

**INTERNATIONAL JOURNAL OF LAW
MANAGEMENT & HUMANITIES**
[ISSN 2581-5369]

Volume 9 | Issue 5

2026

© 2026 *International Journal of Law Management & Humanities*

Follow this and additional works at: <https://www.ijlmh.com/>

Under the aegis of VidhiAagaz – Inking Your Brain (<https://www.vidhiaagaz.com/>)

This article is brought to you for free and open access by the International Journal of Law Management & Humanities at VidhiAagaz. It has been accepted for inclusion in the International Journal of Law Management & Humanities after due review.

In case of **any suggestions or complaints**, kindly contact support@vidhiaagaz.com.

To submit your Manuscript for Publication in the **International Journal of Law Management & Humanities**, kindly email your Manuscript to submission@ijlmh.com.

Reconceptualising the Right to Freedom of Expression in Nigeria's Digital Environment

POLYCARP ARINZE OKORO*  AND YAHAYA UMAR**

ABSTRACT

The widespread emergence of digital technology has greatly changed the nature of freedom of expression by redefining how opinions are generated, disseminated, and contested within the public domain. Although freedom of expression is guaranteed under the Constitution of the Federal Republic of Nigeria 1999 (as amended), the growth of social media platforms and State control practices have created a complex regulatory and constitutional conundrum. This article examines freedom of expression as it operates within Nigeria's digitally mediated public sphere, assessing whether existing constitutional safeguards remain adequate to address the contemporary challenges posed by digital innovation. It explores the relationship between constitutional speech rights and regulatory measures such as the Cybercrimes (Prohibition, Prevention, etc.) Act and other policy instruments regulating online expression. Through doctrinal and comparative legal analysis, the article posits that current regulatory approaches, if not properly applied, may decimate democratic engagement and frustrate legitimate expression. It therefore advocates a constitutionally grounded, proportionate, and rights-oriented framework for the regulation of speech, which reconciles the protection of fundamental freedoms with the State's legitimate interests in security, public order, and the management of harmful online content.

Keywords: *Freedom of expression, Digital rights, African Charter, Constitutional law, Freedom of information*

I. INTRODUCTION

The digital innovation of communication has tremendously altered the method of conveying ideas in modern societies. In Nigeria, the advent of social media platforms has enlarged the public sphere beyond traditional media practices.¹ Digital technologies now enable citizens to take part effectively in political discourse, social mobilisation, and public accountability. This trend has moved freedom of expression from a largely traditional civil liberty into a central pillar of digital democratic engagement.²

* Author is a Lecturer at the Faculty of Law, University of Calabar, Cross River State, Nigeria. ORCID: <https://orcid.org/0009-0004-5046-9250>

** Author is a Lecturer at the Nigerian Law School, Port Harcourt Campus, Nigeria.

¹ MANUEL CASTELLS, COMMUNICATION POWER (Oxford Univ. Press 2009).

² JÜRGEN HABERMAS, THE STRUCTURAL TRANSFORMATION OF THE PUBLIC SPHERE: AN INQUIRY INTO A CATEGORY OF BOURGEOIS SOCIETY (Thomas Burger & Frederick Lawrence trans., MIT Press 1989).

Freedom of expression is expressly contained in Nigeria's constitutional framework. Section 39 of the Constitution of the Federal Republic of Nigeria 1999 (as amended) guarantees the right to hold opinions and to receive and impart ideas and information without interference.³ Judicial interpretation of this provision has historically developed within the context of conventional media structures such as newspapers, radio, and television.⁴ The contemporary digital environment, however, presents situations that were neither contemplated nor directly addressed by the framers of the Constitution. The decentralised, transnational, and algorithm-driven nature of digital communication has complicated the application of established constitutional principles.⁵

The expansion of digital platforms has simultaneously empowered citizens and unsettled regulatory institutions. On the one hand, digital technologies have lowered barriers to participation, amplified marginalised voices, and facilitated civic engagement.⁶ On the other hand, they have raised concerns relating to misinformation, hate speech, national security, cybercrime, and public order.⁷ In response, the Nigerian State has been using statutory instruments, regulatory policies, and executive actions to govern online expression. Measures such as the Cybercrimes (Prohibition, Prevention, etc.) Act 2015, broadcasting regulations with digital reach, and episodic restrictions on online platforms reflect an evolving regulatory posture toward digital speech.⁸ These developments have generated serious constitutional tensions.

II. THE CONSTITUTIONAL AND REGIONAL ARCHITECTURE FOR FREEDOM OF EXPRESSION

According to Okoye and others, constitutional protection is general in nature.⁹ The legal foundation of freedom of expression in Nigeria is embedded in the Constitution of the Federal Republic of Nigeria 1999 (as amended). While section 39(1) of the Constitution provides a broad guarantee of the freedom to hold opinions and impart information,¹⁰ that right is

³ CONSTITUTION OF THE FEDERAL REPUBLIC OF NIGERIA (1999) (as amended), § 39. It is pertinent to note that while section 39(1) guarantees the right to "impart ideas", section 39(3) saves laws that are "reasonably justifiable in a democratic society" for specified purposes, including that of preventing the disclosure of information received in confidence.

⁴ *Director of SSS v. Olisa Agbakoba* (1999) 3 NWLR (Pt. 595) 314 (SC).

⁵ L. Edwards, *Freedom of Expression and the Internet*, 36 COMPUTER L. & SEC. REV. 100 (2018).

⁶ ZEYNEP TUFEKCI, *TWITTER AND TEAR GAS: THE POWER AND FRAGILITY OF NETWORKED PROTEST* (Yale Univ. Press 2017).

⁷ U.N. HUMAN RIGHTS COUNCIL, *Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression*, U.N. Doc. A/HRC/38/35 (Apr. 6, 2018).

⁸ Cybercrimes (Prohibition, Prevention, etc.) Act, 2015 (Nigeria).

⁹ A. Obi Okoye, B. Chigozie Umenzekwe & Polycarp Arinze Okoro, *Powers of the Legislature in the Removal of Judicial Officers in Nigeria under the 1999 Constitution*, 2 INT'L J.L. & CLINICAL LEGAL EDUC. 32 (2021).

¹⁰ CONSTITUTION OF THE FEDERAL REPUBLIC OF NIGERIA (1999) (as amended), § 39(1).

immediately circumscribed by section 45, which permits laws that are reasonably justifiable in a democratic society in the interest of defence, public safety, public order, public morality or public health.¹¹ Historically, the Nigerian judiciary has struggled to define the precise boundary of what is reasonably justifiable, often granting the executive wide latitude when national security is invoked as a defence for restricting speech.

Nigeria's domestic constitutionalism does not, however, exist in a vacuum. As a party to the African Charter on Human and Peoples' Rights, Nigeria is bound by article 9, which provides that every individual shall have the right to receive information and to express and disseminate opinions within the law.¹² The African Commission on Human and Peoples' Rights has made clear that the phrase "within the law" must not be read as a blank cheque for domestic legislation to nullify the Charter's protections; any restrictive law must instead meet the international standards of proportionality and necessity.¹³

This regional oversight has been fortified by the ECOWAS Community Court of Justice. In the landmark case of *SERAP v. Federal Republic of Nigeria*,¹⁴ the Court held that the suspension of a digital platform, specifically Twitter, by the Nigerian government was unlawful, as it lacked a clear legal basis and was not necessary in a democratic society.¹⁵ That ruling established a critical precedent: digital expression is protected under the same regional umbrella as traditional speech, and any State interference must be grounded in a law that is accessible, certain, and predictable.

Furthermore, the principle of legality requires that laws restricting speech, such as the Cybercrimes Act, be drafted with enough precision to allow citizens to regulate their conduct. Where a statute uses vague terminology, it fails the precision requirement essential for any law to be "reasonably justifiable" under section 45 of the Nigerian Constitution.¹⁶ The reconceptualisation of expression in Nigeria must therefore begin with aligning these domestic derogation clauses with the rigorous tripartite test of legality, legitimacy, and necessity found in African regional jurisprudence.

¹¹ *Id.* § 45(1).

¹² African Charter on Human and Peoples' Rights art. 9, June 27, 1981, 1520 U.N.T.S. 217. Unlike the European Convention on Human Rights, the African Charter does not include an explicit list of "necessary" restrictions, which led the African Commission to develop its Declaration of Principles (first adopted in 2002 and revised in 2019) to provide a more robust protective framework.

¹³ AFRICAN COMM'N ON HUMAN AND PEOPLES' RIGHTS, *Declaration of Principles on Freedom of Expression and Access to Information in Africa*, princ. 9(1) (2019).

¹⁴ *SERAP v. Federal Republic of Nigeria*, Judgment No. ECW/CCJ/JUD/40/22 (ECOWAS Ct. Just. July 14, 2022). In that case, the Court emphasised that the internet is a platform for the exercise of the right to freedom of expression and that any restriction on access must be strictly provided by law.

¹⁵ *SERAP*, *supra* note 14.

¹⁶ See *Pansy Tiakula v. Zimbabwe*, Commc'n 409/12 (Afr. Comm'n on Human and Peoples' Rights 2014).

III. THE 2024 LEGISLATIVE PIVOT AND DIGITAL CONTROL

The enactment of the Cybercrimes (Prohibition, Prevention, etc.) (Amendment) Act 2024 was ostensibly a response to years of domestic and international outcry against the draconian nature of the original 2015 legislation.¹⁷ Section 24 of the 2015 Act in particular had become a notorious tool for the criminalisation of annoyance, under which, as Freedom House and civil society monitors have documented, journalists and activists were frequently arrested for online posts that powerful actors deemed insulting or grossly offensive.¹⁸ That broad wording essentially allowed subjective emotional reactions to dictate the boundaries of criminal liability.

The 2024 Amendment sought to refine this by substituting the vague descriptors of annoyance and insult with more specific triggers. Under the amended section 24(1)(b), criminal liability now attaches to messages that the sender knows to be false and sends for the purpose of causing a breakdown of law and order or posing a threat to life.¹⁹ On the surface, this narrowing of scope appears to safeguard legitimate journalistic inquiry and social media commentary. By tethering the offence to a threat to life or a breakdown of law and order, the legislature seemingly moved toward a standard of actual harm rather than perceived offence.

A deeper legal analysis reveals, however, that the pivot may be more cosmetic than substantive. The primary concern lies in the interpretative vacuum surrounding the phrase “breakdown of law and order”. Unlike a threat to life, which has a relatively settled meaning in criminal jurisprudence, a breakdown of law and order remains an elastic term that is easily susceptible to executive manipulation. In the contemporary Nigerian context, the phrase risks becoming a digital-age equivalent of sedition, a charge that critics say has often been used to suppress speech that merely inconveniences the government or exposes institutional failures.²⁰

Furthermore, the amended Act maintains a harsh punitive regime, with fines of up to ₦7 million and imprisonment for up to three years.²¹ That severity, coupled with the continued lack of a clear judicial test for what constitutes a digital incitement to lawlessness, ensures that the

¹⁷ Cybercrimes (Prohibition, Prevention, etc.) (Amendment) Act, 2024 (Nigeria).

¹⁸ Cybercrimes (Prohibition, Prevention, etc.) Act, 2015, § 24(1) (Nigeria); see FREEDOM HOUSE, *Nigeria: Freedom on the Net 2024* (2024) (noting that section 24 has frequently been used to arrest or imprison journalists and activists). This provision was famously challenged in *Incorporated Trustees of Laws and Rights Awareness Initiatives v. Federal Republic of Nigeria*, Judgment No. ECW/CCJ/JUD/16/20 (ECOWAS Ct. Just. July 10, 2020), where the ECOWAS Court found the section inconsistent with article 9(2) of the African Charter and ordered the Nigerian government to repeal or amend it.

¹⁹ Cybercrimes (Prohibition, Prevention, etc.) Act, 2015, § 24(1)(b) (Nigeria), as amended by the Cybercrimes (Prohibition, Prevention, etc.) (Amendment) Act, 2024. The shift from annoyance to “breakdown of law and order” recalls the public-order rationale of the colonial-era sedition provisions in section 50 of the Criminal Code Act. This suggests a cyclical return to State-security-based speech regulation under a digital veneer.

²⁰ See SERAP, “End Use of Cybercrime Act Against Journalists, Release Those in Custody”, SERAP, NGE Tell Tinubu Govt, Others (Press Release, May 4, 2025), <https://serap-nigeria.org/2025/05/04/end-use-of-cybercrime-act-against-journalists-release-those-in-custody-serap-nge-tell-tinubu-govt-others/>.

chilling effect persists.²² Arrests of activists in 2024 and 2025, documented by Freedom House and by civil society groups, suggest that the State continues to use the threat of prosecution under the Cybercrimes Act to enforce a de facto silence, even where the charges are ultimately dropped or fail at trial.²³ Consequently, while the 2024 Act removes the annoyance clause, it preserves a framework in which the State remains the sole arbiter of which digital truths are deemed dangerous to the public peace.

IV. THE 2025 JURISPRUDENTIAL SHIFT: THE FOI BREAKTHROUGH

A critical turning point in the reconceptualisation of digital expression in Nigeria occurred on 11 April 2025, when the Supreme Court delivered its landmark judgment in *Osakue v. Edo State Agency for the Control of AIDS*.²⁴ For over a decade, the implementation of the Freedom of Information (FOI) Act 2011 had been hampered by a jurisdictional schism: several state governments argued that, as federal legislation, the Act did not bind sub-national institutions unless specifically domesticated by state houses of assembly.²⁵ The Supreme Court's 2025 decision decisively dismantled this domestication defence, affirming that the FOI Act is a law of national application that binds all thirty-six states and local governments.

This judgment is significant not merely for its administrative implications but for its constitutional symbolism. By ruling that the National Assembly has the legislative competence to enact laws on public records for the entire Federation, the Court effectively elevated the right to know to a structural component of Nigerian federalism.²⁶ In the context of digital expression, this creates a profound legal contradiction: while the Cybercrimes (Amendment) Act 2024 seeks to restrict the flow of disruptive digital information, the 2025 FOI ruling mandates its disclosure.

The reconceptualisation proposed in this article views the *Osakue* decision as the other side of the coin to section 39. If the Supreme Court now recognises a universal, cross-jurisdictional right to access public information, then the digital platforms used to disseminate that information must be afforded a higher tier of protection. As the Attorney-General of the

²¹ Cybercrimes (Prohibition, Prevention, etc.) Act, 2015, § 24(1) (Nigeria), as amended by the Cybercrimes (Prohibition, Prevention, etc.) (Amendment) Act, 2024.

²² For an empirical analysis of how vague criminal statutes lead to self-censorship in West Africa, see Alaba, *Digital Rights and the Burden of Vague Legislation in Nigeria*, 12 J. AFR. LEGAL STUD. 45 (2025). The author argues that the mere threat of arrest under section 24 serves as a de facto prior restraint on investigative journalism.

²³ FREEDOM HOUSE, *supra* note 18; *see also* SERAP, *supra* note 20.

²⁴ *Osakue v. Edo State Agency for the Control of AIDS*, Appeal No. SC/614/2018 (Nig. Sup. Ct. Apr. 11, 2025) (unreported). The Court held that the Freedom of Information Act 2011 binds state institutions because the National Assembly is competent to legislate on the archives and public records of the Federation, which comprises the States as well as the Federal Government.

²⁵ *See Edo State Agency for the Control of AIDS v. Osakue* (2018) LPELR-44157 (CA); *Edoghayhe v. Edo State Government* (2018) LPELR-44302 (CA).

²⁶ *Osakue*, *supra* note 24 (per Mohammed Lawal Garba, J.S.C.).

Federation observed in December 2025, “access to information is the oxygen of transparency”; without it, the constitutional right to freedom of expression is rendered anaemic.²⁷

This jurisprudential shift also challenges the State’s reliance on public order derogations to justify digital censorship. If a citizen uses a digital platform to share information obtained through an FOI request, even where that information exposes State failure, the 2025 precedent suggests that such expression is the fulfilment of a national transparency mandate rather than a breakdown of law and order under the Cybercrimes Act. Consequently, the Nigerian judiciary has, perhaps inadvertently, provided the tools for a new rights-based interpretation of the digital sphere, one in which the State’s duty to disclose information overrides its impulse to suppress the subsequent digital discourse.

V. RECONCEPTUALISING THE FRAMEWORK

To resolve the tension between digital regulation and constitutional liberty, this article proposes a shift from a containment model of speech to a rights-based digital sovereignty framework.²⁸ Unlike traditional sovereignty, which emphasises the State’s power to control its digital borders and police its citizens, a rights-based approach views the digital sphere as a public forum essential to the exercise of modern citizenship.²⁹ Under this framework, any derogation under section 45 must not only be “reasonably justifiable” but must also pass the strict scrutiny test typically reserved for physical violations of fundamental rights.³⁰

VI. COMPARATIVE ANALYSIS: AFRICAN RESPONSES TO DIGITAL REGULATION

To understand the urgency of reconceptualising expression in Nigeria, it is necessary to examine broader legislative and judicial developments across Africa. In East Africa, particularly in Kenya and Tanzania, recent reforms of digital regulatory frameworks have been criticised as driven largely by security-first rationales that prioritise State control, surveillance, and public order over individual liberties. These approaches reflect an emerging regional trend that legitimises extensive governmental oversight of digital spaces in the name of national security.

²⁷ Lateef Fagbemi, Att’y Gen. of the Fed’n, Address at the International Human Rights Day Conference (Abuja, Dec. 10, 2025); see *Fagbemi Calls FoI “Oxygen of Democracy” as Stakeholders Demand Overhaul of Transparency Systems*, THISDAY (Dec. 11, 2025), <https://www.thisdaylive.com/2025/12/11/fagbemi-calls-foi-oxygen-of-democracy-as-stakeholders-demand-overhaul-of-transparency-systems/>.

²⁸ For a deeper exploration of how African States are redefining sovereignty in the digital age, see G. Fombo, *West African Digital Sovereignty: Control or Connectivity?*, INT’L REV. L. COMPUTERS & TECH. 14 (2026).

²⁹ See Polra Victor Falade & Oluwafemi Osho, *Nigeria’s Digital Sovereignty: Analysis of Cybersecurity Legislation, Policies, and Strategies* (arXiv preprint, Dec. 18, 2025), arXiv:2601.06050v1, <https://arxiv.org/abs/2601.06050>.

³⁰ The strict scrutiny test proposed in this article is adapted from the jurisprudence of the United States Supreme Court in *Reno v. ACLU*, 521 U.S. 844 (1997), where the Court first recognised that the internet deserves the highest level of First Amendment protection.

South Africa, by contrast, has adopted a markedly different trajectory. In *amaBhungane Centre for Investigative Journalism NPC v. Minister of Justice*,³¹ the Constitutional Court articulated a rights-centred model of digital governance by imposing strict judicial limits on State surveillance and affirming the constitutional importance of privacy and journalist-source confidentiality. The decision underscores the principle that digital regulation must be subject to rigorous constitutional scrutiny and cannot be justified solely on security grounds.

The divergent approaches evident in East and Southern Africa reveal competing models of digital governance on the continent: one that privileges State authority and preventive control, and another that foregrounds constitutionalism, accountability, and fundamental rights. For Nigeria, this comparative landscape offers valuable normative guidance. Rather than uncritically adopting security-driven regulatory models, Nigeria can draw lessons from the South African precedent by embedding robust safeguards, judicial oversight, and rights-based limitations within its digital regulatory framework.

A. The Kenyan experience

The Kenyan experience provides a useful comparative illustration of the constitutional concerns that may arise from mandatory device-identification systems. In *Okoiti v. Communications Authority of Kenya*,³² decided on 19 April 2018, the High Court of Kenya considered constitutional objections to the proposed Device Management System (DMS), including concerns relating to privacy and the proposed collection and processing of mobile-device information. The High Court held that the proposed integration of the DMS with mobile network operators' systems, particularly the proposed access to information relating to subscribers, constituted a threat to the subscribers' constitutionally protected right to privacy, and it issued orders restraining the implementation of the system in the form proposed.

The High Court's decision was, however, subsequently overturned by the Court of Appeal in *Communications Authority of Kenya v. Okoiti*,³³ delivered on 24 April 2020. The Court of Appeal allowed the appeal, set aside the orders of the High Court, and directed the Communications Authority to continue consultations with stakeholders and mobile network operators, to complete the technical and consumer guidelines for the DMS, and to subject the relevant guidelines or regulations to public participation. The decision therefore does not support the proposition that Kenyan law presently prohibits mandatory IMEI collection or the

³¹ *amaBhungane Centre for Investigative Journalism NPC v. Minister of Justice* [2021] ZACC 3 (S. Afr.).

³² *Okoiti v. Communications Authority of Kenya*, Petition No. 53 of 2017, [2018] KEHC 7513 (KLR) (H.C. Apr. 19, 2018) (Kenya).

³³ *Communications Authority of Kenya v. Okoiti*, Civil Appeals Nos. 166 & 167 of 2018 (Consolidated), [2020] KECA 754 (KLR) (C.A. Apr. 24, 2020) (Kenya).

establishment of a DMS. Rather, it demonstrates the importance of legality, stakeholder consultation, public participation, and the protection of privacy in the development and implementation of regulatory measures involving mobile-device information.

The Kenyan experience is consequently instructive to Nigeria not because it establishes a settled judicial prohibition against mandatory IMEI collection, but because it demonstrates the constitutional and administrative issues that may arise when regulatory authorities introduce device-identification systems. It underscores the need for any Nigerian regulatory framework involving mandatory device identification, or the collection and processing of device-related information, to satisfy the applicable requirements of legality, constitutional privacy protection, proportionality, meaningful stakeholder engagement, and procedural safeguards. The Kenyan experience thus offers a comparative basis for judicial scrutiny of such measures in Nigeria without treating an overturned foreign decision as the prevailing law of that jurisdiction.

B. Tanzania: regulating the digital gatekeepers

Tanzania has taken a different route by focusing on the “gatekeepers” of information. The Electronic and Postal Communications (Online Content) (Amendment) Regulations 2025 specifically target internet service providers, requiring them to establish and deploy mechanisms to prevent, restrict, and bar access to prohibited content.³⁴

Notably, the 2025 Tanzanian regulations also introduced a new category of prohibited content: “unethical, fabricated and artificial intelligence generated content”.³⁵ This highlights a growing regional anxiety over content generated by artificial intelligence, an area on which Nigeria’s 2024 Act remains largely silent. Tanzania’s approach demonstrates a move toward automated censorship, in which the State delegates its policing power to private service providers, a trend that Nigerian scholars must watch closely as a potential future for West African digital regulation.

C. The South African judicial approach

In South Africa, the Constitutional Court in the landmark case of *amaBhungane* addressed the secrecy of, and lack of safeguards in, State surveillance, ultimately ruling that the confidentiality of journalists’ sources is a core component of the right to freedom of expression.³⁶ More

³⁴ Electronic and Postal Communications (Online Content) (Amendment) Regulations, 2025, G.N. No. 57 of 2025, reg. 6 (Tanz.) (inserting reg. 9A). These regulations represent a significant departure from the 2020 version by extending content-control obligations to internet service providers, a move that has been critiqued for encouraging “private censorship” by technology firms.

³⁵ Electronic and Postal Communications (Online Content) (Amendment) Regulations, 2025, G.N. No. 57 of 2025, reg. 9 (Tanz.) (inserting sch. para. 1(d)).

³⁶ *amaBhungane*, *supra* note 31. This case is considered relevant because it constitutionalised strong limits on State surveillance and firmly protected journalist-source confidentiality in the digital age. In Nigeria, the case is useful

recently, in *Botha v. Smuts* (2024), the Constitutional Court grappled with the paradox of conflicting rights, emphasising that in the digital age the law must remain flexible enough to prioritise expression where the information disclosed is of significant public interest, even if it touches on personal data, while holding that the publication of the applicant's home address went further than the public interest required.³⁷

For Nigeria, the lesson is clear: digital expression cannot be governed by a static interpretation of section 39. As Kollapen J observed in the first judgment, the balance between expression and privacy calls for an analysis akin to a proportionality test, under which even a warranted invasion of privacy must go only as far as is reasonably necessary.³⁸

The comparison reveals a significant divergence in how African States are reconceptualising digital expression. The Kenyan experience illustrates the continuing tension between State regulatory and security objectives and the protection of constitutional rights, particularly the right to privacy, demonstrating the ongoing judicial struggle to balance governmental authority with individual liberties. Tanzania, on the other hand, moves toward platform-level enforcement and the regulation of artificial intelligence, prioritising State oversight and preventive control over individual liberties. In contrast, South Africa has constitutionally imposed strict limits on secret State surveillance, as illustrated by the Constitutional Court in *amaBhungane Centre for Investigative Journalism NPC v. Minister of Justice*,³⁹ which reinforced the protection of privacy and journalist-source confidentiality.

Nigeria, following the 2025 *Osakue* ruling, is uniquely positioned to link digital expression to transparency and federalism, offering a potential rights-based model within a regional context. Situating Nigeria in this African landscape demonstrates that the reconceptualisation proposed in this article is part of a broader continental struggle to define the boundaries of the digital public sphere. In this struggle, Nigeria's approach emphasises the elevation of the right to receive information as a constitutional shield against the vague public order triggers that characterise the cybercrimes statutes of its regional peers. By integrating judicial safeguards, constitutional oversight, and a commitment to fundamental freedoms, Nigeria can navigate between the extremes of security-driven regulation and rights-protective governance.

A reconceptualised framework requires the Nigerian judiciary to adopt a more rigorous definition of the "breakdown of law and order" found in the 2024 Amendment. This article

as persuasive authority in matters involving journalists' rights, investigative reporting, and surveillance under the Cybercrimes Act.

³⁷ *Botha v. Smuts* [2024] ZACC 22 (S. Afr.) (Oct. 9, 2024).

³⁸ *Botha*, *supra* note 37, para. 152 (Kollapen, J.).

³⁹ *amaBhungane*, *supra* note 31.

proposes a clear and imminent harm test, under which the State should be barred from prosecuting digital speech unless it can demonstrate:

1. *Intent*: the speaker specifically intended to incite physical violence.
2. *Imminence*: the speech was likely to result in immediate lawlessness.
3. *Proportionality*: no less restrictive means (such as a public rebuttal or an administrative correction) could have mitigated the perceived threat.

By integrating the 2025 FOI mandate into this test, a transformative conclusion follows: if information is legally obtainable through an FOI request, its subsequent digital dissemination, however annoying it may be to the State, is constitutionally protected as a form of participatory sovereignty.⁴⁰ This reconceptualisation ensures that the Nigerian digital ecosystem remains a space for accountability rather than a theatre for State-monitored compliance.

VII. CONCLUSION AND RECOMMENDATIONS

Reconceptualising freedom of expression in Nigeria requires moving beyond the colonial-era instinct to police the tongue and instead protecting the digital breath of the citizen. By synthesising the 2024 legislative pivot with the 2025 judicial advances, Nigeria has a unique opportunity to lead the continent in rights-based digital governance. If the right to speak is truly to be the lifeblood of Nigerian democracy, the law must stop treating the internet as a danger to be managed and start treating it as a liberty to be cherished.

The reconceptualisation of freedom of expression in Nigeria is not merely a theoretical necessity but a pragmatic imperative for the survival of its digital democracy. As this article has demonstrated, the current containment model typified by the Cybercrimes (Amendment) Act 2024 is increasingly at odds with the transparency mandate established by the 2025 Supreme Court FOI breakthrough. To harmonise Nigeria's digital ecosystem with international human rights standards, this article offers the following recommendations.

A. Legislative refinement of law and order

The National Assembly must move to amend section 24 of the Cybercrimes Act further, to provide an exhaustive, rather than illustrative, definition of "breakdown of law and order". In line with the proposed clear and imminent harm test, criminal liability should attach only to speech that directly and intentionally incites physical violence. Furthermore, the legislature should fast-track the National Digital Economy and E-Governance Bill⁴¹ to ensure that the

⁴⁰ ARTICLE 19 WEST AFRICA, *Nigeria: Free Expression Is Key to Strengthen Sovereignty* (Oct. 1, 2025), <https://www.article19.org/resources/nigeria-free-expression-is-key-to-strengthen-sovereignty/>.

⁴¹ National Digital Economy and E-Governance Bill (Nigeria), currently before the National Assembly.

regulation of emerging technologies, including content driven by artificial intelligence, prioritises human rights and transparency over State surveillance.⁴²

B. Judicial activism and digital literacy

The Nigerian judiciary must move from being a passive arbiter of national security to an active custodian of digital constitutionalism. Building on the momentum of the 2025 All Nigerian Judges Conference, courts should adopt practice directions that recognise digital platforms as protected public forums.⁴³ Judges must be equipped with the technical literacy to distinguish between political annoyance and an actual cyber threat. Otor and others rightly note that many people in Nigeria are oblivious of their legal rights and that, even when informed and aware of such rights, they are reluctant to approach the courts for enforcement because of factors such as poverty, illiteracy, and corruption, which militate against the Nigerian legal system.⁴⁴

C. Integration of regional standards

Nigeria should lead the ECOWAS sub-region by domesticating the Declaration of Principles on Freedom of Expression and Access to Information in Africa. This would involve shifting the burden of proof in digital speech cases: rather than the citizen proving that the speech is safe, the State must prove that any restriction is the least intrusive measure available to achieve a legitimate democratic aim.⁴⁵

⁴² *Nigeria Set to Pass AI Law by End of March 2026*, THE LEGAL WIRE (Jan. 13, 2026), <https://thelegalwire.ai/nigeria-set-to-pass-ai-law-by-end-of-march-2026/>.

⁴³ STATE HOUSE, ABUJA, *President Tinubu to Judges: No Amount of Reform Can Succeed if Integrity Is Compromised* (Press Release, Nov. 17, 2025), <https://statehouse.gov.ng/president-tinubu-to-judges-no-amount-of-reform-can-succeed-if-integrity-is-compromised/>.

⁴⁴ Enoch Ibu Otor, Polycarp Arinze Okoro, King James Nkum & Alphonsus Okoh Alubo, *Appraisal of the Liability of Health Care Practitioners and Facilities for Medical Negligence in Nigeria: A Case Study of Plateau State, Nigeria*, 4 ICRRD QUALITY INDEX RSCH. J. no. 2, at 207–224 (2023), <https://doi.org/10.53272/icrrd.v4i2.8>.

⁴⁵ See *SERAP*, *supra* note 14.