



Joint Civil Society Statement on the Proposed Cyber Protection Act, 2026

Dhaka, 17 September 2026

We, the undersigned civil society organizations, human rights defenders, media practitioners, and digital rights advocates, express our serious concern over the proposed amendments to the Cyber Protection Act, 2026. These amendments were developed without any meaningful process of public consultation, and their substance appears, in many respects, more regressive than the Digital Security Act, 2018 (DSA), continuing its legacy of criminalizing expression while expanding the scope of speech-related offenses.

No meaningful public consultation

The proposed amendments were not developed through any meaningful process of public consultation. Civil society, media practitioners, technologists, and the wider public had little to no genuine opportunity to review or respond to the draft before it advanced further in the policymaking process. This is not an isolated lapse but part of a pattern that has persisted across successive governments since the DSA itself was enacted in 2018 with negligible public input. Making a draft available is not meaningful consultation unless all relevant stakeholders have sufficient time to respond and their recommendations inform the outcome. Meaningful consultation is a basic precondition for democratic lawmaking, not a procedural courtesy and its continued absence should concern anyone, regardless of their views on the substance of the law.

Expanded, vaguely defined speech offenses

The proposed amendment considerably broadens the definition of defamation beyond the Penal Code definition previously adopted by the DSA and CSA, while introducing new offenses relating to maligning, rumor, and disinformation — each framed through broad, imprecise definitions that leave considerable room for subjective interpretation and inconsistent enforcement. Whether a statement is defamatory, false, misleading, or a rumor requires careful judicial fact-finding, not summary assessment.

The draft includes no meaningful safeguards for freedom of expression, media freedom, or public-interest reporting. It establishes no narrow, well-defined thresholds, requires no proof of concrete harm, and provides no adequate procedural safeguards against abuse. It criminalizes online expression, permits pre-trial detention, and imposes penalties of up to ten years' imprisonment and BDT 4 million — creating serious risk of selective enforcement and punishment before contested claims can be properly ascertained.



A ministry positioned to control the information ecosystem

The Ministry of Information and Broadcasting appears, for the first time, to be taking a leading role in this amendment process — a departure from past practice, where cyber legislation has generally fallen within the remit of the Ministry of Posts, Telecommunications and Information Technology. The basis and scope of this role remain unclear.

This institutional shift raises broader concerns about regulatory design. Crucial terms like "defamation," "malicious," "rumour," and "disinformation" reflect an increasing emphasis on regulating information and expression, echoing a colonial-era legal tradition in which broadly framed speech restrictions served as instruments of information control. Rather than establishing clear platform duties, meaningful user remedies, and a credible content-governance regime, the amendments simply expand the state's power to determine what remains online.

Weakened safeguards

Several other changes weaken the overall framework, which remains fundamentally punitive rather than protection-oriented. Making certain offences prosecutable through the Mobile Courts Act, 2009 risks weakening due-process and fair-trial guarantees in cases involving contested speech and serious criminal consequences. Adding more state officials to the National Cyber Protection Council while removing representation from the National Human Rights Commission risks reinforcing executive dominance without institutional safeguards. The amendments also expand the government's rule-making powers over online content and platform regulation, leaving significant aspects to executive discretion without legislative scrutiny.

This imbalance is illustrated in revisions to Section 8, which further empower the Ministry of Information and Broadcasting, alongside other executive agencies, to seek removal of a wider range of content on expanded grounds — without clear procedural standards, notice to affected users, independent scrutiny, or effective avenues of appeal.

Our recommendations

We, the undersigned, call on the government to:

- 1. Withdraw the current draft of the amendments to Cyber Protection Act, 2026.**
- 2. Open a meaningful, time-bound consultation process involving civil society, media practitioners, legal experts, technologists, and other relevant stakeholders before taking further steps.**
- 3. Draft a revised version underpinned by wide stakeholder consultations that addresses broader concerns in cyberspace and empowers Bangladeshi citizens, while being aligned with Bangladesh's obligations under international human rights law.**



In solidarity:

1. Tech Global Institute
2. Transparency International Bangladesh
3. Cyber Support for Women and Children Platform
4. Bangladesh Legal Aid and Services Trust
5. Ain o Shalish Kendro
6. Article 19
7. Bangladesh Internet Governance Forum
8. Bangladesh Mohila Parishad
9. Bandhu Social Welfare Foundation
10. Cyber Crime Awareness Foundation
11. Cyber teens
12. Digitally Right
13. Human Rights Support Society
14. Institute for Informed Development
15. Manusher Jonno Foundation
16. Naripokkho
17. Orroddho Foundation
18. The Tech Academy
19. Voice