

Media Regulation in the Digital Age: A Comparative Analysis of Nigeria and Bangladesh

ABUBAKAR UMAR GACHI¹, MARYAM ETI SHEHU², JOSEPH OJOMUGBO BALA³,
MOHAMMED MUSA SALEH⁴, MUSA GARBA BABA⁵
^{1,2,3,4,5}. ICT Department, National Space Research and Development Agency (NARSDA)

Abstract- *This study examines the difficulties of policing free speech in the internet era by contrasting Bangladesh and Nigeria. As lower-middle-income democracies with active online populations, both countries are increasingly concerned about digital dissent, hate speech, and disinformation. To investigate three main themes (1) ambiguous and punitive legal frameworks, (2) misinformation as a rationale for censorship, and (3) surveillance and platform governance—the study employs a qualitative comparative case study methodology and consults legal texts, civil society reports, and secondary literature. The results show that the wording of Bangladesh's Digital Security Act (2018) and Nigeria's Cybercrimes Act (2015) is unclear, allowing for selective enforcement against people, journalists, and activists. The study concludes that while regulation of digital harms is necessary, the current approaches in Nigeria and Bangladesh prioritize state control over fundamental freedoms, undermining democratic values. Despite these challenges, opportunities for reform are emerging. Civil society organizations, judicial interventions, and international human rights advocacy continue to push for greater accountability, transparent platform governance, and alignment of national laws with global standards. While disinformation is a real threat during elections and protests, governments in both contexts frequently weaponize it to suppress opposition rather than promote transparency. Additionally, surveillance regimes and opaque partnerships with global technology platforms further erode user rights and civic trust. Maintaining democratic governance in the digital age requires a rights-based framework that strikes a balance between security considerations and freedom of speech.*

Keywords: Media, Regulation, Digital Age, Security.

I. INTRODUCTION

The nature of public discourse, speech, and state control have all changed dramatically in the digital age. Global internet platforms that facilitate mass content transmission and real-time communication

have supplanted traditional gatekeepers like newspapers, broadcasters, and regulatory bodies. Although democratic engagement has increased as a result of this evolution, there are now serious governance issues. Global worries about striking a balance between free speech and social protection have been sparked by the proliferation of hate speech, disinformation, and online harassment (Gillespie, 2018; Gorwa, 2019). To counter these challenges, governments all over the world are creating more and more legislative and policy frameworks; yet, many of these measures raise grave concerns about censorship, overreach, and the degradation of fundamental rights.

Many states struggle with how to protect the right to free speech while regulating harmful online information. The cross-border nature of platforms like Facebook, Twitter, and YouTube, as well as the development of digital technology and opaque content control processes, make this especially challenging. Furthermore, governments frequently confuse criticism with destabilization in politically unstable or semi-authoritarian settings, and regulation turns into a means of stifling dissent (Freedom House, 2022). While authoritarian governments frequently place a higher priority on speech repression, democracies struggle with the accountability of tech platforms. In hybrid regimes, like those in the Global South, where authoritarian practices coexist with democratic institutions, these dynamics are particularly complicated.

Bangladesh and Nigeria provide interesting case studies for examining this regulatory conundrum. Both are majority-populated, lower-middle-income democracies with thriving online communities and high social media usage rates. However, both governments have enacted contentious legislation to

regulate digital speech—Bangladesh's Digital Security Act (2018) and Nigeria's Cybercrimes Act (2015)—and have used false information and national security as excuses for speech limitations (Iwuoha & Ezeibe, 2021; Haque, 2021). Even while freedom of expression is formally protected by the constitution, there are still many restrictions in practice.

Understanding not only the regulatory instruments but also the institutional and political environments in which they function requires a comparative perspective. Although Bangladesh and Nigeria have different governance cultures, legal traditions, and histories, they both have authoritarian tendencies when it comes to handling online dissent. We can spot reoccurring trends like ambiguous legal wording, selective enforcement, and government-platform conflict by examining how free expression is regulated in these two nations. Additionally, in the Global South, where public faith in institutions is frequently low and state capacity may be limited, such study provides insight into the interactions between local regulatory frameworks and global platform governance (Gorwa, 2019; Mwakalombe, 2021).

The regulation of digital speech in Bangladesh and Nigeria, as well as the wider ramifications for democratic governance, are critically compared in this paper. It focuses on three interconnected topics: (1) institutional and legal frameworks for media regulation; (2) the use of false information as an excuse to censor speech; and (3) the role of surveillance and data protection in speech governance. Use case studies, civil society reports, and recent academic literature, the paper illustrates the similarities and differences in their regulatory strategies. It makes the case that although both nations are legitimately threatened by online harm, their regulatory approaches frequently jeopardize democratic norms, especially civil liberties, accountability, and freedom of expression.

II. LITERATURE REVIEW: REGULATING FREE SPEECH IN THE DIGITAL AGE

The Digital Dilemma: Free Expression vs Regulation

Particularly in nations with weak or hybrid democratic institutions, the emergence of digital technology and social media has reshaped the parameters of free expression. Online platforms have allowed previously unheard-of levels of civic engagement, but they have also made it easier for hate speech, false information, and political disinformation to proliferate. To maintain information integrity, national security, and public order, nations are progressively imposing regulatory authority over digital spaces (Gillespie, 2018; Gorwa, 2019).

There is a basic conflict between preventing injury and preserving free speech in this regulatory tendency. Rahman (2020) asserts that governments in transitional democracies frequently enact restrictive legislation that, while seemingly reasonable, really work to quell opposition. Bangladesh and Nigeria provide a striking example of this tension. Both nations have implemented laws that purport to fight "fake news," but they have drawn harsh criticism for facilitating censorship and making free expression illegal (Freedom House, 2022).

Vague and Punitive Legal Frameworks

The use of ambiguously written legislative instruments that provide state authorities considerable discretion is one of the most frequently mentioned issues in the literature on digital regulation. The Cybercrimes (Prohibition, Prevention, etc.) Act of 2015 in Nigeria makes several online behaviors illegal, such as defamation and cyberstalking, however it is unclear what exactly qualifies as "offensive" or "false" content (Ojebode et al., 2021). According to critics, the law has been frequently applied to detain bloggers, journalists, and members of civil society on general charges of defamation or cyberbullying (Iwuoha & Ezeibe, 2021).

In a same vein, anyone found to post or distribute content that "creates unrest," "hurts religious sentiments," or "defame the image of the state" may be arrested under Bangladesh's 2018 Digital Security Act (Haque, 2021). Reporters, cartoonists, and even students have been imprisoned under these regulations for posting on social media. Specifically, Article 19 of the International Covenant on Civil and

Political Rights is cited by scholars as being violated by this legislation in terms of freedom of expression (Khan, 2022).

Such legal tools not only make it difficult to distinguish between political criticism and damaging information, but they also have the chilling effect of making people self-censor in order to protect themselves from state reprisals. The fundamental democratic ideals that Bangladesh and Nigeria uphold by their constitutions are compromised by this.

Misinformation as Justification for Censorship

In both nations, disinformation has become a significant governance concern, especially during elections, medical emergencies, and demonstrations. According to scholars, false information has the potential to polarize societies, undermine public trust, and provoke violence (Iwuoha & Ezeibe, 2021; Rahman & Ahmed, 2021). During the 2019 general elections and the #EndSARS protests in Nigeria, false information was widely disseminated via Facebook groups and WhatsApp. Similar patterns were seen in Bangladesh during the 2018 general elections, when modified photos, fake news, and deepfakes were widely shared online (Haque, 2021). The state's response has frequently veered into digital totalitarianism, even though misinformation poses a genuine threat. The governments of Bangladesh and Nigeria have centralized authority over what is deemed "true" or "false," frequently coordinating these definitions with the objectives of the ruling parties rather than enabling independent fact-checkers. This increases public mistrust and damages the legitimacy of regulatory initiatives.

State-Centric Surveillance and Data Governance

The rise of surveillance-based governance structures in both nations is another important theme in literature. While Western data privacy rules (like the EU's GDPR) are based on user rights, emerging economies frequently implement data policies that prioritize control and national security. Although it lacks a solid civil remedy and an independent enforcement authority, Nigeria's 2019 Nigeria Data Protection Regulation (NDPR) offers a loose framework for data governance (Abubakar, 2020).

The Personal Data Protection Act that Bangladesh has proposed, however, is criticized by academics for prioritizing government access to personal data over user rights (Khan, 2022). Actors from civil society are concerned that this legislation will provide authorities with more authority to keep an eye on citizens, online activity in the name of data protection or crime prevention.

According to Gorwa (2019) and Gillespie (2018), platform regulation and surveillance frequently coexist in weak democracies. Under the guise of digital regulation, governments can more easily target journalists, human rights advocates, and political dissidents selectively due to a lack of judicial monitoring and transparency in data use.

Platform Governance and the Role of Tech Companies

Platform governance is an expanding area of research examining how multinational internet companies such as Facebook, Google, and Twitter operate in countries including Bangladesh and Nigeria. These platforms act as both mediators and enforcers of online speech, determining what content remains available, what is removed, and which accounts are suspended (Gillespie, 2018). In both countries, platforms have faced government pressure to remove flagged content, often without transparent review procedures. For example, Facebook removed hundreds of posts in Nigeria and Bangladesh following government complaints (Freedom House, 2022).

Leerssen (2020) therefore advocates for greater transparency in platform algorithms and content-moderation practices, particularly in non-Western contexts where civil rights protections and democratic institutions may be weaker. Without independent accountability mechanisms, platform regulation may effectively become a tool for online repression.

Thematic Summary

The literature converges on three key themes:

- i. The use of vague laws to criminalize digital speech,

- ii. The misuse of misinformation narratives to suppress dissent, and
- iii. The entrenchment of surveillance and platform control as tools of digital governance.

Bangladesh and Nigeria both have authoritarian inclinations in digital regulation, while having diverse political structures and legal traditions. According to academics, the main issue is not whether regulation is required, but rather how it should be conceived, carried out, and justified. There is a chance that justifiable governance issues may be used as pretexts to restrict free expression, which is becoming more and more common in both nations.

III. MATERIALS AND METHOD

Research Design

To investigate how Bangladesh and Nigeria control and limit free expression in the digital era, this study uses a qualitative, comparative case study methodology. Given the emphasis on institutional practices, legal frameworks, and government policy, a comparative analysis makes it possible to identify both commonalities and differences between the two nations' practices (Yin, 2018). Nigeria and Bangladesh were specifically chosen because they are both sizable, lower-middle-income democracies in the Global South with strong civil societies, substantial internet penetration, and a history of both authoritarian responses to protest and constitutional protections (Freedom House, 2022).

The study intends to investigate legislative frameworks, enforcement trends, and normative tensions surrounding free expression rather than test hypotheses. Because it places more emphasis on context, meaning making, and power dynamics than on numerical generalization, this interpretivist method is appropriate for the subject (Neuman, 2014).

Data Sources

The research is grounded in secondary sources, including:

- Peer-reviewed academic literature on digital media regulation, comparative governance, and human rights;
- Country-specific legal documents such as Nigeria's Cybercrimes Act (2015) and Bangladesh's Digital Security Act (2018);
- Policy reports and indices from organizations like Freedom House, Reporters Without Borders, and Article 19;
- News archives and case studies documenting enforcement actions (e.g., arrests, platform bans);
- Platform transparency reports (e.g., Facebook and Twitter's removal data) relevant to government takedown requests.

Literature was chosen using terms like free-speech Nigeria, Digital Security Act Bangladesh, cybercrime laws, and social media regulation from databases including Scopus, Google Scholar, and JSTOR. The inclusion of documents was based on their scholarly legitimacy, relevance to digital media, and recentness (2015–2023).

Analytical Framework

A thematic comparison framework guides the analysis. A synthesis of the literature led to the pre-definition of three main themes: (1) legal and legislative frameworks; (2) the use of disinformation narratives; and (3) data privacy and surveillance (Gorwa, 2019; Gillespie, 2018). To enable both intra-country description and cross-country comparison, data from every nation was tagged under these categories.

Each theme was analyzed by asking:

- What legal tools are used to regulate speech online?
- How are these tools justified (e.g., national security, public order)?
- Who are the primary targets of enforcement (e.g., journalists, activists)?
- What are the implications for freedom of expression, accountability, and civic trust?

The method ensures a structured but flexible analysis, allowing for the emergence of contextual nuances while maintaining thematic consistency.

Case Selection Justification

Bangladesh and Nigeria were chosen because their system designs were the most similar (Lijphart, 1971). Both postcolonial democracies have engaged online communities, politicized law enforcement, and continuing discussions on legal change in relation to digital governance. However, their levels of regulatory aggression vary; Nigeria's regulatory environment is more fragmented and contested, whereas Bangladesh exhibits more centralized control (Iwuoha & Ezeibe, 2021; Haque, 2021).

By examining these two nations, one can gain a practical grasp of how global discourses like "fighting fake news" are localized in different political and legal frameworks. Analytical depth and generalizability within comparable sociopolitical situations are improved by this comparative logic.

Limitations

This study's limitations as a desk-based investigation stem from its dependence on publicly accessible resources. Its lack of original interviews, ethnographic information, and official answers may limit how thoroughly it examines enforcement tactics or intentions. Furthermore, access to specific legal information may be limited because a large number of court cases and legal papers in both nations are not usually fully translated or digitized.

Reports from NGOs and the media may also be biased, particularly in situations when opinions are divided. In order to counteract this, the study triangulates data from a variety of sources and, when feasible, gives priority to scholarly research and data from global watchdogs. The methodology permits a thorough, comparative, and context-sensitive investigation of the research question in spite of these drawbacks.

IV. RESULTS AND DISCUSSION

The difficulties in policing and defending free expression in Bangladesh and Nigeria are compared thematically in this section. Three main conclusions can be drawn from an analysis of secondary literature, legal texts, and civil society reports: (1) both nations use punitive and ambiguous laws to

control online speech; (2) they use false information to defend censorship; and (3) they show increasing inclinations towards digital surveillance and state-aligned platform governance. The following analysis of these findings focusses on the consequences for civil liberties and democratic government.

Vague Laws as Tools of Control

Bangladesh and Nigeria have both enacted laws from the digital age that make online speech illegal under vague and generalized definitions. The Cybercrimes (Prohibition, Prevention, etc.) Act of 2015 in Nigeria has drawn a lot of criticism for its ambiguously worded provisions on "cyberstalking" and "defamation." When online activists, journalists, or political opponents criticize public officials, these rules are frequently used to arrest them (Iwuoha & Ezeibe, 2021). For example, several journalists have been prosecuted for writing pieces that are said to damage the reputation of government agencies.

The Digital Security Act (DSA) of 2018 has also emerged as a key instrument in Bangladesh for quelling opposition. The Act makes it illegal to publish or distribute any content that is thought to be "offensive," "false," or "defamatory" about the government, religion, or public personalities. According to Haque (2021) and Khan (2022), the absence of distinct legal thresholds grants authorities broad authority to interpret and apply the law in whatever way they see fit. The DSA has resulted in scores of arrests as of 2022, many of which have been made against journalists and social media users who have made critical remarks about the administration.

Comparative Insight: Although digital dissent is illegal in both nations, Bangladesh's enforcement is more systematic and forceful. Opposition media are often suppressed by the DSA, frequently during pre-election periods. In contrast, enforcement in Nigeria is more irregular and politicized, with security agencies employing the Cybercrimes Act as a crude instrument rather than through formal judicial proceedings. However, in both situations, the existence of ambiguous rules permits legal harassment, which suppresses free expression.

Misinformation as a Regulatory Justification

The threat of "fake news" or misinformation is being used by governments in Bangladesh and Nigeria more frequently as an excuse to impose stricter speech regulations. Misinformation has been especially harmful in Nigeria during social rallies like the #EndSARS campaign, national elections, and ethnic conflicts. Political and communal divisions have been widened by the spread of provocative rumors on social media platforms, especially Facebook and WhatsApp (Ibrahim, 2020). The Nigerian government has responded by considering stricter rules on social media sites and proposing changes to the NBC Code.

Similar trends have been seen in Bangladesh, particularly during the COVID-19 pandemic and the 2018 general elections. There was a lot of misinformation spread about political rivalries and religious matters, which occasionally led to mob violence (Rahman & Ahmed, 2021). In response, the government used the DSA to make mass arrests and remove content, claiming that these actions were required to stop societal unrest. Civil society organizations contend, however, that these measures unfairly single out dissident voices rather than the real spreaders of misinformation (Freedom House, 2022).

Comparative Insight: Even though disinformation poses serious problems for both states, their regulatory remedies lack multi-stakeholder, transparent, and independent governance systems. The judicial and security forces have direct influence over Bangladesh's more centralized reaction. Nigeria's is more disjointed and involves both ad hoc presidential decrees and regulators such as the NBC. Digital literacy, fact-checking capabilities, and algorithmic transparency—all crucial for combating false information at its source rather than just penalizing its dissemination—are not adequately funded in any scenario.

Surveillance and Platform Governance

Under the pretext of public order or national security, Nigeria and Bangladesh are both progressively using surveillance-based approaches to digital governance. Although the Nigeria Data Protection Regulation

(NDPR) offers a flexible framework for the regulation of personal data in Nigeria, institutional independence and enforcement are lacking (Abubakar, 2020). There have been reports of unlawful use of digital monitoring tools and phone tracking to spy on journalists and opponents, especially during election seasons or large-scale demonstrations (Iwuoha & Ezeibe, 2021).

Bangladesh's proposed Data Protection Bill gives the government extensive authority to access user data without judicial scrutiny, seemingly offering nothing in the way of user privacy (Khan, 2022). Furthermore, it has been alleged that organizations like the Rapid Action Battalion (RAB) have tracked and arrested protesters using internet monitoring technologies. Bangladesh's paradigm, according to Haque (2021), is a classic example of digital authoritarianism, in which individual liberties are subordinated to state security.

Another crucial element of this monitoring trend is platform regulation. Governments in both nations frequently ask Facebook, YouTube, and Twitter to remove content. Despite their claims to implement content restrictions consistently, research indicates that these platforms are more likely to comply with government requests in nations with less press freedom (Gorwa, 2019). In 2020, for example, Facebook deleted hundreds of posts in Bangladesh after receiving complaints from the authorities (Freedom House, 2022).

Comparative Insight: Nigeria displays a patchwork of regulatory and security agency actions, whereas Bangladesh exemplifies a more centralized and systemic form of digital surveillance. However, platform governance is nonetheless opaque and unduly reliant on unofficial state-platform interactions in both situations, with neither transparency nor significant user rights. Both nations fail to guarantee independent judicial review of removal or surveillance orders, and neither has completely established a rights-based framework for platform responsibility.

Democratic Implications and Institutional Fragility
According to the results in these three areas, regulating digital speech presents significant institutional issues for Bangladesh and Nigeria. Although freedom of expression is officially recognized in both nations, their regulatory frameworks frequently operate against the principles of the constitution. Dissent is not only discouraged but criminalized in this governance context because of ambiguous rules, politicized enforcement, and securitized data regimes.

Public trust, democratic accountability, and media independence are all impacted by these trends. For fear of being arrested, journalists are becoming increasingly self-censored. Online organization is more difficult for civil society organizations. Both digital censorship and digital disinformation can distort elections. Such circumstances, according to Leerssen (2020) and Gillespie (2018), produce an ecosystem of "platform repression," in which platforms and the government fail to adequately serve the public interest.

Furthermore, abuse is rarely stopped since there is a lack of independent regulators or strong legal oversight. Although Nigerian courts do occasionally challenge censorship, their impartiality varies. When it comes to implementing digital rules, Bangladesh's judicial institutions have generally sided with the executive branch (Rahman, 2020). Under the guise of regulatory necessity, democratic principles are weakened as a result.

Emerging Opportunities for Reform

There are new prospects in spite of these obstacles. In both nations, civil society organizations are becoming more active in promoting digital rights, demanding that cyber laws be changed, and asking platforms to be more transparent. The legal community in Nigeria has started contesting certain provisions of the Cybercrimes Act in court, while activists and journalists in Bangladesh are still resisting the DSA's expansive wording.

Both administrations have also been urged by international organizations, including the EU, the African Commission on Human and Peoples' Rights,

and the UN Human Rights Council, to harmonize domestic laws with global human rights norms. Frameworks that strike a compromise between user rights and public interest regulation can be inspired by models like the EU's General Data Protection Regulation (GDPR) (Gorwa, 2019).

However, consistent pressure from both above and below—through conditional funding, diplomatic lobbying, and cross-border regulation standards—as well as from below—through civic involvement, legal mobilization, and regional solidarity—will be necessary for reform.

V. CONCLUSION

Through a comparative comparison of Bangladesh and Nigeria, this paper has critically addressed the difficulties in regulating and safeguarding free expression in the digital age. Although both nations have constitutional guarantees for free speech and function under ostensibly democratic frameworks, there are significant inconsistencies in their digital governance systems. The main conclusion is that in both situations, laws that are ambiguous, punitive, and politically motivated—like Bangladesh's Digital Security Act (2018) and Nigeria's Cybercrimes Act (2015)—are increasingly restricting free speech. These laws are frequently justified by the need to fight misinformation or maintain national unity (Haque, 2021; Iwuoha & Ezeibe, 2021).

The comparative study also discovered that both nations use disinformation narratives as a tool to justify censorship and quell political dissent. In both states, regulatory measures prioritize punitive control over preventive or instructional strategies, despite the fact that digital misinformation does represent actual concerns, especially during elections and protests (Rahman & Ahmed, 2021; Ibrahim, 2020). Governments frequently rely on takedowns, internet shutdowns, and arrests rather than investing in public awareness campaigns or transparent platform engagement. These reactions undermine democratic accountability, diminish public trust, and encourage self-censorship among activists, journalists, and regular people.

Additionally, state-centric monitoring and opaque platform governance are becoming more prevalent in Bangladesh and Nigeria, where governments are pressuring private tech companies to delete or censor information without following the proper legal procedures (Gorwa, 2019). Such monitoring systems function without sufficient checks and balances in the absence of strong data protection laws and independent regulatory bodies, endangering people's civil liberties and privacy.

Both nations show areas of resistance and reform potential in spite of these obstacles. More accountability in digital regulation has been demanded by human rights organisations worldwide, journalists in Bangladesh, and legal challenges in Nigerian courts (Freedom House, 2022; Leerssen, 2020). These pressures offer a starting point for reconsidering how to better safeguard free expression while simultaneously addressing the justifiable negative effects of the digital ecosystem.

Recommendations

Both Nigeria and Bangladesh need to reevaluate their institutional and legislative frameworks in order to strike a balance between the protection of free speech and the regulation of dangerous information. The evidence-based suggestions listed below are meant to encourage that change:

Revise and Clarify Legal Frameworks

To ensure that ambiguous phrases like "false information," "offensive content," and "defamation" are precisely defined, narrowly circumscribed, and in line with international human rights norms, governments should conduct a thorough review of the current cybercrime and digital security legislation (Khan, 2022). Due process should be protected, and speech that simply expresses dissident views or critiques government actions should not be criminalized. Stakeholder consultations, judicial panels, and legal reform commissions can all support the revision process's legitimacy and openness.

Establish Independent Digital Regulation Authorities
Establishing autonomous, multi-stakeholder regulatory organisations to supervise digital media regulation would be advantageous for both nations.

Civil society, academia, the legal profession, the commercial sector, and the media should all be represented in these organisations. They would be in charge of examining requests for material removal, keeping an eye on platform agreements with the government, and making sure that laws uphold the rights to privacy and freedom of speech. The perception and use of regulation as a political tool will persist in the absence of such independent scrutiny.

Promote Transparency and Accountability in Platform Governance

Governments ought to demand more openness from tech firms doing business in their countries, including regular updates on data sharing policies, algorithmic content filtering, and takedown requests. The rights of users must not be jeopardized in the process. Platforms must reject excessive political influence while simultaneously being subject to local standards. Co-developed with civil society, a code of conduct for platform-state engagement can offer procedural and ethical principles.

Invest in Media Literacy and Counter-Misinformation Initiatives

Governments should prioritize proactive strategies to counter misinformation rather than merely using punitive measures. These include funding for investigative journalism, collaborations with independent fact-checkers, public awareness campaigns, and digital literacy initiatives in schools. Research from other nations demonstrates that enhancing citizens' ability to recognize false information is more democratic and successful than limiting free expression (Gillespie, 2018).

Strengthen Data Privacy and User Rights Protections

Strong data protection rules that put user rights first must be in place to restrain the growth of surveillance-based governance. In order to create independent enforcement authorities, offer legal recourse for rights abuses, and guarantee that surveillance technology cannot be used without judicial authorization, Nigeria's NDPR and Bangladesh's proposed Data Protection Bill need be amended. Since people cannot freely express

themselves in a setting where surveillance is ubiquitous, privacy is fundamental to free speech.

Engage in Regional and Global Dialogue

Lastly, both nations ought to take a more active role in regional and global forums pertaining to media freedom and digital rights. Collaboration with organizations such as the African Union, SAARC, the UN Human Rights Council, and civil society networks can assist align domestic laws with global standards. Furthermore, opportunities to exchange experiences and jointly create frameworks appropriate for their political and cultural settings are provided by global south-to-south cooperation.

In the end, democratic legitimacy should not be sacrificed in the sake of regulating digital expression. Even in the digital era, Nigeria and Bangladesh need to abandon a government model that views dissent as a threat and adopt one that values free speech as a fundamental democratic principle. In addition to being morally required, a legislative framework that promotes open communication, guarantees institutional accountability, and protects civil freedoms is also strategically sound. Free speech-protected societies are better able to endure false information, foster trust, and negotiate the challenges of the digital age.

REFERENCES

- [1] Abubakar, A. (2020). Media regulation and democratic governance in Nigeria. *Journal of African Media Studies*, 12(3), 421–437. https://doi.org/10.1386/jams_00025_1
- [2] Freedom House. (2022). Freedom on the Net 2022: Nigeria and Bangladesh country reports. <https://freedomhouse.org/report/freedom-net/2022>
- [3] Gillespie, T. (2018). *Custodians of the Internet: Platforms, Content Moderation, and the Hidden Decisions That Shape Social Media*. Yale University Press.
- [4] Gorwa, R. (2019). The platform governance triangle: Conceptualizing the informal regulation of online content. *Internet Policy Review*, 8(2). <https://doi.org/10.14763/2019.2.1398>
- [5] Haque, M. (2021). Digital authoritarianism in Bangladesh: The impact of the Digital Security Act 2018 on free speech. *Asian Journal of Comparative Politics*, 6(4), 450–466. <https://doi.org/10.1177/20578911211027418>
- [6] Ibrahim, J. (2020). Social media, elections, and democratic consolidation in Nigeria. *African Journal of Democracy and Governance*, 7(1), 65–82.
- [7] Iwuoha, V. C., & Ezeibe, C. C. (2021). Social media, fake news, and Nigeria's struggle for democracy. *Social media + Society*, 7(2), 1–12. <https://doi.org/10.1177/20563051211019098>
- [8] Khan, A. (2022). Freedom of expression under siege in Bangladesh: An assessment of the Digital Security Act. *Journal of South Asian Development*, 17(2), 133–151. <https://doi.org/10.1177/09731741221105675>
- [9] Leerssen, P. (2020). The soapbox as a black box: Regulating transparency in social media recommender systems. *European Journal of Law and Technology*, 11(2).
- [10] Lijphart, A. (1971). Comparative politics and the comparative method. *American Political Science Review*, 65(3), 682–693. <https://doi.org/10.2307/1955513>
- [11] Mwakalombe, G. (2021). Comparative perspectives on digital media regulation in Africa and Asia. *Journal of Information Policy*, 11(1), 120–140. <https://doi.org/10.5325/jinfopoli.11.2021.0120>
- [12] Neuman, W. L. (2014). *Social research methods: Qualitative and quantitative approaches* (7th ed.). Pearson.
- [13] Ojebode, A., Adedoyin, T., & Ojo, T. (2021). State power and digital dissent: The #EndSARS movement in Nigeria. *African Affairs*, 120(481), 499–514. <https://doi.org/10.1093/afraf/adab015>
- [14] Rahman, M. (2020). Press freedom in Bangladesh: Navigating censorship and control. *Media Asia*, 47(2–3), 105–118.

<https://doi.org/10.1080/01296612.2020.1829043>

- [15] Rahman, M., & Ahmed, S. (2021). Fake news and elections in Bangladesh: Challenges and implications. *Journal of Information Technology & Politics*, 18(2), 178–194. <https://doi.org/10.1080/19331681.2021.1910753>
- [16] Yin, R. K. (2018). *Case study research and applications: Design and methods* (6th ed.). Sage Publications.