



THE
FUTURE
OF
FREE
SPEECH

THAT VIOLATES MY POLICIES 2026

AI LAWS, CHATBOTS, AND
THE FUTURE OF EXPRESSION

DIRECTED BY:

Jordi Calvet-Bademunt,
Jacob Mchangama,
and Isabelle Anzabi

www.futurefreespeech.org

ACKNOWLEDGMENTS

The Future of Free Speech is an independent, nonpartisan think tank based at Vanderbilt University. Our mission is to reaffirm freedom of expression as the foundation of free and thriving societies through actionable research, practical tools, and principled advocacy. We envision a world in which the right to freedom of expression is safeguarded by law and strengthened by a culture that embraces diverse viewpoints.

This project was led by Jordi Calvet-Bademunt (Senior Research Fellow), Jacob Mchangama (Executive Director), and Isabelle Anzabi (Research Associate) at The Future of Free Speech. Jordi Calvet-Bademunt authored the chapter on the European Union, and Isabelle Anzabi and Ashkhen Kazaryan (Senior Legal Fellow) authored the chapter on the United States.

We are grateful to Ajdin Muratovic (Director of Communications) for overseeing the report's design, and to Wendy H. Burch (Chief Operating Officer) for coordinating all administrative aspects of the project.

We extend our thanks to the leading experts who contributed chapters on their respective jurisdictions: Tomiwa Ilori (Nigeria); Matías González Mama, Lina Palacios, and Francesca Chocano Villanueva (Peru); Emmanuel Vargas Penagos, Katalin Kelemen, and Sandi Rizvic (Sweden); Yaman Akdeniz (Türkiye); Eliza Bechtold (United Kingdom); and Trịnh Hữu Long (Vietnam).

We are further indebted to Justin Hayes for designing the report.

Finally, we are especially grateful to the Rising Tide Foundation and the Swedish Postcode Lottery Foundation for their generous support of this work.



PREFACE

In the 2026 edition of our report *“That Violates My Policies”: AI Laws, Chatbots, and the Future of Expression*, we explore the ways in which public and private governance of generative artificial intelligence (AI) shapes the space for free expression and access to information.

Since the launch of ChatGPT by OpenAI in November 2022, generative AI has moved from a novelty to a tool embedded in everyday communication and information access.¹ As its reach has grown, so has the urgency for legislators around the world to determine how it should be governed, and what that governance means for freedom of expression and access to information.

Recognizing generative AI’s growing impact on freedom of expression and access to information, The Future of Free Speech undertook a first-of-its-kind analysis of how national legislation and corporate practices shape expression in the era of generative AI. The 2025 report analyzed AI legislation in Brazil, China, the European Union, India, the Republic of Korea, and the United States. It focused on laws and public policies addressing AI-generated content, particularly around elections and political speech, hate speech, defamation, explicit content, copyright, and measures that actively promote freedom of expression.²

This year, we built on those findings and expanded them considerably. This report, the first of two publications The Future of Free Speech will release this year, examines AI legislation, bills, policies, and case law in the European Union, Nigeria, Peru, Sweden, Türkiye, the United Kingdom, the United States, and Vietnam. It considers how these frameworks shape

¹ Generative AI refers to systems that create content — including text, images, video, audio, and software code — in response to user prompts. Cole Stryker and Mark Scapicchio, “What Is Generative AI?,” IBM Think, March 22, 2024, <https://www.ibm.com/think/topics/generative-ai>.

² Jordi Calvet-Bademunt, Jacob Mchangama, and Isabelle Anzabi, *“That Violates My Policies”: AI Laws, Chatbots, and The Future of Expression* (Nashville: The Future of Free Speech, October 2025), <https://futurefreespeech.org/wp-content/uploads/2025/10/AI-Report-2025-Full-Report.pdf>.

THAT VIOLATES MY POLICIES 2026

freedom of expression and access to information across election and political content, hate speech, defamation, explicit content, copyright, and measures that empower freedom of expression, such as policies supporting linguistic diversity, media literacy, and open-source development. We have added dedicated sections on protection of minors and AI-powered surveillance to reflect these increasingly salient issues.

This report seeks to provide a rigorous and timely analysis of how generative AI is reshaping the space for free expression in both the public and private spheres. Building on these insights, The Future of Free Speech is developing guidelines to help policymakers ensure that generative AI protects and enhances freedom of expression and access to information, two cornerstones of democratic societies. A second report, focused on model analysis and related good practices for companies, will follow later this year.

In an era of rapid technological change, safeguarding free expression protects both individual rights and the conditions for open, informed, and thriving democracies.



ARTIFICIAL INTELLIGENCE & FREEDOM OF EXPRESSION IN NIGERIA

By
Tomiwa Ilori



TOMIWA ILORI

Tomiwa Ilori (LLM, LLD) is a human rights scholar and practitioner. He is currently a senior technology and human rights researcher at Human Rights Watch. His work has focused on the implications of technologies, including new and emerging technologies, on human rights. His research areas include platform governance, artificial intelligence, data protection, surveillance law, and digital public infrastructure.

Disclaimer: This report is written in the author's personal capacity as an independent expert. The views expressed are solely those of the author and do not represent those of the author's employer or affiliations. Responsibility for the content rests entirely with the author.



ABSTRACT

This chapter examines how the emerging artificial intelligence (AI) governance framework engages with generative AI and the right to freedom of expression in Nigeria. Although constitutional and international law formally guarantee this right, its practical scope is narrowed by overlapping and often broadly framed legal regimes governing cybercrime, elections, criminal law, and surveillance.

Focusing on the intersection of generative AI and freedom of expression, the chapter shows that Nigeria is developing a governance approach that is broad in scope but lacking in substance. Legislative proposals and national policy instruments adopt sweeping regulatory models, yet do not directly address key questions relating to freedom of expression or the governance of AI-generated content. As a result, AI-related risks are largely managed through legal frameworks that were designed neither for large language models nor for automated or synthetic forms of expression.

This indirect approach has two interconnected consequences. First, it allows harmful content—including electoral disinformation, hate speech, and nonconsensual intimate imagery—to scale through the use of generative AI systems. Second, it increases the likelihood of overbroad enforcement under vague legal provisions. Together, these dynamics can suppress lawful expression and encourage self-censorship, particularly in politically sensitive contexts.

Nigeria already has a sufficient normative foundation in constitutional and international human rights law to guide effective regulatory standards on generative AI and freedom of expression. These standards, however, are not yet meaningfully integrated into emerging AI governance efforts in national contexts. Closing this gap therefore requires a more explicit rights-based framework that incorporates principles of legality, necessity, and proportionality, together with clearer transparency and accountability obligations for generative AI systems.

1. INTRODUCTION

Generative artificial intelligence (AI) has rapidly become embedded in everyday communication, reshaping how information is produced, distributed, and consumed.¹ Although these developments might initially appear to create opportunities for development, at their core they raise major questions for human rights protection, particularly freedom of expression.² In legal systems where the protection of freedom of expression is already inadequate, AI poses new risks that are intensified by its scale and impact.³

In Nigeria, freedom of expression is formally guaranteed under constitutional and international human rights law, including the right to seek, receive, and impart information. In practice, however, the right operates within a restrictive regulatory environment. Multiple legal frameworks—ranging from cybercrime and criminal law to electoral and surveillance law—impose broad and vague restrictions on speech. At the same time, Nigeria is actively developing AI policies and legislation, including proposals for dedicated governance institutions and national strategies that reflect AI’s growing importance.

These developments raise a central question: how can freedom of expression be protected in a restrictive regulatory environment in which emerging technologies such as generative AI are evolving rapidly? Current AI regulatory approaches tend to fold broad ethical principles into horizontal AI frameworks without clearly addressing the specific implications of AI on

¹ Petar Radanliev, “Artificial Intelligence: Reflecting on the Past and Looking towards the next Paradigm Shift,” *Journal of Experimental & Theoretical Artificial Intelligence* 37, no. 7 (2025): 1045–62, <https://doi.org/10.1080/0952813X.2024.2323042>.

² Recent research suggests that the risk of generative AI stems not only from regulatory gaps but also from its underlying design as they are unlawful by design due to their reliance on large-scale and non-consensual data extraction that conflicts with international human rights law on privacy, reframing its governance as a question of not just outputs but of data practices and business models that generate systemic risks to human rights including freedom of expression. See Amnesty International, *Violations in the Shell: Exposing the Human Rights Costs of Generative AI* (May 2026), <https://www.amnestyusa.org/wp-content/uploads/2026/05/Violations-in-the-Shell-Exposing-the-Human-Rights-Costs-of-Generative-AI.pdf>; Thomson Reuters Foundation, *Artificial Media, Real Rights: The Impact of Gen AI on Freedom of Expression in Eastern and Southern Africa* (September 2025), <https://www.trust.org/wp-content/uploads/2025/12/GenAI-and-Freedom-of-Expression-SEP-2025-V4-Final-for-publication.pdf>.

³ Council of Europe, *Guidance Note on the Implications of Generative AI for Freedom of Expression*, adopted December 3–5, 2025, <https://www.coe.int/en/web/freedom-expression/-/new-guidance-note-on-generative-ai-implications-for-freedom-of-expression>.

freedom of expression or how those implications should be regulated.

This chapter therefore examines how Nigeria's emerging AI governance framework engages with generative AI and freedom of expression. It analyzes the extent to which existing legal standards and evolving policies shape, constrain, or enable expression. Drawing on constitutional provisions, regional and international human rights standards, legislation, and draft laws, the chapter focuses on the areas where these interactions are most visible: election and political content, hate speech, defamation, the protection of minors, explicit content, copyright, AI-powered surveillance, and data protection.

Although legal and policy discussions on AI and freedom of expression are under way in Nigeria, the current regulatory landscape remains restrictive, fragmented, and poorly adapted to AI systems. This matters because Nigeria is still at a formative stage in shaping its AI governance framework and could still change course. The next section outlines the general standards governing freedom of expression in Nigeria before turning to the country's evolving AI policy and legislative landscape.

2. GENERAL STANDARDS OF FREEDOM OF EXPRESSION

Nigeria’s constitutional and legal framework protects the right to freedom of expression and of the press.⁴ It also subjects the right to specific restrictions, including those prescribed by law that are reasonably justifiable in a democratic society.⁵ The Constitution does not, however, recognize access to information as a standalone right. Access to information is instead protected through the same constitutional guarantee of freedom of expression, which includes the right “to receive and impart ideas and information without interference.” Access to information in Nigeria is governed in detail by the Freedom of Information Act, 2011.⁶

The Nigerian Constitution broadly mirrors the guarantee of freedom of expression in the International Covenant on Civil and Political Rights (ICCPR).⁷ Under the ICCPR, the right to freedom of expression—including the freedom to seek, receive, and impart information—is commonly interpreted to include a right of access to information held by public bodies, and the Nigerian Constitution is read the same way.⁸ This interpretation reflects a traditional understanding of access to information as concerned with accessing publicly held records and, in some specific instances, with information held by private bodies. Over time, the right has expanded to include access to information on the internet and through digital communication systems.⁹

The African Charter on Human and Peoples’ Rights (African Charter) is the primary regional

4 Constitution of the Federal Republic of Nigeria (1999, as amended), sec. 39 <https://www.placng.org/i/wp-content/uploads/2020/05/Constitution-of-the-Federal-Republic-of-Nigeria.pdf>.

5 Nigeria’s constitutional protection of freedom of expression is subject to both direct textual limitation and general derogation clause. The proviso under section 39(3) of the Constitution operates as a direct, speech-specific restriction, as it explicitly qualifies the exercise of the right. By contrast, section 45 functions as a general restriction and derogation clause that applies across multiple rights, including freedom of expression only indirectly, unlike the more explicit and speech-specific limitation in section 39(3).

6 Freedom of Information Act (Nigeria), 2011, <https://placng.org/i/wpcontent/uploads/2019/12/FreedomOfInformationAct2011.pdf>.

7 Nigerian Const. secs. 39 and 45; ICCPR, art. 19.

8 ICCPR, art. 19(2).

9 African Commission on Human and Peoples’ Rights, *Declaration of Principles on Freedom of Expression and Access to Information in Africa*, 2019, Principle 37(1), <https://achpr.au.int/sites/default/files/files/2022-08/declarationofprinciplesonfreedomofexpressioneng2019.pdf>.

human rights instrument. It binds its State Parties, including Nigeria, which has ratified the Charter incorporated it into national law.¹⁰ The African Charter is distinctive in expressly guaranteeing both freedom of expression and access to information as standalone rights.¹¹ It provides that “every individual shall have the right to receive information” and in the subsection that follows, that “every individual shall have the right to express and disseminate his opinions within the law.”¹² The phrase “within the law” is a clawback clause that the African Commission on Human and Peoples’ Rights (African Commission)—the African Union body charged with implementing the African Charter—has interpreted to mean within international law, not national law. This interpretation prevents states from relying on broad and vague national laws to justify restrictions on expression.¹³

Adopted by the African Commission under Article 9 of the African Charter, the Declaration of Principles on Freedom of Expression and Access to Information in Africa, 2019 (Declaration of Principles) is a soft-law instrument that provides an authoritative interpretation of regional standards in light of recent developments affecting freedom of expression and access to information.¹⁴ It sets out principles and state obligations on how these rights should be respected, protected, and fulfilled in the region, including in digital and technology-mediated environments.¹⁵ Notably, the Declaration requires State Parties to ensure that the development, deployment, and use of AI and algorithmic technologies comply with international human rights law, particularly the rights to freedom of expression and access to information.¹⁶

Similarly, the Guidelines on Access to Information and Elections in Africa, 2017, adopted

¹⁰ African Commission on Human and Peoples’ Rights, “State Parties to the African Charter,” <https://achpr.au.int/en/states>; *African Charter on Human and Peoples’ Rights (Ratification and Enforcement) Act*, 1983 (Nigeria), sec. 1 <https://www.placng.org/laws/nigeria/print.php?sn=24>.

¹¹ Rachel Murray, *The African Charter on Human and Peoples’ Rights: A Commentary* (Oxford: Oxford University Press, 2019), 266–93 (art. 9), <https://academic.oup.com/oxford-law-pro/book/57134/chapter-abstract/473338359?redirectedFrom=fulltext>.

¹² Article 9(1) and (2) of the African Charter on Human and Peoples’ Rights.

¹³ *Media Rights Agenda and Others v Nigeria*, Communications 105/93, 128/94, 130/94 and 152/96 (African Commission on Human and Peoples’ Rights, 1998), para. 64–71; Elena Abrusci and Juliana da Cunha Mota, “Borrowing, Rephrasing, or Inventing? How the African Commission and Court on Human and Peoples’ Rights Have Filled the Gap on Legitimate Restrictions to Freedom of Expression,” *Human Rights Law Review* 26, no. 1 (2026): 6–11. Principle 4 of the Declaration of Principles further rests this debate as it significantly reshapes the operation of claw-back clauses by requiring that, where national and international standards diverge, the most rights-protective standard prevails.

¹⁴ African Commission, *Declaration of Principles*, Introduction and Preamble.

¹⁵ Tomiwa Ilori, “Protecting Digital Rights through Soft Law: Ensuring the Implementation of the Revised Declaration of Principles on Freedom of Expression and Access to Information in Africa,” *African Human Rights Law Journal* 24 (2024): 10, <http://dx.doi.org/10.17159/1996-2096/2024/v24n1a1>.

¹⁶ African Commission, *Declaration of Principles*, Principle 39.

by the African Commission, translate the right of access to information into concrete obligations for State Parties across the electoral cycle.¹⁷ In particular, the Guidelines assign obligations to key electoral actors—election management bodies, media and online platform providers, and media regulators to ensure proactively that the right is protected throughout the electoral process.¹⁸ Although adopted before the widespread deployment of generative AI, the Guidelines offer a relevant normative framework for assessing how AI systems may affect voters’ access to information and electoral integrity in the region.

The African Charter on Democracy, Elections and Governance, 2007 (ACDEG) is a binding African Union treaty that imposes enforceable obligations on State Parties, including Nigeria, concerning democratic governance and electoral integrity.¹⁹ Within that framework, the ACDEG reinforces the rights to freedom of expression and access to information. Its provisions on access to information, on the development and use of information and communication technologies, and on the promotion of freedom of expression are especially relevant to generative AI.²⁰

The African Union’s Continental Artificial Intelligence Strategy adds a regional policy framework intended to guide the development and governance of AI in Africa in a manner consistent with human rights and democratic values.²¹ Although not legally binding, the Strategy recognizes the need to adopt and implement ethical principles for AI “within the framework of regional and international human rights law.”²² In particular, it identifies AI-enabled election manipulation, the dissemination of disinformation, and unlawful AI-facilitated surveillance as human rights risks.²³ It names human rights, including those enshrined in the African Charter, together with transparency and inclusive access to information through linguistic diversity, as key principles for AI governance.²⁴ The Strategy also stresses safeguarding information integrity and public trust in AI through responsible

17 African Commission on Human and Peoples’ Rights, “Guidelines on Access to Information and Elections in Africa” (2017), <https://www.africafoicentre.org/wpdmpro/guidelines-on-access-to-information-and-elections-in-africa/>.

18 African Commission, “Guidelines on Access to Information and Elections,” Preface and Preamble.

19 African Union, “African Charter on Democracy, Elections and Governance” (2007), <https://au.int/en/treaties/african-charter-democracy-elections-and-governance>.

20 African Union, “African Charter on Democracy, Elections and Governance,” arts. 2(10), 27(7)-(8).

21 African Union, “Continental Artificial Intelligence Strategy: Harnessing AI for Africa’s Development and Prosperity” (July 2024), 27–28, https://au.int/sites/default/files/documents/44004-doc-EN-_Continental_AI_Strategy_July_2024.pdf.

22 African Union, “Continental Artificial Intelligence Strategy,” 4.

23 African Union, “Continental Artificial Intelligence Strategy,” 26.

24 Ibid.

use and strengthened media and information literacy, and it highlights generative AI risks such as misinformation, disinformation, and hate speech that undermine social cohesion and democratic processes. It calls on states to combine literacy initiatives, regulatory measures, and coordinated strategies so that people can engage critically with AI-mediated information ecosystems.²⁵

These principles are reflected in domestic human rights guidance as well, in an advisory issued by the National Human Rights Commission.²⁶ Consistent with its statutory mandate, the Commission emphasized that restrictions on freedom of expression must be lawful, necessary, and proportionate, and must not be used to suppress legitimate opinion or public discourse. In particular, the advisory identifies obligations of specific actors, including law enforcement agencies and the judiciary, to protect freedom of expression, including when applying certain provisions of Nigeria's cybercrimes law.

Nigeria's framework for freedom of expression and access to information thus rests on constitutional provisions, access to information legislation, and binding and soft international and regional human rights law. Although the Constitution does not recognize access to information as a standalone right, Nigeria's legal regime read in light of Article 19 of the ICCPR and Article 9 of the African Charter, treats access to information as an important component of freedom of expression. Regional standards, such as the Declaration of Principles, elaborate these standards and clarify state obligations, including Nigeria's, in contexts that bear on generative AI, such as platform governance, elections, and political speech. Together, these frameworks provide the normative basis for assessing how the development, deployment, and regulation of generative AI in Nigeria affect freedom of expression and access to information.

²⁵ African Union, "Continental Artificial Intelligence Strategy," 49-51.

²⁶ National Human Rights Commission, "Advisory on the Right to Freedom of Expression in Nigeria," April 4, 2025, <https://www.nhrc.gov.ng/files/NHRC%20Advisory%20on%20Right%20to%20Freedom%20of%20Expression%20in%20Nigeria.pdf>.

3. AI LEGISLATION LANDSCAPE

Nigeria's AI governance landscape can be divided into two parts. The first consists of ongoing legislative efforts to adopt binding laws, including draft bills that would assign responsibilities to key actors and establish AI governance institutions. The second consists of nonbinding policy instruments that offer broad national guidance on AI development and governance. Together, the two reflect a largely horizontal approach to AI governance; neither yet establishes an AI-specific framework that addresses human rights protection in general or generative AI and freedom of expression in particular.

3.1 Ongoing Legislative Efforts

Like other African countries, Nigeria is introducing legislation on AI. Recent efforts indicate a two-track approach within the National Assembly. The House of Representatives, the lower house, is pursuing an AI-specific institutional framework through a consolidated bill that would establish a dedicated regulator for AI and robotics.²⁷ The Senate, the upper house, is moving toward a broader bill on the digital economy and e-governance. It would establish a regulatory standard for the entire economy, governing electronic transactions and the use emerging technologies—including AI—in public administration.²⁸ Both initiatives point toward horizontal, rather than targeted, regulation of generative AI, or of its effects on freedom of expression.

The House bill, titled “A Bill for an Act to Provide for Establishment of the National Institute for Artificial Intelligence and Robotic Studies Sciences Regulation Commission (HBs. 143, 601, 942, and 1810),” which consolidates several House bills into a single draft law on AI regulation, signals an effort to streamline the statutory landscape and create a

27 The National Assembly has yet to publish a full official version of the Bill. However, its Order Paper which lists the House's activities for December 3, 2024, identified the Bill for second reading: <https://nass.gov.ng/documents/download/11167>. Other sources also corroborate the existence and content of the Bill: Parliament Reports, “AI Bill and Probe of CBN Mass Retirements | House Gist Today,” Parliament Reports (blog), <https://parliamentreports.com/cbn-mass-retirement-bill-on-ai-house-gist-today/>; <https://regulations.ai/regulations/RAI-NG-NA-ENIAIXX-2024>.

28 National Assembly, “National Digital Economy and EGovernance Bill, 2025,” <https://nass.gov.ng/documents/billdownload/11219.pdf>.

single regulatory framework on AI in Nigeria.²⁹ Substantively, the bill is organized around institutional control and is therefore likely to operate horizontally, covering providers, deployers, and importers of AI systems across sectors. It has been referred to the House Committee on Information and Technology, the stage at which expert testimony is invited, each clause scrutinized, and amendments are proposed.³⁰ The primary freedom of expression concern is that the bill's broad and discretionary approval mechanisms could institutionalize informational chokepoints within the digital communication ecosystem. Narrowing the scope specifically to generative AI would transform the House bill into a statutory framework for governing speech infrastructure.

The National Digital Economy and E-Governance Bill (2025), jointly drafted by the Senate and House Committees on ICT and Cybersecurity, would establish a comprehensive framework for legally recognized digital transactions and public service delivery. Its provisions govern electronic records, digital signatures, electronic contracts, and the delivery of government services through digital platforms. The draft also addresses critical mechanisms of generative AI governance; for example, it contains provisions for the “use of automated systems for contract formation” and introduces an “intermediary liability” framework in the electronic contracts chapter.³¹ Although these provisions are not framed as AI rules, the allocation of liability for machine-mediated communications and transactions directly impacts how AI systems generate content, automate customer interactions, and broker decisions. The bill's policy rationale, as demonstrated through the National Assembly's committee engagement and stakeholder consultations, explicitly adopts a risk-based regulatory framework for emerging technologies, such as AI.³²

Neither the House nor Senate approach provides a fully articulated, speech-specific liability regime for generative systems that produce hate speech, electoral disinformation, or nonconsensual intimate imagery. The regulatory direction instead points to indirect control: ex ante compliance obligations—registration, standards, and audits—on providers and deployers, and intermediary-liability rules that may be applied to platform functions and

29 The Guardian, “Reps Step Down Bill on Artificial Intelligence Regulation,” December 3, 2024, <https://guardian.ng/news/nigeria/national/rep-step-down-bill-on-artificial-intelligence-regulation/>.

30 Ibid.

31 National Digital Economy and E-Governance Bill, 2025, secs. 9, 10, 12.

32 Federal Ministry of Communications, Innovation and Digital Economy (Nigeria), “Public Hearing on National Digital Economy and E-Governance Bill 2025 Holds in Abuja,” May 25, 2026, <https://fmcide.gov.ng/public-hearing-on-national-digital-economy-and-e-governance-bill-2025-holds-in-abuja/>.

automated systems. This approach can manage systemic risk effectively, but it also invites over-removal and chilling effects when intermediaries face uncertain or strict liability for user-facing AI outputs.

The House bill would create a single body to set technical standards and oversee AI across sectors. Such a structure could help address risks that do not fit neatly into existing categories, such as opaque AI systems, large-scale manipulation, biased automated decisions, and the use of AI to scale scams or propaganda. The jointly drafted digital economy bill, by contrast, normalizes automated systems in commerce and public administration and strengthens the legal infrastructure for digital government. These developments can improve access to information and service delivery, but they can also enable AI-driven surveillance and automated exclusion if not paired with strong human rights safeguards.³³ Both bills would benefit from clearer integration of human rights standards through concrete safeguards: mandatory impact assessments for high-risk systems, including recommender systems and generative tools used at scale; transparency for users when they interact with synthetic content or automated decision-making; and enforceable limits and independent oversight for AI used in surveillance or security contexts. Such safeguards mitigate systemic risks without imposing broad, preemptive controls on the technologies that enable expression.

In short, Nigeria still lacks a statute addressing AI and its implications for freedom of expression. Current legislative efforts point instead toward a horizontal, institution-led approach embedded within broader digital economy and e-governance frameworks. That key drafts are not publicly available also underscores persistent transparency gaps in AI policymaking itself.

3.2 AI-Specific Policies

Nigeria's National Artificial Intelligence Strategy (NAIS) is a policy instrument rather than a binding regulatory framework. It was published in September 2025 under the leadership of the Federal Ministry of Communications, Innovation and Digital Economy (FMCIDE), the National Information Technology Development Agency (NITDA), and the National Centre for

³³ According to Nigeria's Minister of Communications, the ChatBot provides easy access to information for more than 35 ministries and 60 government agencies. See GovGuide Nigeria, "GovGuideNigeria," <https://govguide.ng/>; The Guardian, "FG, Firm Launch GovGuideNigeria AI Platform to Boost Governance," May 22, 2026, <https://guardian.ng/news/fg-firm-launch-govguidenigeria-ai-platform-to-boost-governance/>.

Artificial Intelligence and Robotics (NCAIR).³⁴ Its primary function is to articulate a national vision, guiding principles, and an implementation roadmap for AI adoption.³⁵ Even so, the NAIS will shape the horizontal logic of future AI regulation, including how generative AI, content practices, and systemic risks are likely to be governed in Nigeria.

The NAIS is explicitly horizontal: it does not focus on any particular type of AI or target specific domains such as media or elections. Rather, it frames AI—including large language models and other generative systems—as a general-purpose technology capable of transforming all sectors simultaneously.³⁶ This framing reflects the developmentalist approach through which many African governments view AI, prioritizing its potential for socioeconomic transformation while treating its impacts on ethics, accountability, risk management, and human rights as secondary concerns.³⁷

The NAIS situates generative AI within a broader ecosystem of infrastructure, data, skills, and standards, while acknowledging emerging risks such as misleading outputs, bias, system fragility, and vulnerability to manipulation.³⁸ This framing underscores the Strategy's focus on systemic capacity building and risk awareness and positions it as a foundational document for horizontal AI governance rather than a quasi-regulatory framework with prescriptive rules.

The NAIS also contains no liability provisions for AI-generated content. It neither defines responsibility for harmful generative outputs nor allocates liability among developers, deployers, platforms, and end users. Liability is addressed only implicitly, through commitments to ethical AI design, accountability, and transparency, and through alignment with existing legal frameworks, particularly data protection and sector-specific law.

As a result, the NAIS leaves critical questions, such as liability for AI-amplified disinformation and hate speech, to future legislation and to existing regimes of defamation, electoral, cybersecurity, and data protection law. From a freedom of expression perspective,

34 Federal Ministry of Communications, Innovation and Digital Economy, “National Artificial Intelligence Strategy,” (September 2025), <https://ncair.nitda.gov.ng/wp-content/uploads/2025/09/National-Artificial-Intelligence-Strategy-19092025.pdf>.

35 FMCIDE, “National Artificial Intelligence Strategy,” 11.

36 FMCIDE, “National Artificial Intelligence Strategy,” 15.

37 Kinfe Yilma and Kebene Wodajo, “Strategy as Governance: The Governance of AI in Africa,” *Science and Public Policy* 53 (2026): 236, <https://doi.org/10.1093/scipol/scag011>.

38 FMCIDE, “National Artificial Intelligence Strategy,” 48.

this omission has two consequences: the Strategy avoids laying down rules on harmful content, but it also fails to articulate expression-specific safeguards such as lawfulness, necessity, and proportionality. A possible explanation for this omission is that the NAIS operates as a high-level, horizontal policy blueprint mandated to set the AI governance agenda rather than to prescribe detailed regulation.

The NAIS emphasizes risk-based governance and identifies key factors and outcomes that could address it, but it stops short of defining binding thresholds, enforcement mechanisms, or remedies for generative AI.³⁹

The NAIS repeatedly invokes ethics, inclusion, and social impact.⁴⁰ It does not, however, translate human rights and freedom of expression safeguards, into requirements for AI design or deployment. Speech-related risks such as misinformation, manipulation, and cultural exclusion are framed as governance and trust challenges rather than as questions of human rights protection.⁴¹ Although the NAIS recognizes AI risks to information integrity and the need to promote local language models and inclusive datasets, it leaves unresolved how generative AI should be governed where it intersects with political speech, journalism, satire, or dissent, deferring these issues to implementation phases and future regulation.

39 FMCIDE, “National Artificial Intelligence Strategy,” 54.

40 FMCIDE, “National Artificial Intelligence Strategy,” 27, 44, 57.

41 FMCIDE, “National Artificial Intelligence Strategy,” 50.

4. ELECTION AND POLITICAL CONTENT

The regulation of election and political content in Nigeria is fragmented across electoral, cybercrimes, and criminal law. Electoral law restricts certain forms of campaign speech, including abusive or inflammatory language and coercive political messaging, while political disinformation is addressed through broader cybercrimes and criminal provisions that are often vague and prone to overreach. Although political satire, parody, and artistic expression remain constitutionally protected, they may be mischaracterized as false or harmful content, especially when amplified or generated by AI systems. Nigeria also lacks clear rules on AI-generated content and synthetic media in elections. This gap leaves authorities to rely on general offenses provisions that are ill suited to distinguishing harmful electoral manipulation from protected political expression.

4.1 Election Content

The Electoral Act, 2026, is the primary statute governing elections in Nigeria. The Independent National Electoral Commission (INEC) is responsible for its implementation.⁴² Although the Act does not directly regulate online content, several of its provisions affect political speech during elections. The most directly relevant provision prohibits certain conduct during political campaigns.⁴³ It requires campaigns to avoid undermining social cohesion or public order, and it prohibits the use of abusive language in campaign messages or slogans that directly or indirectly insult or injure religious, ethnic, tribal, or sectional groups.⁴⁴

The Act further bars abusive, intemperate, slanderous, or base language, including insinuations and innuendo, where such language is intended or likely to provoke violent reactions or intense hostility.⁴⁵ It also restricts the venues that may be used for political

⁴² *Electoral Act, 2026*, <https://placng.org/i/wp-content/uploads/2026/03/ElectoralAct2026.pdf>.

⁴³ *Electoral Act, 2026*, sec. 96.

⁴⁴ *Electoral Act, 2026*, sec. 96(1).

⁴⁵ *Electoral Act, 2026*, sec. 96(2).

activity: places of worship, police stations, and public offices may not be used for political campaigns, rallies, or processions, or for promoting or attacking political parties, candidates, or their programs.⁴⁶

The Act also prohibits the use of threats of force or violence, whether direct or indirect, to coerce individuals into supporting or not supporting a political party or candidate during a campaign.⁴⁷

4.2 Political Disinformation

Nigeria has no single statute that comprehensively regulates political disinformation; its regulation is spread across criminal and cybercrimes law. The Criminal Code, which applies in most southern states, and the Penal Code, which applies in most northern states, address it indirectly through public order and disorderly conduct provisions. The Criminal Code criminalizes the publication of false statements or rumors likely to cause fear or disturb the public peace,⁴⁸ and it addresses offensive or disorderly publications that may include misleading or harmful content.⁴⁹ The Penal Code similarly prohibits acts or statements that may incite public disorder or undermine authority, which can extend to the use of false or deceptive information.⁵⁰

Under the Cybercrimes Act, it is an offense to knowingly send false messages through computer systems that cause “annoyance,” “hatred,” or “ill will.”⁵¹ During election periods, this provision has been invoked against individuals for online political posts, allegations against public officials, and controversial commentary shared on social media and messaging platforms.⁵²

Election-related disinformation can cause real harm, including voter suppression and the delegitimization of election results, but the provision’s broad language does not clearly

46 *Electoral Act, 2026*, sec. 96(3).

47 *Electoral Act, 2026*, sec. 97(1).

48 *Criminal Code Act*, sec. 59.

49 *Criminal Code Act*, sec. 249(d).

50 *Penal Code Act*, secs. 114 and 115.

51 *Cybercrimes (Prohibition, Prevention, etc.) Act 2015 (as amended)*, sec. 24, [https://www.dropbox.com/scl/fi/tiwbmbt70syr380ppludg/cybercrime-act-2024-full version.pdf.pdf?rlkey=mu4oom2o4ah4qnkyjw4kkoto7&dl=0](https://www.dropbox.com/scl/fi/tiwbmbt70syr380ppludg/cybercrime-act-2024-full%20version.pdf.pdf?rlkey=mu4oom2o4ah4qnkyjw4kkoto7&dl=0).

52 Ifeoma E. Nwafor, “Cyberstalking in Nigeria: An Exploratory Study of Section 24 of the Nigerian Cybercrimes (Prohibition, Prevention, etc.) (Amendment) Act, 2024,” *International Cybersecurity Law Review* (2024), <https://doi.org/10.1365/s43439-024-00126-0>.

distinguish between intentional disinformation from opinion, error, or satire. This creates a chilling effect, particularly when citizens fear arrest for sharing or criticizing political information.⁵³ Journalists, bloggers, and ordinary citizens have repeatedly been harassed under these provisions.⁵⁴ A clear pattern is their use by powerful public figures against ordinary citizens, reflecting broader power asymmetries in the enforcement of cybercrime law in Nigeria.⁵⁵ Notably, the Economic Community of West African States (ECOWAS) Court of Justice has held these provisions incompatible with freedom of expression and ordered Nigeria to amend them, but the government has yet to comply.⁵⁶

4.3 Satire, Parody and Arts

Political satire, parody, cartoons, songs, and dramatic skits are central to Nigeria's political culture. Although no statute explicitly protects satire, such expression falls squarely within the Constitution's guarantee when it communicates ideas, opinions, or criticism.⁵⁷ Satirical and artistic expression does not purport to make factual claims and should therefore be distinguished from disinformation. In practice, however, enforcement actors and automated moderation systems may misread satire as false or harmful content because they lack local context, especially when satire uses realistic or AI-generated visuals.⁵⁸ Clear recognition of satire as protected political expression is therefore essential in any AI governance framework affecting elections.

Nigeria's legal framework thus regulates election-related content indirectly. Political expression is formally protected under the Constitution but restricted in practice through electoral offenses, criminal law, and cybercrime provisions. The rise of AI-generated political content magnifies longstanding tensions between electoral integrity and freedom of

⁵³ Ibid.

⁵⁴ Media Foundation for West Africa, "ECOWAS Court orders Nigeria to align its Cybercrime Law with its international obligations," March 28, 2022, <https://mfwa.org/ecowas-court-orders-nigeria-to-align-its-cybercrime-law-with-its-international-obligations/>.

⁵⁵ Premium Times, "SERAP, Editors Decry Widespread Use of Cybercrime Act to Harass Journalists, Activists," December 11, 2025, <https://www.premiumtimesng.com/news/top-news/842174-serap-editors-decry-widespread-use-of-cybercrime-act-to-harass-journalists-activists.html>.

⁵⁶ The Incorporated Trustees of Laws and Rights Awareness Initiatives v Federal Republic of Nigeria (ECW/CCJ/JUD/16/20 ECOWAS Court of Justice, 10 July 2020) para. 186 <https://caselaw.ihrda.org/entity/s8gzucy29q?file=1603296563496p5wdd2fhglp.pdf&page=42>.

⁵⁷ Nigerian Const. sec. 39(1).

⁵⁸ Centre for Journalism Innovation and Development (CJID), *AI and Disinformation: A Discursive Analysis of West African Elections* (2025), <https://thecjid.org/wp-content/uploads/2025/10/AI-and-Disinformation-A-Discursive-Analysis-of-West-African-Elections.pdf>; Soorya Balendra, "Meta's AI Moderation and Free Speech: Ongoing Challenges in the Global South," *Cambridge Forum on AI: Law and Governance* (2025), <https://doi.org/10.1017/cfl.2025.5>.

expression, in a setting where neither the state nor technology companies has drawn a clear line between lawful and unlawful expression in electoral contexts.

4.4 Deepfakes and Synthetic Media

Nigeria currently lacks provisions that explicitly address AI-generated or synthetic political content, including deepfake videos, manipulated audio, and AI-generated campaign messaging. Existing legal tools—the Electoral Act, the Cybercrimes Act, and criminal defamation under the Criminal and Penal Codes—are instead applied by analogy. This gap creates uncertainty in two respects. Authorities may rely on broad criminal provisions to respond to such media, risking the conflation of harmful electoral manipulation with lawful political speech. At the same time, there is no clear statutory basis for imposing transparency obligations such as labeling AI-generated political content.

5. HATE SPEECH

Nigeria has neither a single hate speech statute nor a framework tailored to AI-generated hate speech. Laws and enforcement instead draw on constitutional limits, electoral law, broadcasting rules, and cybercrime provisions that address incitement as well as abusive and offensive communications. This patchwork leaves AI-generated hate speech free to proliferate rapidly and at low cost while also producing uneven enforcement. Vague and overbroad provisions create both regulatory gaps and restrictions inconsistent with international human rights standards.

Cybercrime speech offenses in Nigeria have been applied to offensive or annoying communications, particularly under section 24 of the Cybercrimes Act, whose vague terms such as “ill will” and “hatred” give enforcement actors broad discretion. The ECOWAS Court of Justice’s finding that this provision is incompatible with freedom of expression underscores how such overbroad provisions can function as grounds for suppressing lawful speech, which may now include AI-generated content.⁵⁹ By contrast, the same Act narrowly criminalizes racist or xenophobic material and threats or incitement linked to protected characteristics, requires intent, and grounds the offenses in harms such as discrimination or violence.⁶⁰ These provisions highlight the core problem in Nigeria’s online hate speech framework: the use of vague, affect-based offenses that invite overbroad enforcement. AI-generated hate speech, which can be produced in large volumes, amplifies the problem by increasing both enforcement pressure and the likelihood of wrongful attribution.

In broadcasting, the National Broadcasting Commission (NBC) regulates hate speech and fake news under the content rules of the Nigeria Broadcasting Code. Breaches can lead to administrative sanctions such as fines.⁶¹ The ECOWAS Court of Justice, however, has held that these provisions are vague and therefore incompatible with Nigeria’s obligations to

⁵⁹ The Incorporated Trustees of Laws and Rights Awareness Initiatives v Federal Republic of Nigeria (ECW/CCJ/JUD/16/20) para. 185(b).

⁶⁰ *Cybercrimes Act*, sec. 26.

⁶¹ *Nigeria Broadcasting Code*, 6th ed., amended, National Broadcasting Commission (2026), <https://www.nbc.gov.ng/wp-content/uploads/2026/02/NBC-Brochure-6TH-EDITION-AMENDED-addendum.pdf>.

protect freedom of expression.⁶²

Generative AI complicates hate speech regulation in Nigeria in three ways:

- **Intent:** Incitement standards often hinge on purpose or the likelihood of harm, but generative AI blurs the evidentiary trail across prompts, outputs, and the people who share them;⁶³
- **Attribution:** Existing legal provisions often assume a human speaker, yet hate speech outputs may be produced and surfaced by chatbots or recommender systems, which complicate the liability chain;⁶⁴ and
- **Scale:** Generative AI enables low-cost, targeted ethnic or religious attacks, including synthetic audio and manipulated images that spread and quickly heighten offline tensions.⁶⁵

Where hate speech is undefined or vaguely defined, the prohibition can also be turned against lawful dissent, journalism, and unpopular speech.⁶⁶ Nigeria's stringent hate speech provisions, together with the ECOWAS Court's critique of vague cybercrime speech offenses, show how broad terms undermine legal certainty and encourage self-censorship. In the AI context, this uncertainty is compounded by inaccurate, hallucination-prone, and decontextualized automated moderation and detection tools that increase the likelihood that lawful speech will be removed.⁶⁷

International human rights law requires Nigeria to prohibit only a narrow category of expression when regulating hate speech: advocacy of national, racial, or religious hatred that constitutes incitement to discrimination, hostility, or violence, as set out in the

62 The Incorporated Trustees of Expression Now Human Rights Initiative v Federal Republic of Nigeria (ECOWAS Court of Justice) <https://globalfreedomofexpression.columbia.edu/cases/the-incorporated-trustees-of-expression-now-human-rights-initiative-v-federal-republic-of-nigeria/>.

63 Xinyu Wang, Sai Koneru, Pranav Narayanan Venkit, Brett Frischmann, and Sarah Rajtmajer, "The Unappreciated Role of Intent in Algorithmic Moderation of Social Media Content," arXiv (2024), <https://arxiv.org/pdf/2405.11030>.

64 Ibid.

65 Ibid.

66 UN General Assembly, *Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression*, A/74/486 (9 October 2019), para. 1, https://www.ohchr.org/sites/default/files/Documents/Issues/Opinion/A_74_486.pdf.

67 Center for Democracy & Technology, *Mixed Messages: The Limits of Automated Social Media Content Analysis* (Washington, DC: Center for Democracy & Technology, November 2017), <https://cdt.org/wp-content/uploads/2017/11/Mixed-Messages-Paper.pdf>.

ICCPR.⁶⁸ Such regulation must be implemented through clear laws and through necessary and proportionate sanctions consistent with Article 19. The African Commission's 2019 Declaration of Principles similarly requires that prohibited speech be criminalized only as a last resort and only in the most severe cases. The Declaration also directs its attention to factors such as the prevailing social and political context and the status of the speaker in relation to the audience. States may not prohibit speech merely because it lacks civility or because it offends or disturbs.⁶⁹

For generative AI and freedom of expression, these standards imply regulation built on clear and context-sensitive definitions of hate speech, due-process protections for removals and sanctions, and differentiated responsibilities across the value chain, supported by transparency measures that reduce incentives for blanket takedowns.⁷⁰

Given how broadly Nigeria regulates hate speech, any AI-related hate speech law, and its enforcement, should be narrow in scope and consistent with international human rights standards. Practical priorities for generative AI and hate speech include aligning domestic standards with the ICCPR and the relevant provisions of the African Charter and the Declaration of Principles; favoring transparency and the labeling of AI-generated content in high-risk political contexts over blanket regulation; and ensuring that regulators act within clear statutory limits.⁷¹

68 ICCPR, art. 20(2).

69 African Commission, *Declaration of Principles*, Principle 23.

70 UN Human Rights Council, *Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression*, A/HRC/38/35 (6 April 2018), para. 66, <https://docs.un.org/en/A/HRC/38/35>.

71 ICCPR, arts 19 and 20(2).

6. DEFAMATION

Nigeria has defamation laws, including criminal libel and slander, but none that directly addresses AI-generated content. Defamation in Nigeria traditionally takes one of two forms: libel, which is defamatory matter in permanent form, including print and broadcast; and slander, which covers transient, typically spoken statements.⁷² These offenses sit alongside the online speech offenses in the Cybercrimes Act that the ECOWAS Court found incompatible with freedom of expression because of their vagueness.

Applied to generative AI, this could mean that the person or entity responsible for disseminating an AI-generated allegation, including a deployer of the chatbot where appropriate, would ordinarily bear primary liability as the publisher, even if the AI tool produced the text or voice. The AI system is best understood as a tool that can be used to produce libelous or slanderous content, including synthetic audio, which leaves victims to pursue remedies against the identifiable person or entity that released the content to the public.

International human rights standards disfavor criminalizing defamation. The Human Rights Committee has warned that criminal defamation laws must not stifle expression and that imprisonment is never an appropriate penalty. The Declaration of Principles likewise states that “the imposition of custodial sentences for the offenses of defamation and libel are a violation of the right to freedom of expression” and requires public figures to tolerate a greater degree of criticism.⁷³ The African Court on Human and Peoples’ Rights has also held that custodial sentences for defamation violate freedom of expression.⁷⁴ These authorities capture the direction of international human rights law and are especially relevant where AI-generated allegations can be deployed at scale against journalists, critics, and political opponents.

⁷² *Criminal Code Act*, secs. 373–375; *Penal Code Act*, secs. 391–393.

⁷³ African Commission, *Declaration of Principles*, Principles 21(1)(b) and 22.

⁷⁴ *Lohé Issa Konaté v Burkina Faso* (Application No. 004/2013), African Court on Human and Peoples’ Rights, 5 December 2014) paras. 176(3)–(8), <https://www.african-court.org/cpmt/storage/app/uploads/public/633/40b/e27/63340be2743c3757080189.pdf>.

ARTIFICIAL INTELLIGENCE AND FREEDOM OF EXPRESSION IN NIGERIA

For AI-generated libel and slander, human rights safeguards should focus on publication and actual reputational harm, alongside the defenses of truth and honest opinion.⁷⁵ Given the realities of AI-generated media, remedies should prioritize correction, the right of reply, and civil process over criminal sanctions, with due-process guarantees for any proceedings.⁷⁶

⁷⁵ Human Rights Committee, *General Comment No. 34: Article 19 (Freedoms of opinion and expression)*, CCPR/C/GC/34 (2011) para. 28 and 47, <https://www.ohchr.org/sites/default/files/english/bodies/hrc/docs/GC34.pdf>.

⁷⁶ Ibid.

7. PROTECTION OF MINORS

Nigeria does not yet have a legal framework tailored to AI's impact on children. Existing protection derives from general child-protection law and from draft legislation on online child safety. The Child Rights Act, 2003, contains a catch-all prohibition on forms of sexual abuse and exploitation of children which arguably extends to the online abuse of minors.⁷⁷ The Cybercrimes Act criminalizes the production, distribution, procurement, and possession of child pornography, as well as online grooming, solicitation, and the exploitation of children in the production of child pornography.⁷⁸

The difficulty is that these provisions were not designed for AI systems. They criminalize abuse and exploitation after they occur, but they do not address AI companions, emotionally manipulative design, highly persuasive synthetic content, or transparency where children are interacting with bots rather than people. In practice, the law remains largely reactive: it can only punish harm after the fact but does not yet require child-specific safeguards designed into the tools themselves, such as age-appropriate defaults or disclosure that a system is AI. That gap matters because generative AI can make harmful content more immersive, more personalized, and harder for children and caregivers to detect early.

The most recent legislative effort, the Child Online Access Protection Bill (HB. 244), passed by the House, is the first attempt to build a systemic, platform-oriented child safety regime in Nigeria.⁷⁹ The bill would establish a dedicated E-Commissioner and a multi-agency task force to coordinate enforcement.⁸⁰ Its model is interventionist, empowering authorities

⁷⁷ *Child Rights Act 2003*, secs. 32-33.

⁷⁸ *Cybercrimes Act*, sec. 23.

⁷⁹ *House of Representatives Order Paper*, Thursday, 21 December 2023, item on *Child Online Access Protection Bill, 2023 (HB. 244)*, <https://placng.org/i/wp-content/uploads/2024/01/House-of-Reps-order-paper-Thursday-21-December-2023.pdf>.

⁸⁰ *Child Online Access Protection Bill, 2023 (HB. 244)*, sec. 2, <https://placng.org/i/wp-content/uploads/2024/01/House-of-Reps-order-paper-Thursday-21-December-2023.pdf>; Premium Times, "Reps Pass Child Online Safety Bill to Protect Minors in Digital Space," December 8, 2025, <https://www.premiumtimesng.com/health/health-news/841607-rep-passes-child-online-safety-bill-to-protect-minors-in-digital-space.html>.

to issue removal notices, blocking requests, and app takedowns for harmful material affecting children, often on very short timelines (for example, twenty-four hours).⁸¹ This reflects a strong emphasis on rapid response and content control rather than ex ante design obligations.

Although not yet law, the bill matters because it shows the direction of reform. Unlike the Child Rights Act, it moves beyond punishment after harm occurs by creating complaint systems, rapid removal tools, and platform duties to reduce children's exposure to harmful material. Its approach, however, remains content-focused and enforcement-driven, and does not directly address AI-specific risks such as manipulative conversational systems or the psychological effects of sustained interaction with synthetic agents.

None of these frameworks were designed for children in an AI environment, which introduces new risks, including emotional manipulation and dependency fostered by AI companions, and exposure to harmful synthetic content. The result is a significant regulatory gap that, if left unfilled, leaves Nigerian children without adequate safeguards against these risks.

⁸¹ *Child Online Access Protection Bill, 2023 (HB. 244)*, sec.11(1)(i).

8. EXPLICIT CONTENT

Nigeria has no dedicated framework for regulating AI-generated nonconsensual intimate images (NCII) or synthetic sexual content. Regulation relies instead on the Cybercrime Act's cyberstalking offense, which has been used to address the nonconsensual sharing of intimate material.⁸² This provision, however, was not designed for generative AI and does not distinguish between real and synthetic content. It therefore risks underenforcement against novel harms and overbroad application where intent or harm is unclear. Enforcement is also reactive, focusing on punishment after harm has occurred rather than on prevention.

This risk of overbroad application is particularly acute in Nigeria's restrictive legal environment, which includes the Same-Sex Marriage (Prohibition) Act, 2013. This legislation criminalizes certain forms of same-sex expression and association.⁸³ That environment increases the likelihood that enforcement and moderation systems, especially automated moderation, will disproportionately target sexual minorities.

⁸² *Cybercrimes Act*, sec. 24(2).

⁸³ *Same-Sex Marriage (Prohibition) Act*, 2013 (Act No. 1 of 2014), Laws of the Federation of Nigeria, secs. 1-8 [https://placng.org/lawsofnigeria/laws/Same%20Sex%20Marriage%20\(Prohibition\)%20Act,%202013.pdf](https://placng.org/lawsofnigeria/laws/Same%20Sex%20Marriage%20(Prohibition)%20Act,%202013.pdf).

9. COPYRIGHT

Nigeria's copyright framework rests on the Copyright Act, 2022, which does not yet directly address generative AI. The Act lists the works eligible for copyright protection, including literary, musical, and artistic works,⁸⁴ and its provisions will govern the use of copyrighted works for AI training, the status of AI outputs, and enforcement.⁸⁵ The law is built on a human-centered model of authorship, ownership, and liability, a model that creates uncertainty when applied to AI-generated content and to large-scale use of copyrighted material. This mismatch raises at least three concerns about how Nigeria's copyright regime applies to AI tools.

First, the Act does not address the use of copyrighted works as training data. It permits reproduction and adaptation under fair dealing for specific purposes, but it contains no express exception for text and data mining or for large-scale reproduction by AI systems. Section 20, which covers general exceptions, thus creates a gray area: AI developers may rely on these exceptions, but whether their activities qualify as fair dealing is unresolved because the provisions were not designed for data extraction at the scale of large language models. The absence of explicit text- and data-mining rules therefore risks either leaving rights holders without adequate protection or deterring innovation.

Second, AI-generated outputs raise unresolved questions of authorship and ownership. Copyright subsists in original works created by identifiable human authors, which implies a threshold of human creativity.⁸⁶ Purely AI-generated content does not fit easily within this framework, leaving such content either unprotected or artificially attributed to a user with little creative input.⁸⁷

⁸⁴ Copyright Act 2022, sec. 2.

⁸⁵ Copyright Act 2022, secs. 10 and 12.

⁸⁶ Copyright Act 2022, sec. 2.

⁸⁷ Zeynep Ülkü Kahveci, "Attribution Problem of Generative AI: A View from US Copyright Law," *Journal of Intellectual Property Law & Practice* 18, no. 11 (2023): 796–807, <https://doi.org/10.1093/jiplp/jpad076>.

ARTIFICIAL INTELLIGENCE AND FREEDOM OF EXPRESSION IN NIGERIA

Third, copyright enforcement has important effects on freedom of expression. Nigeria's copyright regime includes both civil and criminal penalties, which are legitimate but can reach lawful speech.⁸⁸ In the context of generative AI, this risk is heightened because these tools produce large volumes of content with unclear provenance, and platforms seeking to avoid liability may remove content too readily. Copyright complaints can also be used to silence journalism or criticism, especially where ownership of the content is unclear.

This creates a familiar pattern from other areas of speech regulation: uncertainty in the law shifts risk onto intermediaries, who respond by removing disputed content, including lawful expression such as parody, satire, or caricature.⁸⁹

Nigeria's copyright framework can be applied to AI tools, but it was not designed for them. The key challenge is the lack of clear, balanced rules on training data, authorship, and platform liability.

⁸⁸ Copyright Act 2022, secs. 44-47.

⁸⁹ Copyright Act 2022, sec. 20(1)(a)-(d).

10. AI-POWERED SURVEILLANCE

Nigeria's surveillance regime is governed by existing cybercrime and telecommunications legislation. These laws allow the government to monitor communications, but they do not clearly regulate how AI tools, including generative AI, may be used for that purpose.

The Cybercrimes Act is the main legal basis. It allows law enforcement agencies to intercept communications, access computer systems, and require service providers to retain and share data, subject to judicial authorization.⁹⁰ These powers are broad and technology-neutral, so they extend readily to AI systems that analyze large volumes of data, detect patterns, or flag online communications.

In addition, the Nigerian Communications Commission's Lawful Interception of Communications Regulations, 2019, require telecommunications companies to build in lawful interception capabilities and to cooperate with government agencies.⁹¹ This suggests that the technical infrastructure for surveillance is therefore already in place. A recent report by the International Centre for Investigative Reporting (ICIR) showed how Nigerian authorities have repurposed technology intended for tracking criminals to tap calls and monitor journalists.⁹² Combined with AI tools, this infrastructure can enable real-time monitoring and large-scale analysis of communications, rather than targeted interception alone. That shift puts expression and privacy rights at risk.

Nigeria's surveillance framework does not clearly limit how far these powers extend. There are no specific rules on bulk surveillance, automated monitoring, or AI-driven profiling, and oversight is limited. Although some surveillance measures require court approval, there is no comprehensive system of transparency, accountability, or independent review of how these

⁹⁰ Cybercrimes Act, sec. 39.

⁹¹ Nigerian Communications Commission (NCC), *Lawful Interception of Communications Regulations* (2019), <https://www.ncc.gov.ng/media/1123/download>.

⁹² Nanji Nandang Venley, "How Nigerian Authorities Used Technology to Tap Calls, Monitor Journalists," *The International Centre for Investigative Reporting (ICIR)*, May 14, 2026, <https://www.icirnigeria.org/how-nigerian-authorities-used-technology-to-tap-calls-monitor-journalists/>.

powers are used.

Nigeria's framework grants significant surveillance powers but provides limited safeguards against their misuse, a gap that AI tools for mass surveillance make more dangerous. The core deficiency is the absence of clear rules on necessity, proportionality, and limits on automated monitoring. Without these safeguards, AI-powered surveillance could shift from targeted law enforcement to broad monitoring of online communications, with serious implications for freedom of expression.

11. MEASURES EMPOWERING FREEDOM OF EXPRESSION

Nigeria does not yet have targeted policies that use generative AI to promote freedom of expression. Measures that support freedom of expression come indirectly from existing laws and digital policies that expand access to information and connectivity and encourage local innovation.

The Constitution's guarantee of freedom of expression, for example, could serve as a foundation for using AI tools to expand participation in public discourse.⁹³ Similarly, the Freedom of Information Act, 2011, supports access to public information that journalists, researchers, and civil society actors can analyze and disseminate with AI tools.

On the policy side, the NAIS is the only instrument that sets out the government's direction on AI. Its emphasis on inclusion, local-language development, and skills building matters for ensuring that AI tools can be used across Nigeria's diverse linguistic and social groups. These commitments could help expand access to information and support underrepresented communities. The NAIS, however, remains broad and nonbinding, with limited implementation detail.

More broadly, digital access policies and telecommunications regulation under the Nigerian Communications Act, 2003, support the expansion of broadband infrastructure.⁹⁴ The Universal Service Provision Fund (USPF), to which telecommunications operators must contribute, was established to provide internet access to underserved communities and could help close the rural-urban access gap.⁹⁵ Connectivity matters because it is a basic condition for using AI tools to create and share information. Without reliable connectivity, the expressive benefits of generative AI remain unevenly distributed.

Key gaps remain, however. Nigeria has no explicit measures to support marginalized

⁹³ Nigerian Const. sec. 39.

⁹⁴ *Nigerian Communications Act 2003*, <https://lawsofnigeria.placng.org/print.php?sn=355>.

⁹⁵ *Nigerian Communications Act 2003*, sec. 114.

ARTIFICIAL INTELLIGENCE AND FREEDOM OF EXPRESSION IN NIGERIA

communities in using AI, no structured media or AI literacy programs at scale, and limited support for open-source or public-interest AI tools. As a result, Nigeria's current framework does not yet support the use of AI to broaden participation or access to information.

In sum, measures that support freedom of expression in Nigeria exist in law and policy, but they are indirect and underdeveloped in the AI context, leaving significant room for more targeted, rights-based interventions.

12. MISCELLANEOUS

Nigeria's data protection regime is principally governed by the Nigeria Data Protection Act, 2023. Although not an AI-specific law, it is likely to be one of the most important horizontal frameworks shaping how AI systems are developed and deployed, because generative and other AI systems rely on the collection, reuse, analysis, and sharing of personal data for training, fine-tuning, and profiling.⁹⁶ Data protection therefore matters to freedom of expression and access to information not only as a privacy instrument but also as a governance framework that determines when personal data may be processed, for what purposes, and subject to which safeguards.⁹⁷

Importantly, the Act addresses automated decision-making and governs cross-border transfers of personal data,⁹⁸ provisions that are directly relevant where AI systems infer personal characteristics, rank users, or personalize information flows. In this sense, the Act may operate as an indirect but significant check on data-intensive AI practices that chill expression, facilitate profiling, or enable opaque forms of informational control.

The Nigeria Data Protection Commission's General Application and Implementation Directive (GAID) is the key operational instrument under the Act, specifying the practical compliance requirements for data controllers and processors.⁹⁹ The GAID provides detailed guidance on lawful bases for data processing, data subject rights, cross-border data transfers, and accountability measures, including documentation, impact assessments, and breach notification.¹⁰⁰ Although the GAID is not AI-specific, its provisions on automated decision-making, profiling, and risk management apply directly to AI systems that rely

96 OECD, *AI, Data Governance and Privacy* (Paris: OECD Publishing, 2024), https://www.oecd.org/content/dam/oecd/en/publications/reports/2024/06/ai-data-governance-and-privacy_2ac13a42/2476b1a4-en.pdf.

97 UN Human Rights Council, *Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression*, A/HRC/23/40 (17 April 2013), <https://docs.un.org/en/A/HRC/23/40>.

98 *Nigeria Data Protection Act 2023*, secs 37 and 41-43, <https://placng.org/i/wp-content/uploads/2023/06/Nigeria-Data-Protection-Act-2023.pdf>.

99 Nigerian Data Protection Commission, *General Application and Implementation Directive* (20 March 2025), <https://ndpc.gov.ng/wp-content/uploads/2025/03/NDP-ACT-GAID-2025-MARCH-20TH.pdf>.

100 *General Application and Implementation Directive*, arts. 16, 36-40, 45, 26, 28 and 33.

ARTIFICIAL INTELLIGENCE AND FREEDOM OF EXPRESSION IN NIGERIA

on personal data, so it functions as a horizontal governance framework for data-driven technologies.¹⁰¹ The GAID can therefore play an important role in mediating between AI deployment and freedom of expression: it shapes how personal data is collected, processed, and used in content generation, moderation, and targeting, and it imposes safeguards that may reduce the risk of opaque decision-making and unlawful restrictions on expression.

¹⁰¹ *General Application and Implementation Directive*, arts. 18, 28(3)(b), 35(6)(b).

13. CONCLUSION

Nigeria lacks a coherent, AI-specific framework for AI and freedom of expression. The field is governed instead by an indirect and fragmented body of law that both constrains expression and fails to protect it adequately. Constitutional protections provide a strong formal guarantee, but they are consistently limited by broadly framed statutory restrictions that enable state control over speech. AI and expression are therefore regulated indirectly, through general laws on elections, cybercrime, and criminal conduct, rather than through rules designed for digital or AI-driven environments.

A central finding of this chapter is that Nigeria's AI governance model is horizontal in design and substantively inadequate in protecting the right to freedom of expression. Current legislative efforts and the NAIS rely on horizontal regulation but leave the core issues unresolved, including the regulation of harmful AI-generated content. In practice, these gaps are filled by indirect governance mechanisms—intermediary liability, compliance duties, and institutional oversight—that shape the information environment without clear human rights safeguards.

This governance model produces two major issues for freedom of expression. On one side, regulatory gaps allow harmful practices—disinformation, manipulation, and abusive content—to proliferate at scale. On the other, vague and overbroad legal provisions create strong incentives for intermediaries and state actors to over-enforce, leading to content over-removal, self-censorship, and chilling effects, particularly in politically sensitive contexts. These dynamics are especially pronounced across key domains examined in this chapter—electoral speech, hate speech, defamation, and AI-powered surveillance—where existing legal frameworks are both ill-suited to AI systems and prone to misuse.

Generative AI intensifies these challenges by complicating attribution, obscuring intent, and dramatically increasing the scale and speed at which content is produced and disseminated. At the same time, Nigeria's data protection framework provides important safeguards for

ARTIFICIAL INTELLIGENCE AND FREEDOM OF EXPRESSION IN NIGERIA

personal data, but these protections coexist with expansive surveillance powers that lack clear limits on automated monitoring and profiling. The result is a governance landscape in which regulatory gaps and overbroad controls operate simultaneously, allowing harmful conduct to persist while increasing the risk of unjustified restrictions on lawful expression.

Addressing these challenges requires a more deliberate integration of human rights standards into Nigeria's emerging AI governance framework. This includes AI-specific transparency obligations, particularly requirements to label AI-generated content clearly in contexts such as elections and political communication. Speech regulation must be grounded in clear, narrow, and lawful standards consistent with international human rights law—above all the principles of legality, necessity, and proportionality—so that vague offenses cannot be turned against legitimate expression. Independent oversight and accountability mechanisms for surveillance are also essential, as are explicit limits on the use of AI for bulk monitoring, profiling, and the interception of communications. Additionally, Nigeria should adopt clearer rules on intermediary liability that reduce incentives for excessive removal while ensuring proportionate responses to unlawful content. Its ongoing governance efforts give Nigeria an opportunity to shape how AI systems interact with fundamental rights. A shift from fragmented, indirect regulation toward a coherent, rights-based AI governance framework is necessary if generative AI is not to undermine freedom of expression.



**THE
FUTURE
OF
FREE
SPEECH**

www.futurefreespeech.org