To,
Mr. Tarique Rahman
Honourable Prime Minister
Government of the People's Republic of Bangladesh
—

Subject: supporting a progressive digital reform agenda for Bangladesh

Bangladesh's digital reforms are at a turning point. We, the undersigned organisations, urge your government to protect what has been achieved, restore the safeguards that have been stripped away, and build a legal and institutional framework that centres people's rights, democratic accountability, and a free, open and secure internet.

Digital reform is an essential part of delivering on your **stated commitment** to strengthen accountability and prevent authoritarianism. Laws and institutions governing online expression, privacy, cybersecurity, surveillance and artificial intelligence shape how people participate in public life, access services, organise, communicate and hold power to account.

Prior to the interim government assuming office, the *Digital Security Act, 2018 (DSA) and Cyber Security Act, 2023 (CSA)* were **repeatedly used to target journalists, activists and others for online expression**, internet **shutdowns were imposed** during periods of political mobilisation; and **surveillance and interception capabilities expanded** without sufficient transparency or independent oversight. Some reforms were initiated during the interim administration, which included somewhat **narrowing the criminalisation of some forms of online expression** through the repeal of the CSA and enactment of the Cyber Security Ordinance, 2025, introducing requirements for explicit consent to process personal data with exemptions to such protection in limited circumstances under the **Personal Data Protection Ordinance, 2025**, and establishing a **prohibition on internet shutdowns**, now retained in ***section 63 of the Bangladesh Telecommunication (Amendment) Act, 2026***, which amends *section 97 of the Bangladesh Telecommunication Regulation Act, 2001*.

The subsequent legislative process has exposed how easily rights safeguards can be weakened while broader state powers remain intact. The Bangladesh Telecommunication (Amendment) Act, 2026 kept the Ordinance's **wide interception powers** but removed or diluted several safeguards. The Ordinance had **abolished the National Telecommunication Monitoring Centre (NTMC)** and replaced it with the Centre for Information Support, prohibited interception for political or ideological purposes, and required every interception to be approved by a court or review council under detailed conditions. But the 2026 Act reversed all three. According to section 64 of the 2026 Act, which amends section 97(A) of the 2001 Act, interception may now be approved **by a court or simply by "an authority constituted by the government",** and the government alone decides which agency carries it out. The NTMC, **whose operations were extended for another year by the Ministry of Home Affairs**, continues to function without a clear, public-facing statutory mandate, independent oversight framework or meaningful transparency requirements. The *Personal Data Protection Act, 2026*, likewise, **exempts state authorities on broad and undefined grounds such**

as national security, public order and public interest, without judicial supervision or any duty of transparency when the exemption on consent requirements for the processing of personal information is invoked.

These concerns are not abstract. The **UN fact-finding investigation** into the events of July and August 2024 described how surveillance-derived intelligence was used in connection with repression of civil and political rights. A **government committee subsequently reviewed** the procurement and use of surveillance technologies, but its report has still not been made public.

At the same time, proposals to criminalise "rumours", "disinformation", and "defamatory information" through **amendments to the *Cyber Security Act 2026*** would reverse the progress made by repealing earlier speech offences. Our objection is not to how these terms are drafted but to treating them as crimes at all. Under international human rights law, the dissemination of false or unverified information is not in itself a legitimate ground for criminal sanction; the UN Human Rights Committee has made clear that imprisonment is never an appropriate penalty for defamation. The vaguely defined proposed offences fail this test: for instance, "rumours" could cover any unverified information that creates, or merely risks creating, confusion or unrest, and the offence could carry up to five years' imprisonment. This would stifle debate and discussion and have a chilling effect on free speech. Bangladesh's experience under the DSA and CSA demonstrates the dangers of broadly worded offences that give authorities significant discretion to decide what information is false, harmful or unacceptable. Introducing these speech offences would appear to be incompatible with Article 39 of Bangladesh's Constitution, which guarantees freedom of speech and expression, and with Article 19 of the International Covenant on Civil and Political Rights (ICCPR), which, as the UN Human Rights Committee explained in General Comment No. 34, permits restrictions on freedom of expression only when these are provided by law, pursue a legitimate aim, and meet strict tests of necessity and proportionality.

Digital reform must therefore be approached holistically as a connected agenda. Removing speech offences from one law will have limited effect if expression can be restricted through other criminal, telecommunications or cybersecurity powers. Rights to privacy and protection of personal data cannot be meaningfully ensured if state authorities are allowed unchecked access to the personal information of citizens on overbroad grounds, without sufficient statutory guardrails. And cybersecurity cannot be strengthened by weakening the security and confidentiality of people's communications. Effective security and respect for human rights are not competing objectives; they reinforce one another.

Bangladesh is also developing a new framework for artificial intelligence. We welcome elements of the draft National AI Policy that recognise a risk-based approach, enhanced safeguards for high-risk systems, human oversight, transparency, and restrictions on uses such as social scoring and indiscriminate biometric surveillance. These commitments should be translated into enforceable safeguards before high-impact systems are deployed in areas such as policing, welfare, healthcare, education or access to public services.

We therefore urge your government to:

- Protect freedom of expression and access to information. Refrain from introducing criminal offences concerning “rumours”, “disinformation”, “defamatory information” or similar categories of expression.
- Review laws regulating online expression taking into consideration Bangladesh’s Constitution and its obligations under international human rights law including the ICCPR, and ensure that restrictions on content in any framework are lawful, necessary, proportionate and subject to effective independent and judicial review.
- Guarantee access to the broadest possible internet connection for all. Preserve and fully implement the prohibition on internet shutdowns introduced through the telecommunications reform process, and ensure it cannot be circumvented through throttling, service-specific restrictions, whitelisting or other measures that render communications and information inaccessible.
- Drop the proposed offence of 'belittling' or 'bullying', which now expressly includes caricatures, memes, and synthetic content, and would impose criminal liability on internet users creating and/or sharing content depicting satire, cartoons, and political criticism, or content involving critical reporting, thereby curtailing free speech and civic participation. Add safeguards for public-interest expression, coverage of investigations, political commentary, satire, and good-faith reporting, and extend these protections to all journalists, including local and independent journalists and those attached to unregistered media outlets, and sources and whistleblowers, as well as researchers and fact-checkers. Withdraw the power to suspend or cancel the registration or licence of media outlets based on content published online.
- Reform surveillance, interception and data-access powers. Establish clear statutory limits, prior independent judicial authorisation and effective parliamentary and independent oversight of surveillance and interception. Impose restrictions on the currently broad exemptions from data protection obligations for state authorities, ensure strict limits on data collection, retention and sharing, strengthen transparency around the procurement and use of surveillance technologies, and publish the report of the committee that reviewed surveillance procurement.
- Ensure cybersecurity powers are used to protect systems and people. Cybersecurity institutions should have clearly defined mandates, reporting and redressal mechanisms, independent oversight and safeguards preventing cybersecurity infrastructure from being used for political surveillance or content control. Bangladesh should protect strong encryption, including end-to-end encryption, and reject exceptional-access requirements that weaken secure communications.
- Build human rights protections into AI governance from the outset. High-risk AI systems should be subject to prior human rights and security impact assessments, transparency, meaningful human oversight, independent scrutiny and effective remedies. Uses of AI that are incompatible with fundamental rights, including indiscriminate biometric mass surveillance and social scoring should be prohibited. There must be accountability for the ways in which AI tools collect and retain data, and use data for training and targeted ads. The regulatory framework must push for the development and deployment of privacy-preserving AI.

- Facilitate participatory public consultations on proposed legal and policy reforms that meaningfully engage a wide range of actors, including civil society, fact-checkers, journalists, human rights defenders, legal, forensic, tech and cyber experts and frontline service providers, and representatives of communities most likely to be significantly and disproportionately affected by policy frameworks regulating the online and digital space. Draft laws and policies should be made available in full with the official translations in relevant languages, including English, with sufficient time for scrutiny. Ensure regulatory and oversight bodies are independent from the executive to scrutinise state power rather than administer it.

Bangladesh has an opportunity to move beyond a cycle in which one restrictive digital framework is replaced by another while the structures enabling arbitrary control remain unchanged. The reforms of the past two years show that meaningful change is possible. The task now is to preserve those gains, address the safeguards that remain absent or have been weakened, and ensure that future reforms do not recreate the same avenues for censorship, surveillance and abuse. To this end, it is imperative that the government visibly engage in a rights-respecting legislative and policy reform process, which can be initiated in the forthcoming parliamentary sessions, through steps to extend review of the proposed amendments to the Cyber Security Act, scrap proposed offences that restrict and criminalise free speech, and work with key stakeholders to build in substantive, procedural and infrastructural changes that strengthen protection of fundamental rights.

The attached Core Principles for Rights-Respecting Digital Governance in Bangladesh set out in greater detail the standards that we believe should guide the implementation and further development of Bangladesh's digital policy framework.

We respectfully urge your government to take forward this reform agenda through an open and consultative process, and we remain ready to engage constructively in support of it.

Sincerely,

Access Now
Activate Rights.
Asia Democracy Network (ADN)
CIVICUS: World Alliance for Citizen Participation
Committee to Protect Journalists
Digitally Right
Odhikar
Southeast Asia Freedom of Expression Network (SAFEnet)
Tech Global Institute
Transparency International Bangladesh (TIB)

Core principles for digital rights policies

- **Access to the internet:**
  - Internet shutdowns, throttling, service specific blocking, whitelisting of permitted services or connections and any means of intentional disruption of access to the internet and digital communications platforms even in times of crisis must be prohibited. Internet shutdowns are inherently disproportionate and cause severe harms to human rights, particularly for marginalised and at-risk communities and individuals.
  - There must be no discrimination between types of services or content to be accessed through the internet, through a policy of net neutrality.

- **Content governance:**
  - Content governance policies must have a clear legal basis, a precisely outlined scope, and specific application. This is necessary for certainty, foreseeability, and to avoid creating a "chilling effect" on free speech.
  - Content governance policies must not give the government unilateral or overbroad powers to block and remove content and their implementation must be subject to independent oversight. People must have an enforceable right to redressal, including judicial review, against restrictions on speech and expression.
  - Content governance policies must incorporate the need for social media services and other private companies with an effect on online speech to protect people's human rights. This can include holding platforms accountable by requiring meaningful transparency reports, consultations with stakeholders in policy and product development.
  - Platform accountability must not become a tool for censorship — content governance policies must allow for exemptions from liability with clear and reasonable conditions for liability which do not incentivize private companies to take down more speech than is necessary.
  - Content governance policies must not impose any general monitoring obligations on digital platforms, nor create arbitrary or disproportionate take-down procedures. . They should clearly identify the specific types of illegal content which are to be targeted and adopt different response mechanisms to address them. Rights-respecting notice-and-action procedures must be adopted to ensure that the concerned person is given a hearing, and has access to independent review and redressal mechanisms.
  - Cybersecurity and cybercrime laws must not be used to criminalise expression. offences relating to expressions such as "rumours," "disinformation," defamation, criticism or other forms of lawful expression should not be introduced through cybercrime legislation.

- **Privacy and security:**
  - The state must not compel digitalisation of public services linked to a centralised digital ID without a prior, public assessment of their necessity and proportionality

at both the policy and system level. Such systems must be subject to impact and need assessments, offer equally-accessible non-digital alternatives, ensure strong security for people's personal data, and operate with full transparency.
    - The state must establish strong cyber security standards and practices, and ensure good cyber hygiene incorporating independent audits, research, and feedback.
    - Strong encryption, including end-to-end encryption, must be protected. The state must not require backdoors, exceptional access mechanisms, traceability requirements or other measures that systematically weaken encrypted communications.
    - The state must implement frameworks for accountability and transparency into the use of spyware and surveillance technology, including by law enforcement. People must be able to question the government and know how their privacy is affected.
    - Surveillance and interception powers must be clearly provided by law and comply with the principles of legality, necessity and proportionality. Their use must be subject to independent authorisation and oversight, and effective remedies must be available where surveillance powers are misused.

- **Data protection:**
    - Data protection laws must prioritise privacy and be based on core principles, including fair and lawful use; purpose and retention limitations; data minimisation; necessity and proportionality; accuracy, integrity and confidentiality; users' rights; and adequacy for cross-border data flows. These principles must be asserted and incorporated in the law.
    - People must have explicitly stated actionable rights, including the right to information about how their data is being used and to object to any such use; to erasure, rectification, and explanation; and to portability, which ensures that digital service providers are unable to exploit users by locking them into their service. This also places an obligation on data controllers, including the state, to implement human rights respecting data practices.
    - The state and its agencies must not be exempted as such from data protection obligations. The state tends to be the biggest collector and user of people's data, which can lead to the building of surveillance systems. Inter-agency data sharing must be subject to strict conditions and aligned with data protection principals.
    - Data protection laws must not give the state a wide discretionary power to exempt entities from data protection obligations. Exemptions must be reasonable and proportionate. For example, it is reasonable to exempt journalists from the obligation to not publish personal data when there is a legitimate public interest in such information.
    - Formulation, implementation and enforcement of data protection policies requires an independent, well-resourced data protection authority with binding powers, technical and adjudicatory functions, and the ability to engage with all stakeholders. It must be institutionally independent from the bodies responsible for operating or coordinating government data systems, and people must have access to effective complaint and redress mechanisms.

- **Artificial intelligence:**
    - Human rights must be a core principle governing the development and use of artificial intelligence and automated decision-making systems. High-impact areas require stricter safeguards.
    - Applications of artificial intelligence and automated decision-making that are incompatible with fundamental human rights must be prohibited.
    - The use of AI in high-impact areas, including public services, healthcare, education, law enforcement and other areas affecting people's rights and access to essential services, must be subject to stronger safeguards, meaningful consultation and human rights impact assessments.
    - All public-sector uses of artificial intelligence and automated decision-making systems must be transparent, including through publicly accessible information on where and for what purposes such systems are being used.
    - People must not be subject to decisions with legal or similarly significant effects solely through automated processes. They must be able to seek meaningful human review, request an explanation, challenge the decision and access effective redress.
    - The state must prohibit the use of artificial intelligence-based facial recognition systems for widespread use in public spaces, where meaningful consent or choice are not possible.
    - AI systems must protect people's privacy and personal data by default, and AI tools should not weaken existing security protections, including encryption.