Criminalizing Online Speech: Cyber Laws and Freedom of Expression in Bangladesh and Nigeria

By Md Ashraful Bari [1] and Tamanna Jahan Tanni [2]

[1] Tulane University; mbari@tulane.edu
[2] Northern Illinois University; ttanni1@niu.edu

1. INTRODUCTION

The growing use of cyber laws in the Global South raises concerns over the criminalization of online speech and the protection of freedom of expression. Bangladesh and Nigeria have the most similar classification, with contextual differences and comparable cyber policy challenges.[1] Both countries have cyber laws that have been amended over time due to their draconian provisions and condemned by various stakeholders for violations of human rights and suppression of free speech. However, the amendments to these laws have not achieved the desired outcomes.

While cyber policies often focus on protecting against cyber fraud, online humiliation, harassment, and threats, vague and overbroad definitions and inconsistent enforcement blur the line between criticism and defamation. This brief seeks to address two key questions. First, how do cyber laws in Bangladesh and Nigeria criminalize online speech? Second, what are the implications for freedom of expression? Understanding these distinctions is crucial for developing clearly defined cyber laws that protect free speech and expression. Drawing on the evolution of cyber laws in Bangladesh and Nigeria, this brief offers policy recommendations to legislators in Bangladesh, Nigeria, and other African countries revising cyber laws.

2. RESEARCH METHODS

This brief employs a qualitative comparative analysis of cyber laws in Bangladesh and Nigeria, focusing on the periods from 2006 to 2026 for Bangladesh and from 2015 to 2026 for Nigeria. These two countries are selected because, while both have adopted and later modified cyber laws, they fail to

[1] Bangladesh and Nigeria are classified as "partly free" in the Freedom House "Freedom in the World 2026" report, with scores of 44 out of 100 for political rights and civil liberties (Freedom House, 2026a, 2026b).

adequately protect freedom of expression. For content analysis, the brief draws on approximately thirty secondary data sources, including journal articles, International NGO reports, government policy documents, newspaper reports, and information from International NGOs and government websites, as well as policy advocacy websites, using keywords such as cyber laws, cybercrime, online censorship, arbitrary arrest, etc.

3. KEY INSIGHTS

Evolving cyber laws struggle to protect freedom of expression in Bangladesh and Nigeria.

Bangladesh adopted the first Information and Communication Technology Act (ICTA) in 2006 due to the internet's growing negative effects on citizens' lives and property. However, section 57 of the ICTA was used to launch an unprecedented crackdown on individuals' fundamental rights, particularly freedom of speech and expression (Bari & Dey, 2019, p. 598).[2] The situation worsened with the amendment of this act in 2013, which deviates from international law by allowing police to arrest without a warrant (ICJ, 2013a). Due to the growing criticisms, the government was forced to repeal the act in 2018, with the adoption of the Digital Security Act (DSA) 2018 (Bari & Dey, 2019, p. 612). Yet this new law created a culture of fear because it incorporated previous sections and laws with harsher penalties (Riaz, 2021; Bhowmik & Fisher, 2026, p. 152).

After widespread criticism of the DSA (Mahmud, 2023; Amnesty International, 2018), the government replaced the law with the Cyber Security Act (CSA) of 2023 (CFJ & CGS, 2025). However, CSA was simply a renamed version of the DSA (Amnesty International, 2024). Following mass protests and the overthrow of the Hasina government in August 2024, Bangladesh's interim government announced a review of the CSA and later published the Cyber Security Ordinance (CSO) in 2025, with significant changes, such as eliminating nine speech-restrictive clauses inherited from the DSA and CSA,

[2] Section 57 (ICTA 2006) criminalizes the publication of online material by stating "If any person deliberately publishes or transmits or causes to be published or transmitted in the website or in electronic form any material which is fake and obscene or its effect is such as to tend to deprave and corrupt persons who are likely, having regard to all relevant circumstances, to read, see or hear the matter contained or embodied in it, or causes to deteriorate or creates possibility to deteriorate law and order, prejudice the image of the State or person or causes to hurt or may hurt religious belief or instigate against any person or organization, then this activity of his will be regarded as an offence" (UNODC, n.d.).

decriminalizing criticism, and formalizing internet access protections (CFJ & CGS, 2025). Recently, Bangladesh's newly elected government made changes to the CSO, including defining offences with vague terms, dismantling some CSO safeguards, and imposing disproportionate penalties (The Daily Star, 2026). The proposed Cyber Protection Act (CPA) 2026 raises concerns about digital rights, online and press freedom (TIB, 2026; The Daily Star, 2026). Thus, the CPA poses serious risks to human rights and freedom of expression, and it mirrors previous cyber laws in Bangladesh.

Conversely, the Nigerian government enacted the Cybercrimes Act in 2015 to combat internet fraud and criminal activity. However, the draconian provision in section 24(1) of the law allowed the authorities to suppress and harass critics, activists, opposition members, and journalists, among others (Amnesty International, 2026; Ogun, 2024).[3] For example, in 2024, lawyer and activist Dele Farotimi was arrested on defamation charges for his book criticizing Nigeria's criminal justice system, resulting in nationwide protests and debates concerning free speech and expression (Osuagwu, 2025). This law was challenged in the Federal High Court, Court of Appeals, and Supreme Court for violating free speech (Ogun, 2024). Eventually, on March 25, 2022, the Economic Community of West African States (ECOWAS) Court ruled that section 24 of the act was arbitrary, vague, and repressive, and ordered Nigerian authorities to stop using it (Amnesty International, 2025). Section 24 was later amended by the Nigeria Cybercrimes (Amendment) Act 2024, which was adopted on February 28, 2024. However, in April 2024, Nigeria's National Human Rights Commission (NHRC) and, later on June 11, 2025, ambassadors from various countries, including the United States, the United Kingdom, Finland, Canada, and Norway, expressed concerns about the amendments (Chioma, 2025), citing growing evidence of misuse of this law.

Vague and overbroad cyber laws allow for the criminalization of online speech.

[3] Section 24 (Cybercrimes Act 2015) criminalizes online freedom of expression by stating "Any person who knowingly or intentionally sends a message or other matter by means of computer systems or network that - (a) is grossly offensive, pornographic or of an indecent, obscene or menacing character and causes any such message or matter to be so sent; or (b) he knows to be false, for the purpose of causing annoyance, inconvenience, danger, obstruction, insult, injury, criminal intimidation, enmity, hatred, ill will or needless anxiety to another or causes such a message to be sent (Policy Registry, n.d.)"

Bangladesh's ICT law of 2006 used several vague and overbroad provisions to define offenses (Rahman, 2014, p. 12), undermining the right to free expression (ICJ, 2013a). For example, section 57, used terms like "creates the possibility" and "may hurt" for defining offense. Furthermore, this section fails to define "tend to deprave" and "corrupt persons," as well as terms such as "publication of information" and "type of information." Sections 25 and 29 of the DSA were most frequently used against journalists because of their ambiguous terms, including "to annoy or insult" and "false information to affect reputation" (CFJ, 2025). Section 31 was used to address actions like "deteriorating the law and order," where the terms defined broadly enough that anyone could be arrested under this section. Using the DSA, anyone could file police complaints and cases against journalists based solely on allegations, even if they were not the direct victims of the online speech (CFJ, 2025). Additionally, the draft CPA 2026 includes several ambiguous terms, including "rumors," "defamation," and "humiliation," which are broad and open to subjective interpretation. These provisions may allow for significant misapplication and arbitrary enforcement (CIVICUS, 2026).

Comparably, the Nigerian Cybercrimes Act contains ambiguous words in several sections (Akua, 2025), allowing authorities to easily manipulate online speech to silence journalists, activists, and anyone else who criticizes. For example, the 2015 law used words like "causing annoyance", "inconvenience", or "ill will" to arrest and detain anyone under section 24 (Ogun, 2024; The Guardian, 2025). Even after amendments, the new law in 2024 criminalizes "misleading" and "false" posts, which may silence dissents (Gyang, 2025). The term "cyberstalking" is also so broad that almost any type of online criticism can be considered criminal activity (Oshunfunrewa, 2026).

Inconsistent enforcement of cyber laws undermines their effectiveness.

In Bangladesh, the amendments to cyber laws were nothing short of draconian (HRW, 2023; ICJ, 2013a). For instance, under the ICT act in 2013, the arbitrary detention of human rights organization *Odhikar*'s Director Nasiruddin Elan (ICJ, 2013b) and the refusal of bail to *Odhikar* Secretary Adilur Rahman Khan (ICJ, 2013c) illustrate the attack on freedom of expression. Moreover, journalists facing DSA charges were often arrested and subject to pretrial detention due to non-bailable provisions where the cases were essentially bailable. Ninety percent of the journalists faced

forced arrest without following any arrest safeguards (CFJ, 2025). Indeed, of the 418 cases filed between January 2020 and October 2021, 31.6% were filed by law enforcement agencies and government officials in Bangladesh for allegedly violating the DSA despite not being personally harmed or defamed by the law itself (Riaz, 2021).

In Nigeria, around 45 cases of attacks on journalists and media houses were reported only between May 2023 and April 2024, of which 60% were carried out by Law enforcement agencies (Ezeamalu, 2024). Only in 2022, 45.31% of the recorded incidents (29 cases) of attacks on freedom of expression were carried out by law enforcement and security agents, while 4.38% were done by government officials (Media Rights Agenda, n.d.). For example, in May 2024, journalist Daniel Ojukwu of the Foundation for Investigative Journalism (FIJ NG) was detained allegedly for publishing articles about procurement fraud against a government official, while the executive director, a reporter, and lawyers of the International Center for Investigative Reporting (ICIR) were detained following an interrogation by the Nigeria Police Force (PLAC, 2025).

4. POLICY RECOMMENDATIONS

Clarify legal definitions and terminology.

Lawmakers in Bangladesh and Nigeria should remove broad and ambiguous language from cyber laws. These vague and overly broad terms limit free expression and facilitate censorship. To prevent the misuse of cyber laws, lawmakers should include clear legal definitions for potential misappropriation in the cyber sector. These laws should distinguish between harm, offense, and discomfort. The laws' predictable application would ensure consistent compliance with the rule of law. Thus, establishing legality and certainty would effectively discourage cybercrime.

Decriminalize defamation.

To differentiate between legitimate criticism of government and defamation, Bangladeshi and Nigerian legislators should consider decriminalizing defamation and address it through civil law. This would prevent cyber law abuse and state harassment of dissenting opinions. Civil remedies can offer a balance between freedom of expression and reputational harm with proportionate measures. The UN Human Rights Committee's General Comment No. 34 recommends decriminalizing defamation and emphasizes that imprisonment is not an appropriate penalty (Human Rights Committee, 2011). Similarly, the African Commission's 2019 Declaration of Principles on Freedom of Expression and Access to Information in

Africa prioritizes protecting freedom of expression while respecting reputational rights (ACHPR, 2019). Therefore, civil remedies can address defamation without criminalizing it.

Strengthen judicial oversight.

There should be Independent judicial oversight to govern the implementation of cyber laws. The judiciary should review arrests and prosecutions, and there should be judicial warrants for surveillance or content removal. In the event of formal proceedings, the law should clearly state due process and provide adequate monitoring. There should be provisions for the right to appeal, which would allow people to challenge decisions made against them. Furthermore, any complaints about the authority's misuse of the legislation should lead to an independent review of executive action.

Periodically review cyber laws.

Due to rapid changes in technology, its usage, and emerging threats, Bangladeshi and Nigerian lawmakers should regularly review cyber laws for assessing human rights impacts. Legislation should include review provisions for regular assessments. Regular legislative reviews would benefit victims and alleged perpetrators by addressing rapid technological changes, assessing proportionality, and adhering to international human rights standards. The legislators should also facilitate different stakeholders and civil society to engage when reviewing legislation. Overall, consensus-based cyber legal reform would make cyberspace safer for everyone.

5. REFERENCES

African Commission on Human and Peoples' Rights (ACHPR). (2019). *Declaration of principles on freedom of expression and access to information in Africa*. https://caselaw.ihrda.org/api/files/1605623598849dpiuruykv5p.pdf

Akua, N. (2025). How anti-cybercrime laws are being weaponized to repress journalism. *Columbia Journalism Review*. https://www.cjr.org/analysis/nigeria-pakistan-jordan-cybercrime-laws-journalism.php

Amnesty International. (2018). *Bangladesh: New Digital Security Act imposes dangerous restrictions on freedom of expression*. https://www.amnesty.org/en/latest/news/2018/09/bangladesh-new-digital-security-act-imposes-dangerous-restrictions-on-freedom-of-expression/

Amnesty International. (2024). *Bangladesh: Repackaging repression: The Cyber Security Act and the continuing lawfare against dissent in Bangladesh*.

https://www.amnesty.org/en/documents/asa13/8332/2024/en/

Amnesty International. (2026). Nigeria 2025. https://www.amnesty.org/en/location/africa/west-and-central-africa/nigeria/report-nigeria/

Amnesty International Nigeria. (2025). "Direct DSS to stop intimidating the media" – Amnesty, SERAP tell President Tinubu. https://www.amnesty.org.ng/2025/02/26/direct-dss-to-stop-intimidating-the-media-amnesty-serap-tell-president-tinubu/

Bari, M. E., & Dey, P. (2019). The enactment of digital security laws in Bangladesh: No place for dissent. *The George Washington International Law Review*, 51, 595-631.

Bhowmik, S., & Fisher, J. (2026). Defensive journalism in Bangladesh: Consequences of the Digital Security Act on journalism practice. *Digital Journalism*, 14(1), 147-166. https://doi.org/10.1080/21670811.2024.2406861

Chioma, U. (2025). Preventing misuse of the Cybercrimes Act: Protecting free speech and unlocking economic growth. *TheNigeriaLawyer*. https://thenigerialawyer.com/preventing-misuse-of-the-cybercrimes-act-protecting-free-speech-and-unlocking-economic-growth/

CIVICUS. (2026). *Bangladesh: Draft Cyber Protection (Amendment) Act 2026 poses serious risk to freedom of expression and mirrors the Digital Security Act used to repress human rights defenders and journalists*. https://civicus.org/index.php/media-resources/news/8806-bangladesh-draft-cyber-protection-amendment-act-2026-poses-serious-risk-to-freedom-of-expression-and-mirrors-the-digital-security-act-used-to-repress-human-rights-defenders-and-journalists

Clooney Foundation for Justice, & Centre for Governance Studies. (2025). *Press freedom in Bangladesh: Lessons from the Digital Security Act*. https://cfj.org/reports/press-freedom-in-bangladesh-lessons-from-the-digital-security-act/

Ezeamalu, B. (2024). Nigeria: Cybercrime law still used to harass citizens despite amendment. *The Africa Report*. https://www.theafricareport.com/348123/nigeria-cybercrime-law-still-used-to-harass-citizens-despite-amendment/

Freedom House. (2026a). *Bangladesh: Freedom in the world 2026 country report*. https://freedomhouse.org/country/bangladesh/freedom-world/2026

Freedom House. (2026b). *Nigeria: Freedom in the world 2026 country report*. https://freedomhouse.org/country/nigeria/freedom-world/2026

Gyang, H. (2025). *Nigeria's cybercrime reform. National Assembly Library Trust*

Fund. https://naltf.gov.ng/nigerias-cybercrime-reform/

Human Rights Committee (HRC). (2011). *General comment No. 34: Article 19-Freedoms of opinion and expression* (CCPR/C/GC/34). United Nations. https://digitallibrary.un.org/record/715606

Human Rights Watch (HRW). (2023). *Bangladesh: Quash conviction and release rights defenders*. https://www.hrw.org/news/2023/09/14/bangladesh-quash-conviction-and-release-rights-defenders

International Commission of Jurists. (2013a). *Bangladesh: Information and Communication Technology Act draconian assault on free expression*. https://www.icj.org/resource/bangladesh-information-and-communication-technology-act-draconian-assault-on-free-expression/

International Commission of Jurists. (2013b). *Bangladesh: Immediately release human rights defender Nasiruddin Elan*. https://www.icj.org/bangladesh-immediately-release-human-rights-defender-nasiruddin-elan/

International Commission of Jurists. (2013c). *Bangladesh: Authorities should immediately drop their opposition to Adilur Rahman Khan's bail application*. https://www.icj.org/bangladesh-authorities-should-immediately-drop-their-opposition-to-adilur-rahman-khans-bail-application/

Mahmud, F. (2023). Bangladesh to tone down "draconian" digital security law. *Al Jazeera*. https://www.aljazeera.com/news/2023/8/7/bangladesh-to-tone-down-draconian-digital-security-law

Media Rights Agenda. (n.d.). *Stifling freedom of expression in Nigeria: Annual report of attacks on free expression and media freedom in 2022*. https://mediarightsagenda.org/stifling-freedom-of-expression-in-nigeria-annual-report-of-attacks-on-free-expression-and-media-freedom-in-2022

Ogun, F. (2024). *Understanding Nigeria's Cybercrimes Act and its implementation mechanism. Centre for Journalism Innovation and Development*. https://thecjid.org/understanding-nigerias-cybercrimes-act-and-its-implementation-mechanism/

Oshunfunrewa, M. (2026). Should Cybercrimes (Amendment) Act 2024 be scrapped? *Tribune Online*. https://tribuneonlineng.com/should-cybercrimes-amendment-act-2024-be-scrapped/

Osuagwu, P. (2025). How misuse of Cybersecurity Act cost Nigeria N1.1 trn in 7 years. *Vanguard*. https://www.vanguardngr.com/2025/08/ho

w-misuse-of-cybercrime-act-cost-nigeria-n1-1trn-in-7-yrs/

Policy and Legal Advocacy Centre. (2025). *The police, Sowore and abuse of the Cybercrime Act*. https://placng.org/Legist/the-police-sowore-and-abuse-of-the-cybercrime-act/

Policy Registry. (n.d.). *Cybercrime Act 2015*. https://policyregistry.org/documents/cybercrime-act-2015/details

Rahman, M. H. (2014). Freedom of speech & expression in Bangladesh in the context of ICT Act 2006. *SSRN*. https://doi.org/10.2139/ssrn.3840306

Riaz, A. (2021). *How Bangladesh's Digital Security Act is creating a culture of fear*. Carnegie Endowment for International Peace. https://carnegieendowment.org/research/2021/12/how-bangladeshs-digital-security-act-is-creating-a-culture-of-fear

The Daily Star. (2026). Any cyber law reform must uphold digital rights, not undermine them. https://www.thedailystar.net/opinion/views/news/any-cyber-law-reform-must-uphold-digital-rights-not-undermine-them-4293306

The Guardian. (2025). To flush cybercrime law of ambiguity and enforcement impunity. https://guardian.ng/opinion/to-flush-cybercrime-law-of-ambiguity-and-enforcement-impunity/

Transparency International Bangladesh. (2026). *Draft Cyber Protection (Amendment) Act, 2026 poses serious risks to freedom of expression and speech; TIB calls for comprehensive revision in light of stakeholder views*. https://www.ti-bangladesh.org/en/articles/press-release/7550

United Nations Office on Drugs and Crime. (n.d.). *Information and Telecommunication Act*. SHERLOC. https://sherloc.unodc.org/cld/document/bgd/2006/information_and_telecommunication_act.html

Institute for Research and Policy Integration in Africa (IRPIA) *is a pan-African think tank serving as a hub for the fusion of evidence-based research with pressing public policy issues.*

Institute for Research and Policy Integration in Africa (IRPIA)
84 Bato, Regent, Freetown
Sierra Leone
Email: irpia@irpia.org
www.irpia.org