Following widespread criticism from various domestic and international stakeholders, this provision was repealed with the enactment of the Digital Security Act, 2018 (DSA).

However, the DSA effectively reintroduced the restrictive elements of Section 57 in a more repressive manner, incorporating them into multiple sections alongside newly defined offenses.

The DSA faced extensive criticism for being employed as a tool by the government to suppress dissent, target political opposition, and curtail the activities of journalists, students, and activists. In September 2023, amid growing domestic and international condemnation, the government replaced the DSA with the Cyber Security Act, 2023 (CSA). Although framed as a more moderate alternative, the CSA retained several controversial provisions, including criminalizing certain forms of free speech, granting arbitrary powers to law enforcement for arrest, search, and seizure, and empowering authorities to block or filter content with minimal oversight. These provisions continue to raise concerns regarding potential misuse and their impact on fundamental rights.

Similar to its predecessors, the newly drafted ordinance raises significant concerns due to its far reaching implications for human rights, governance and accountability specifically provisions that restrict free speech and could potentially be used to harass individuals. Some of the problematic provisions are as follows:

Section 8 of the draft ordinance grants broad and unchecked authority to the executive to block or filter information it finds objectionable. Under international law, any restrictions on freedom of expression must be prescribed by law and meet the criteria of necessity in a democratic society.

Under Articles 12 and 13 of Chapter IV, the establishment of a National Cybersecurity Council is proposed. This body would wield expansive and unchecked powers to develop inter-institutional policies, enact regulations, and effectively control "cybersecurity infrastructural development." It would also oversee the Cybersecurity Agency, which is to be created under the same ordinance.

According to Section 8, the ordinance further grants significant authority to the director general of the National Cybersecurity Agency. The director general could request the removal or blocking of any information deemed to pose "cybersecurity risks." Without judicial oversight, such powers carry a high risk of misuse. Of particular concern is the composition of the Council which will be chaired by the country's Head of State and supported by a high-ranking contingent of government officials, including the ICT Minister and Directorate Generals of various intelligence and defence agencies. This concentration and centralization of authority raises serious concerns about accountability and the potential for government overreach with limited checks and balances.

Bangladesh's persistent challenges in the ICT sector stem from a deliberate policy of centralizing communications infrastructure and control under the former regime. This approach allowed authorities to coercively and arbitrarily pressure internet service providers to intercept data, censor content, and implement internet shutdowns on multiple occasions. These actions resulted in serious human rights violations under international law and produced widespread disruptions to public life, hindering economic activity and violating people’s right to access information, carried out with absolute impunity. The ordinance gives authorities the power to intercept communications and monitor digital activities under the guise of cybersecurity. This raises privacy concerns and risks creating a surveillance state.

Section 25A of the ordinance defines cyberbullying as acts of intimidating, threatening, or harassing individuals or groups online, as well as disseminating harmful information, defamatory content, or abusive language that damages a person's reputation or mental well-being. However, the broad and vague nature of this definition creates significant potential for misuse. It could discourage people from expressing their opinions for fear of causing offense, thereby shrinking the space for open criticism. Journalists, too, would need to exercise extreme caution in their reporting to avoid falling afoul of this provision. If someone claims to feel defamed, insulted, or mentally harmed, they could file a case, leading to the possibility of warrantless arrests by the police.

Section 26 criminalizes the publication of information, in any form, that intends to spread hate. This provision is inconsistent with international standards on freedom of expression, as it seeks to protect religious values or feelings rather than an individual's right to freedom of religion. Vague terms like "hate" can be misinterpreted or exploited to suppress legitimate criticism or dissent, especially on sensitive topics like religion, where such provisions have been used disproportionately against minority groups, journalists, activists, and political opponents. In addition, by criminalizing speech that "intends to spread hate," the provision risks creating a chilling effect, where individuals refrain from discussing or critiquing religious practices, institutions, or policies out of fear of legal repercussions. This discourages open dialogue restricting people's right to freedom of expression and may disproportionately target minority voices.

Section 27 penalizes anyone who "aids" in the commission of an offence under the Act, assigning the same punishment as the primary offence. However, the draft ordinance does not define what constitutes "aiding," leaving room for overly broad subjective interpretations that could criminalize a wide range of internet users, this ambiguity increases the likelihood of misuse. To avoid misuse and ensure fairness, the ordinance must clearly define "aiding," limiting its application to cases where an individual intentionally and substantially contributes to an offense. Safeguards must also be included to protect freedom of expression and prevent arbitrary enforcement. Finally, this provision may discourage people from engaging in legitimate online activities, including discussions, collaborations, and sharing of information. Fear of being accused of "aiding" an offense could lead to self-censorship, undermining freedom of expression and participation in online spaces.

Sections 33 and 35 grant the police sweeping powers to enter, search, seize, and arrest without adequate safeguards, raising significant concerns about undermining individual's rights to privacy and due process, as well as the potential misuse and abuse of authority. They could be weaponized to target political opponents, journalists, activists, or anyone critical of the government, leading to self-censorship, fostering fear, silencing dissent and eroding democratic discourse Without proper safeguards, these provisions may incentivize corrupt practices, such as unlawful detentions, extortion, or confiscation of property under the guise of cybersecurity enforcement. To ensure accountability, the ordinance must require judicial oversight, introduce strict procedural safeguards, and align with international human rights standards. Without these measures, these provisions risk undermining the very principles of justice and security they claim to protect.

Based on past experiences with Section 57 of the ICT Act, the DSA, and the CSA, we believe that the remaining problematic provisions in the draft ordinance could be used to suppress dissent, political opposition, and freedom of expression. In addition, the ordinance fails to address any structural issues around censorship, surveillance, consolidation of state power, and discretionary power given to law enforcement and intelligence agencies. Laws with such significant implications for the general public, journalists, and human rights defenders should not be passed hastily. The Cyber Protection Ordinance 2024 risks undermining democratic principles, curtailing fundamental freedoms, and fostering an environment of fear and surveillance. To address these issues, the ordinance needs substantial revisions, ensuring that cybersecurity measures are implemented in a way that respects fundamental rights, upholds transparency, and includes independent oversight mechanisms. ARTICLE 19 urges a comprehensive review and amendment of these provisions in accordance with the International Covenant on Civil and Political Rights which Bangladesh is a party to.