Why Independent Regulation Matters for Bangladesh's Digital Future: Proposed Way Forward to Protect Users' Rights

Overview

Between 2024 and 2026, Bangladesh's interim administration and the subsequent elected government implemented a series of large-scale and consequential reforms to the country's digital regulatory landscape. For an emerging economy, the availability and accessibility of digital technologies is essential to economic development and public life, and their effective regulation helps safeguard resources, enhance market competitiveness, protect user rights, and ensure that national regulatory frameworks align with international standards.

The Global Network Initiative (GNI) has worked closely with stakeholders in Bangladesh over the last two years on critical questions surrounding data protection, content governance, internet shutdown, and communications surveillance. Drawing on its multistakeholder model and over two decades of experience engaging with governments on international human rights frameworks and industry best practices, GNI supported dialogue among government, industry, and civil society to advance transparent and accountable rulemaking. However, the government's commitment to a digital regulation that is proportional and fit-for-purpose so far remains largely unfulfilled.

How regulations are developed and enforced can be as important as their substance, and many of the newly passed laws replicate gaps in accountability, transparency, and proportionality similar to what stakeholders faced during engagement with the laws under the previous administrations. The objective is not less regulation, but better regulation that is independently and responsibly administered, participatory, effective, and sustainable.

An independent regulation requires regulatory decisions to be made within clear statutory mandates, using transparent procedures, technical expertise, and meaningful as well as timely stakeholder participation, and to remain subject to effective accountability and review. Such regulation is typically carried out by a statutory body that operates independently of the government and the organizations it regulates, thereby reducing the extent to which its decisions are subject to political, commercial, and other external influences. Under Bangladesh's current regulatory landscape, however, decision-making is centralized and top-down, vesting significant authority in the executive branch of government to appoint regulators, exercise control over regulatory operations, oversee enforcement, maintain substantial financial control, shape policy direction, and issue binding directions, which creates the challenge of concentrated power with limited checks and balances and constrains regulators' institutional and operational autonomy. Strengthening regulatory independence can help create greater regulatory certainty for businesses, investors, innovators, and the public, while fostering conditions that support investment, innovation, and broader economic activity. It can help ensure technically complex decisions are based on evidence and expertise, reducing the risk of arbitrary or politically influenced enforcement, ultimately strengthening public confidence and institutional legitimacy.

The case for moving beyond centralized, top-down regulation

One of the primary challenges impeding Bangladesh's digital economy is the trust deficit and insufficient institutionalized engagement among the government, regulatory bodies, technology companies, civil society, academic sector, and investors. This leads to miscommunication and lack of constructive dialogue, weak oversight and accountability, underutilization of technical and policy expertise, and a lack of effective checks and balances.

For instance, over the last decade, successive governments in Bangladesh have relied heavily on content-based restrictions to tackle the spread of mis- and disinformation, without establishing adequate notice-and-action procedures or other comparable mechanisms, an approach technology policy experts have widely viewed as ineffective and prone to infringing on fundamental rights. To achieve better outcomes, multiple jurisdictions including the European Union (EU), the United Kingdom (UK), Australia, and Brazil are shifting towards systemic regulation – a regulatory framework, enforced by independent regulatory agencies, which relies on systems-based and structural risk management as an instrument to establish a baseline of accountability, enhance the compliance and responsibility of regulated entities (e.g., social media companies), and shape their obligations to safeguard national interests and user rights.

Effective regulation depends on cross-sector expertise. While the government maintains the fundamental duty to respect, protect, and fulfill human rights, it often lacks the technical insights needed to adequately assess the operational nuances of complex digital platforms and fulfil its duties under constitutional and international law. To bridge this gap, industry and technical experts can provide the necessary operational context, while civil society and academia can offer critical perspectives on how policy impacts people in practice. Bangladesh can leverage this collective knowledge by establishing a collaborative environment where regulatory bodies consult diverse stakeholders and independently enforce policies and evaluate their implementations. A more decentralized framework also helps insulate regulatory decisions from undue political or commercial pressure.

Risk	Consequence
Regulatory uncertainty	Sudden directives or unclear allocation of responsibilities can increase compliance costs and discourage investment.
Concentration of powers	Combining policy-making, regulatory, enforcement, content-control, and evaluation functions can weaken institutional checks and balances.

Technical misalignment	Rules developed without sufficient technical and industry expertise may be difficult or costly to implement.
Operational disruption	Broad network restrictions can affect financial services, commerce, education and essential communications.
Rights risks	Restrictions on online expression, privacy or access to information may lack sufficient safeguards, proportionality and/or independent review.

These risks are particularly significant as Bangladesh implements a new generation of digital laws, including: the Cyber Protection Act, 2026, the Personal Data Protection Act, 2026, the National Data Management Act, 2026, and the Bangladesh Telecommunication (Amendment) Act, 2026. Effective implementation of these laws will not only depend on their substance, but also on the institutional structures, safeguards, and decision-making processes that govern their application.

Priorities for Stronger Digital Regulation

The next phase of reform should translate international good practice and principles into concrete changes to Bangladesh's regulatory architecture. Based on GNI's longstanding experience in the intersection of technology and human rights, five practical priorities stand out:

1. The government should retain responsibility for setting national policy objectives, while regulatory bodies such as the Bangladesh Telecommunication Regulatory Commission (BTRC) and the National Cyber Security Agency should have sufficient autonomy and resources to implement those objectives through predictable rules and participatory multistakeholder input, and without political or administrative influence.

2. Appointment, tenure, removal, financing, and operational arrangements should protect regulators from inappropriate political or administrative interference, while embedding strict mechanisms for transparency and institutional accountability. To ensure independent regulatory power is balanced with public trust, regulators' operations, annual auditing reports, and human rights due diligence (HRDD) assessments must be made proactively and publicly accessible, ensuring full accountability to Parliament, judicial authorities, and the general public.

3. Regulators must be equipped with adequate technical expertise, financial resources, data access, and institutional capacity as a core condition for effective oversight. As digital governance expands to cover increasingly complex domains, regulators require specialized skills and tools to execute their statutory mandates competently and keep pace with technological change. The regulatory and governance environment should leverage a full spectrum of oversight tools. Incorporating co-regulation, industry self-regulation, and independent multistakeholder benchmarks alongside statutory rules ensures that governance

remains agile, rights-respecting, and technically aligned with rapid advancements in AI, platform architectures, and digital services.

4. Digital legislation, regulation, and policies should be published with sufficient time for meaningful and informed stakeholder input. Consultations should be ongoing, inclusive, and iterative, providing stakeholders with meaningful opportunities to engage throughout the development, implementation, and review of regulatory measures. The government should publish necessary translation of key documents, a summary of substantive feedback received, and explain any departures from consultation recommendations.

5. Regulations and policies should be accompanied by an assessment of their impacts on the economy, technology, competition, privacy, and human rights, including consideration of less restrictive alternatives. One or more dedicated, functionally independent parliamentary committees should undertake the assessment, with the authority to commission independent expert analysis and seek evidence from civil society, academia, industry, and other relevant stakeholders, before significant regulatory measures are adopted.

6. Decisions affecting network access, online content, privacy, or other fundamental rights should have clear legal thresholds, written reasons, prior judicial authorization where appropriate, and accessible mechanisms for independent review and post-facto judicial challenge.

GNI is committed to constructive engagement with the government and other stakeholders, and stands ready to share its global experience, convene relevant expertise, and support efforts to develop a digital regulatory framework that is effective, rights-respecting, and fit for purpose. Stronger institutions and more transparent processes will not only strengthen protections for users, but also provide greater certainty for businesses, investors, and innovators and help build public confidence in Bangladesh's digital future.

About the Global Network Initiative (GNI)

GNI is the leading multistakeholder organization for accountability, shared learning, and collective advocacy on government and company policies and practices at the intersection of technology and human rights. Founded in 2008, GNI is a trusted forum for more than 120 members in our tech company, NGO, academic, and investor constituencies spread across six continents – including organizations active in Bangladesh, such as Google, Meta, Telenor, Cloudflare, Tech Global Institute, and Digitally Right Limited. Over the last several years, GNI has reviewed, commented on, and helped shape a range of "online safety" bills, data protection laws, and intermediary liability laws across several jurisdictions.