e-RIGHTS
Enhancing Digital Rights in Nigeria

AVOCATS SANS FRONTIÈRES FRANCE

THE STATE OF DIGITAL RIGHTS IN NIGERIA

BALANCING INNOVATION, SECURITY, AND FREEDOM

THE e-RIGHTS PROJECT REPORT

JANUARY 2026

Funded by the European Union

IN PARTNERSHIP WITH

CITAD CENTRE FOR INFORMATION TECHNOLOGY AND DEVELOPMENT

SPACES FOR CHANGE | S4C

The e-RIGHTS is funded by the European Union, and implemented by Avocats Sans Frontières France in Nigeria, in partnership with Spaces for Change (S4C), and the Centre for Information Technology and Development (CITAD).

The contents of this publication are the sole responsibility of ASF France,
and do not necessarily reflect the views of the donor.

Table of Contents

List of Acronyms and Abbreviations

3MTT: 3 Million Tech Talents
AI: Artificial Intelligence
AML: Anti-Money Laundering
ASF France: Avocats Sans Frontières France
ATM: Automated Teller Machine
CBN: Central Bank of Nigeria
CFT: Combating the Financing of Terrorism
CIA: Confidentiality, Integrity, and Availability
CITAD: Centre for Information Technology and Development
CNII: Critical National Information Infrastructure
CRA: Child's Rights Act
CSO: Civil Society Organisation
DPIA: Data Protection Impact Assessment
DSA: Digital Services Act (European Union)
e-RIGHTS: Enhancing Digital Rights in Nigeria
EU: European Union
FCC: Federal Communications Commission (United States)
FCCPC: Federal Competition and Consumer Protection Commission
FMCIDE: Federal Ministry of Communications, Innovation and Digital Economy
G2C: Government-to-Citizen
GAID: General Application and Implementation Directive
GDPR: General Data Protection Regulation
GSM: Global System for Mobile Communications
HB: House Bill
HRD: Human Rights Defender
ICAF: Industry Consumer Advisory Forum
ICT: Information and Communication Technology
JRETF: Joint Regulatory and Enforcement Task Force
NCA: Nigerian Communications Act
NCC: Nigerian Communications Commission
NDPA: Nigeria Data Protection Act
NDPC: Nigeria Data Protection Commission
NIMC: National Identity Management Commission
NIN: National Identity Number
NITDA: National Information Technology Development Agency
NJI: National Judicial Institute
NODR: Nigerian Observatory on Digital Rights
POS: Point-of-Sale
PSB: Payment Service Bank
S4C: Spaces for Change
SB: Senate Bill
SON: Standards Organisation of Nigeria

Preface

As Nigeria's digital economy matures, the boundary between our physical and virtual lives has all but vanished. In 2025, digital participation is no longer a luxury of the elite; it is the primary medium through which the Nigerian citizen seeks information, builds livelihoods, and demands accountability. However, this rapid transition has brought us to a critical inflection point where the tools of empowerment are increasingly being repurposed as instruments of control.

This report, a product of the eRIGHTS Project, arrives at a time when the "digital frontier" in Nigeria is both expanding and tightening. While we celebrate milestones like the 2023 Data Protection Act and the rollout of the National AI Strategy, we cannot ignore the persistent shadows of surveillance, the misapplication of the Cybercrimes Act, and the growing digital divide that threatens to leave millions behind.

Since its inception in 2023, the European Union Funded eRIGHTS project—led by Avocats Sans Frontières France in Nigeria in partnership with Spaces for Change (S4C) and the Centre for Information Technology and Development (CITAD)—has stood at the intersection of law, technology, and human rights. We have witnessed a period where "passive compliance" ended, and "active enforcement" began. Yet, the central tension remains unresolved: Does this new era of enforcement serve the public interest, or does it merely consolidate digital authority at the expense of fundamental freedoms?

Within these pages, we present a comprehensive analysis of the state of digital rights in Nigeria. We move beyond statistics to highlight the stories of journalists navigating digital censorship, youth activists and women facing online harassment, and the legislative hurdles that continue to stifle the full expression of a Digital Rights legislation.

The findings within this report confirm that Nigeria's digital trajectory is not a matter of chance, but a matter of choice. As we look beyond the 2023–2025 cycle of the eRIGHTS project, the evidence demands a transition from monitoring violations to institutionalizing protections. To ensure that the digital age strengthens rather than subverts our democracy.

This report is not merely a retrospective; it is a call to action. It serves as a roadmap for legislators to build trust, for civil society to sharpen its advocacy, and for the private sector to prioritize the safety of its users.

The eRIGHTS project has laid the foundation for a more resilient digital society. However, the architecture of freedom is never complete. We invite all stakeholders to move beyond the pages of this report and join us in the active labor of defending the digital frontier. The time for passive observation has passed; the era of principled action is here.

Digital rights are human rights. As we navigate the complexities of 2026 and beyond, our collective goal remains unchanged: to ensure that the Nigerian digital space remains an open, safe, and democratic commons for all.

Angela Uwandu Uzoma-Iwuchukwu
Country Director,
Avocats Sans Frontières France
(Lawyers Without Borders France)

About the e-RIGHTS Project

The Enhancing Digital Rights in Nigeria (e-RIGHTS) project is an initiative aimed at promoting the rights of Nigerians in the digital sphere. It focuses on harnessing the opportunities of new technologies while addressing the unique challenges they present.

The project is implemented by Avocats Sans Frontières France (ASF France) in Nigeria, with funding support from the European Union. It is executed in partnership with Spaces for Change (S4C) and the Centre for Information Technology and Development (CITAD).

Core Objectives of the Project

The e-RIGHTS project addresses the need for a free, open, and safe internet for all citizens. Its specific objectives are to:

- **Provide a safe online platform:** Enable human rights defenders to monitor and report digital rights breaches, including data privacy violations, cyber threats, internet shutdowns, and attacks on social media spaces, ensuring prompt responses to these threats.
- **Establish a Multi-Stakeholder Situation Room:** Create a collaborative hub for CSOs, lawyers, academics, tech providers, and government partners to coordinate on digital rights issues. The technical members of this room will also develop policy guides for data and digital rights protection in Nigeria.
- **Provide Legal Intervention:** Mobilise a network of digital rights lawyers to intervene in identified cases of digital rights violations.
- **Build Capacity:** Train CSOs, lawyers, journalists, activists, and human rights defenders on digital rights advocacy and data security best practices.

Implementation Areas

The project has been implemented in four key locations:

- Federal Capital Territory (Abuja)
- Lagos State
- Kano State
- Imo State

Target Groups & Beneficiaries

The project directly serves:

- Nigerian internet users
- Victims of digital threats
- Private sectors
- Students
- Lawyers and Judges
- Activists and Human Rights Defenders (HRDs)
- Government agencies
- Journalists
- Social media influencers

Acknowledgements

Avocats Sans Frontières France (ASF France) extends its profound gratitude to the numerous individuals and organisations whose expertise, dedication, and support made the e-RIGHTS project possible. Its completion reflects a collective commitment to safeguarding human rights in the digital age.

We sincerely acknowledge the intellectual assistance of Dr. Iheanyi Nwankwo in compiling this report. We also recognise the invaluable research contributions of Angela Uwandu Uzoma-Iwuchukwu, Onyinyechi Nwachukwu and Akinsola Ganiyu.

We extend our sincere appreciation to Antoine Passavant, Program Officer at ASF France Headquarters, and to the entire French pool of expertise, led by Ivan Paneff, for their valuable support on this project.

This work would not have been possible without the strategic partnership and collaborative efforts of Spaces for Change (S4C) and the Centre for Information Technology and Development (CITAD). Your grassroots insights and advocacy experience were instrumental in grounding this report in the lived realities of Nigerians.

We are deeply grateful to the European Union for their generous funding and sustained support of the e-RIGHTS project. In particular, we extend our appreciation to Wynyfred Achu Egbuson of the European Union Delegation to Nigeria for her guidance and commitment to the project's success.

Our sincere thanks go to the members of the eRIGHTS Expert Group, drawn from the Academia, Government Regulators and agencies such as NITDA, NCC, NDPC, NHRC, Journalists, Tech Companies, Lawyers, and Civil Society Organizations whose critical feedback and domain expertise helped in the development of a e-RIGHTS Policy Guide which is a major advocacy tool, an invaluable resource for digital rights policy reforms in Nigeria..

Finally, we acknowledge the federal legislators from the National Assembly and the various government agencies who facilitated critical discussions and provided the legislative context necessary for this review. Your engagement is vital as we work together to bridge the gap between policy and practice in Nigeria's digital ecosystem.

Executive Summary

Nigeria's accelerating digital transformation

Nigeria's accelerating digital transformation has positioned technology as a core driver of economic growth, governance, and social participation. The internet increasingly functions as a new public square—expanding access to services, enabling innovation, and supporting financial inclusion. At the same time, this transformation presents a clear policy challenge: the same digital infrastructure that empowers citizens can also be deployed for surveillance, censorship, and other practices that undermine constitutional rights. Addressing this dual-use reality is now a central governance imperative.

This report assesses the Nigerian digital landscape, focusing on the intricate link between technological advancements and human rights. Rather than simply conflating digital rights with the traditional binary of privacy and freedom of expression, this analysis employs a functional taxonomy built upon five core pillars:

1. **Access and Participation:** The prerequisite capabilities to engage in the digital world.
2. **Personality, Digital Identity and Inheritance:** Protection of the digital self, including privacy and freedom from unauthorised appropriation and digital heritage.
3. **Expression in the Digital Space:** The right to seek, receive, and impart information online.
4. **Remedy and Due Process:** Access to justice when digital rights are violated.
5. **Cybersecurity:** Protection of integrity of systems and protection from cyber-harms.

This report highlights four key findings:

The Pace of Legislative Interventions

Rapid technological change outpaces the legal framework. Legislative progress lags behind technology's evolution and new complex online threats from both public and private entities. Although a recent, swift NDPA amendment suggests improved legislative responsiveness, the judiciary currently acts as a critical stopgap, applying existing law to novel digital contexts.

The Use of New Media and Public Perception

Digital transformation facilitates free expression but fuels misinformation. Government attempts to regulate this, such as the 2019 Hate Speech and Social Media Bills, have been criticised due to provisions seen as suppressing dissent, exacerbated by State actors misusing the Cybercrimes Act.

Public Engagement and Multistakeholders Participation in Digital Governance

Nigeria's digital governance is primarily top-down, limiting engagement and collaboration from the public, civil society, and private sector. Existing G2C platforms prioritise efficiency over democratic participation, making citizens passive users.

The "Rights-Resource" Tension in Nigeria's Digital Landscape

Nigeria's limited digital rights stem mainly from economic and infrastructural deficits, not just legal issues. Achieving digital inclusion requires treating internet access as a public utility and investing heavily in affordable, reliable physical infrastructure, broadband, and the national power grid.

Recommendations

To realise the full potential of the digital landscape while simultaneously safeguarding human rights, the following recommendations are directed toward the key stakeholders:

The Legislature

- Adopt value-guided and strategic legislative architecture.
- Adopt a more proactive legislative approach.
- Leverage research and expertise to keep pace with change.
- Prioritise key digital rights legislation.

The Executive and Regulatory Agencies

- Strengthen inter-agency coordination and close enforcement gaps.
- Ensuring consistent and impartial enforcement across public and private sectors.
- Preventing the misuse of cybercrime laws against journalists and civic actors.

The Judiciary

- Build capacity for digital rights adjudication.

Civil Society and Media

- Strengthen public resilience through digital literacy and strategic litigation.

Private Sector

- Embed human rights, transparency, and accountability in platform design and operations.

INTRODUCTION

The Digital Nigeria and the Rights at Stake

1.1. Background and Context

Nigeria's digital transformation has transcended mere technological adoption to becoming central to the nation's economic, political, and social existence. Fueled by a burgeoning youth demography and the exponential growth of mobile telephony,[1] the digital space in Nigeria has evolved into a primary infrastructure for daily life, from anchoring a globally recognised fintech ecosystem[2] to social mobilisation.[3] This ubiquity signifies a fundamental shift in the locus of power. The internet is no longer a luxury for the elite but a "new public square" for the masses. Consequently, access to the digital realm is now synonymous with access to citizenship itself; to be disconnected is to be economically and politically disenfranchised. Thus, the stakes of digital governance have never been higher.

However, this profound reliance on digital infrastructure creates a "dual-use" paradox: the same tool that democratizes power simultaneously creates new vectors for human rights violations. The 2020 #EndSARS protests serve as the archetype of this tension.[4] While social media platforms allowed citizens to bypass traditional censorship and organize widely, they also exposed the digital footprint of activists to State surveillance and targeted harassment.[5] This dynamic reveals that the digital sphere is a contested terrain. On one hand, it acts as a force multiplier for fundamental rights, enabling freedom of expression and economic inclusion for marginalised groups.[6] Conversely, precisely because it is so effective at challenging the status quo, the digital space has become a priority target for authoritarian control.[7]

[1] Between October 2024 and September 2025, about 7 million mobile GSM subscribers were added, bringing the total number of subscribers to over 142 million as of October 2025. See NCC, "Industry Statistics" https://ncc.gov.ng/market-data-reports/industry-statistics accessed 5 January 2026.
[2] One report estimated the Nigerian fintech market size at ~US$1.13 billion in 2024 and projected it to reach ~US$4.24 billion by 2033 (CAGR ~15.8 %). See Imarc, "Nigeria Fintech Market Size, Share, Trends and Forecast by Deployment Mode, Technology, Application, End User, and Region, 2025-2033" https://www.imarcgroup.com/nigeria-fintech-market accessed 5 January 2026.
[3] A 2024 ranking of daily social media usage places Nigeria 5th globally. See Makua Ubanagu, "Full list: Nigeria ranks fifth globally in daily social media usage" Punch (4 November 2024) https://punchng.com/full-list-nigeria-ranks-fifth-globally-in-daily-social-media-usage/#:~:text=Getting%20your%20Trinity%20Audio%20player,2%20hours%20and%2030%20minutes. See also Joel Augustus-Daddie, et al., "The functionality of social media and its implications for national development in Nigeria" IJO Journal vol 8 (5) 2025 https://ijojournals.com/index.php/bm/article/view/1074/574 accessed 5 January 2026.
[4] Prince Ekoh & Elizabeth George, "The role of digital technology in the EndSars protest in Nigeria during COVID-19 pandemic" J. Hum. Rights Soc. Work 6, 161–162 (2021) https://doi.org/10.1007/s41134-021-00161-5 accessed 5 January 2026.
[5] Hannah Ajakaiye, "Data trails: how Nigeria's state surveillance crackdown on journalists, active citizens" ACSUS (13 October 2022) https://www.africa-usforum.africa/data-trails-how-nigerias-state-surveillance-crackdown-on-journalists-active-citizens/ accessed 5 January 2026.
[6] European Parliament, "Information and communication technologies and human rights" (2010) https://www.europarl.europa.eu/RegData/etudes/etudes/join/2010/410207/EXPO-DROI_ET(2010)410207_EN.pdf accessed 5 January 2026.
[7] European Parliament, "Digital technologies as a means of repression and social control" (2021) https://www.europarl.europa.eu/RegData/etudes/STUD/2021/653636/EXPO_STU(2021)653636_EN.pdf accessed 5 January 2026.

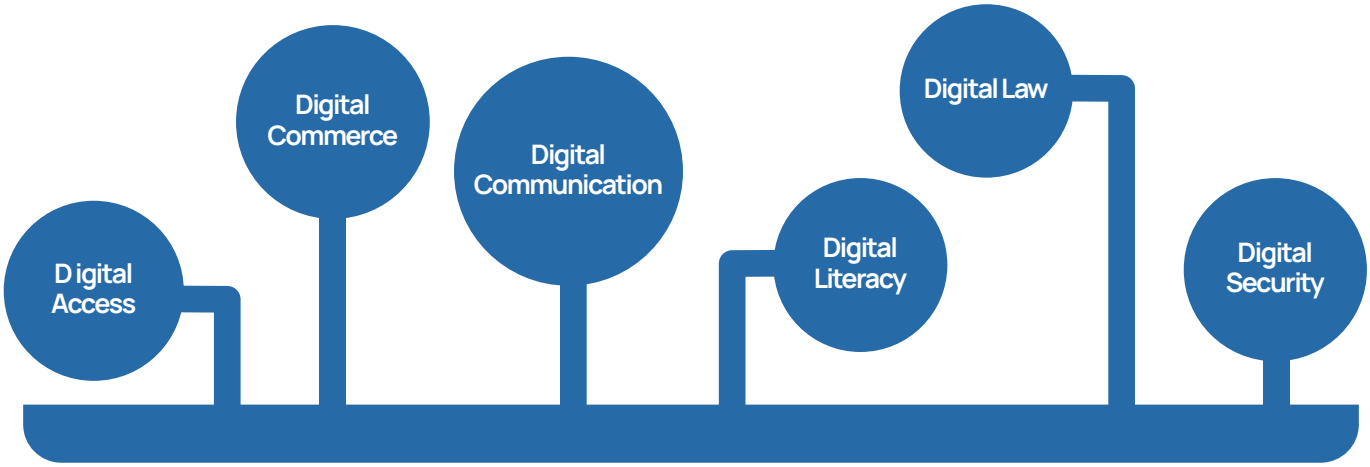
The very architecture that facilitates "citizen journalism" can be weaponised for disinformation, censorship, and opaque surveillance. Therefore, while the digital revolution offers a path to empowerment, it has inevitably set the stage for a new generation of human rights abuses.

1.2. The Nature of Digital Rights

Digital rights are human rights. Human rights are inherent to every person, independent of characteristics such as race, sex, nationality, ethnicity, language, or religion. These rights impose a corresponding duty on the State to respect, protect, or fulfill them.[8] Historically, such rights have been foundational to a just and equitable society, and were typically conceived within the context of physical space. However, the increasing digitization of modern life introduces a new dimension that requires a reassessment of how these traditional rights are interpreted and applied in the digital era.

The prevailing view, encapsulated by the UN Human Rights Council's doctrine of "Offline/Online Equivalence," asserts that "the same rights that people have offline must also be protected online."[9] This doctrine sees digital rights as an extension of the traditional rights. Consequently, States are expected to interpret and apply traditional rights, such as freedom of expression and privacy, so that they extend into the digital realm for their citizens.

However, the "equivalence" model has limits; digital interactions often generate unique frictions that lack a direct analog in the physical world, necessitating the conceptualization of "Novel Rights." For instance, the "Right to Internet Access" or the "Right to Algorithmic Explanation" (in the context of AI) do not have perfect traditional equivalents. Arguments for these new rights are plausible because technologies push the boundaries of human agency in unprecedented ways. Yet, the recognition of these novel rights faces a harsh pragmatic barrier: Cost. Unlike "negative rights" (e.g., freedom from censorship), which cost little to implement, "positive rights" (e.g., right to internet access) require immense capital investment in fiber optics, broadband networks, and data centres. This creates a rights-resource tension, where the theoretical expansion of digital rights collides with the fiscal reality of the State, particularly in developing economies.
Given this complexity, a monolithic definition of digital rights is insufficient for rigorous analysis. Public discourse often conflates these issues, reducing the entire landscape of protecting human rights in the digital space to merely "data privacy" and "freedom of expression." Such oversimplification masks the nuance of the threat landscape because progress in one area (e.g., enacting a Data Protection Act) can often coexist with, or even mask, regression in others (e.g., the lack of effective remedy in disputes arising in the digital environment). Therefore, it is safer to conceive the term digital rights as an umbrella term to represent the many dimensions of rights that are indispensable for effective and meaningful participation in the digital space. These rights are essential not only for upholding democratic values and principles but also for ensuring that the rapidly expanding digital economy is inclusive, secure, and just for all.



[8] United Nations, "Human Rights" https://www.un.org/en/global-issues/human-rights accessed 5 January 2026. [9] See UN Human Rights Council, Forty-seventh session 21 June–14 July 2021, A/HRC/RES/47/16.
[9] See UN Human Rights Council, Forty-seventh session 21 June–14 July 2021, A/HRC/RES/47/16.

There is currently no universally accepted categorisation of digital rights. To assess the true state of how human rights are protected in the digital space in Nigeria, this report utilizes a functional taxonomy to group these rights based on their specific purpose and operational impact. This allows us to map the digital rights landscape into five facets to isolate specific variables and measure their development across the Nigerian ecosystem. This grouping includes rights focusing on the following:

1. Access and Participation
These rights are the prerequisite capabilities required to engage meaningfully in the digital world. They extend beyond mere physical connectivity (infrastructure) to include digital literacy and the removal of economic barriers. Crucially, this is the gateway right; without it, other digital rights cannot be meaningfully exercised.

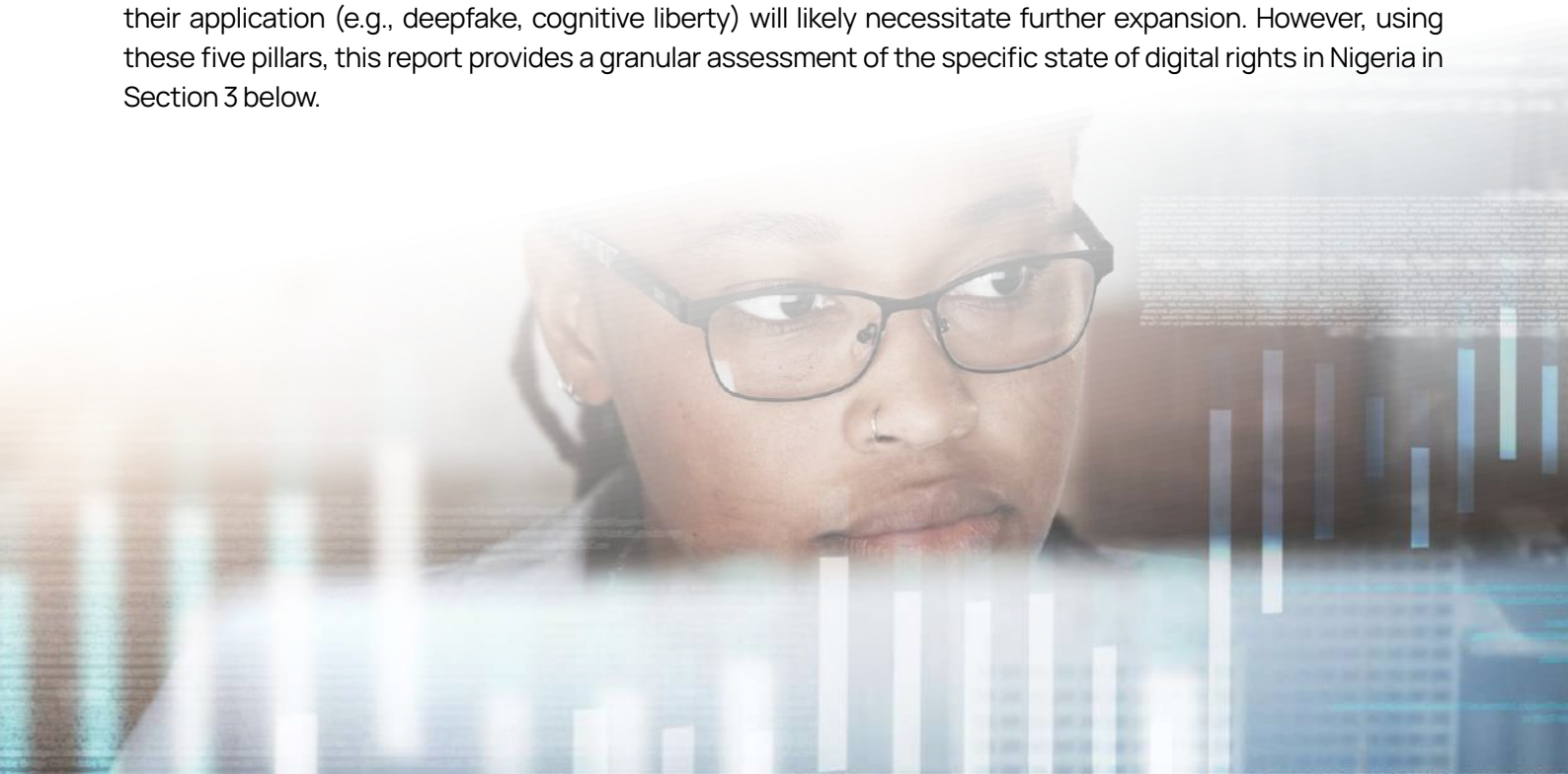
2. Personality, Digital Identity and Inheritance
These encompass the rights of individuals to protect their privacy, dignity, and exert control over their personal information from arbitrary State surveillance or corporate misuse. It also addressed the inheritance of digital assets.

3. Expression in the Digital Space
This critical facet involves the right to seek, receive, and impart information and ideas online without fear of censorship, reprisal, or undue restrictions. It covers aspects like freedom of expression, freedom of the press in online media, and access to diverse sources of information.

4.Remedy and Due Process
Often overlooked but critically important, these rights ensure that citizens have access to effective justice mechanisms and can receive fair redress when their digital rights are violated. This applies whether the infringement is perpetrated by State actors or non-state entities. It includes the right to a fair hearing, access to judicial and non-judicial remedies, and transparent accountability for digital harms.

5. Cybersecurity
These rights are paramount for fostering safety, trust, and resilience within digital spaces. They encompass cybersecurity and protections against cybercrime.

It is crucial to note that this mapping is dynamic. As technologies like Generative AI evolve, issues surrounding their application (e.g., deepfake, cognitive liberty) will likely necessitate further expansion. However, using these five pillars, this report provides a granular assessment of the specific state of digital rights in Nigeria in Section 3 below.



1.3. Methodology and Research Approach

This report adopted a two-pronged research methodology to ensure comprehensive and well-rounded data collection and analysis. First, the study undertook a desktop and doctrinal analysis, involving a systematic examination of existing legal, policy, and scholarly materials to establish the normative and contextual framework for digital rights in Nigeria.

This phase included a review of primary legal sources, such as the Constitution of the Federal Republic of Nigeria, relevant Acts of Parliament, subsidiary legislation, and judicial decisions, which together constitute the foundational legal framework governing rights and freedoms in Nigeria. These instruments were critically assessed for their applicability, adequacy, and adaptability to digital and technology-mediated contexts. In addition, secondary sources, including academic literature, civil society organisation (CSO) reports, policy briefs, and comparative materials, were analysed to provide contextual grounding, comparative insights, and critical perspectives on emerging digital rights issues.

Second, the report analysed empirical and project-generated data produced during the lifespan of the e-RIGHTS Project, enabling the triangulation and validation of findings from the doctrinal review. These sources included field data capturing the lived experiences, and perceptions of diverse digital rights stakeholders across Nigeria; expert group discussions; the e-RIGHTS Digital Policy Guide; the e-RIGHTS Project Brochure; and two thematic policy briefs focusing on cybersecurity and artificial intelligence and human rights.

Taken together, this approach allowed the report to bridge theory and practice by combining legal analysis with lived realities and expert insights. The methodology strengthened the reliability of the findings, ensured contextual relevance, and provided a robust basis for the recommendations advanced in this report.

1.4. Scope and Limitation of the Report

This report presents an assessment of specific themes on the current prevailing legal, regulatory, and policy frameworks around digital rights, together with the practices and institutional mechanisms that affect these rights. The analysis does not cover all emerging issues within the digital rights landscape. The limited availability of comprehensive and reliable public data places constraints on the breadth of coverage of this report.

In addition, the analysis is focused primarily on federal legislation and policies. While notable state-level initiatives or actions and their implications on digital rights are acknowledged,[10] they are not covered in this report.

[10] See Ibrahim Hamisu, "CITAD raises the alarm over rising digital rights violations" Blueprint (21 December 2025) https://blueprint.ng/citad-raises-the-alarm-over-rising-digital-rights-violations/ accessed 19 January 2026.

REGULATORY LANDSCAPE

The Legal and Institutional Framework Around Digital Rights in Nigeria

2.1. Constitutional Foundations

Nigeria, like many other countries, had a constitution that existed before the rapid digitalization that we have today. The 1999 Constitution (as amended) was conceived in an analog era and does not explicitly mention "digital rights." However, its provisions can be interpreted to a large extent to cover digital governance. This extension relies on the doctrine of the Constitution as a "living instrument"—a dynamic document capable of evolving to address realities not envisaged by its original framers.[11] Under this view, cyberspace cannot be seen as a lawless void, rather as a new extension of the Nigerian State's jurisdiction, irrespective of how imaginary such a space looks. Therefore, the fundamental rights enshrined in Chapter IV of the Constitution, such as, Dignity, Privacy, Expression, Assembly, among others, must not be seen merely as physical protections, but as "platform-neutral" guarantees.

This approach allows the "digital citizen" to be situated within the existing constitutional framework, ensuring that a violation committed via cyberspace is treated with the same commitment as if committed in a town square.

The following constitutional provisions illustrate the extent to which this constitutional evolution has been deployed to address digital rights concerns:

The first frontier of this constitutional extension involves the individual's right to Human Dignity (Section 34) and Privacy (Section 37)). While Section 34 traditionally prohibits "inhuman or degrading treatment" such as physical torture, the digital era has introduced new forms of degradation, exemplified by "revenge porn" (the non-consensual sharing of intimate images). Similarly, Section 37 guarantees the privacy of "telegraphic communications," a term that modern jurisprudence naturally extends to emails and encrypted messaging.[12] These provisions are critical because they reframe data violations as human rights abuses. Revenge porn, for instance, is not just a privacy issue; it is a profound violation of human dignity akin to psychological torture. Likewise, by extending Section 37 to cover "personal data," the courts have effectively elevated data protection from a technical best practice to a constitutional obligation.[13] Consequently, a private entity's or State's failure to secure citizen data is not just a business or administrative lapse; it would be seen as a breach of a fundamental right to private life.

[11] See Nafiu Rabiu v. The State (1980) 8–11 SC 130.
[12] In Continental Sales Ltd v. R. Shipping INC (CA/L/807/2010), the court stated: "...There is no reason why, in this context, delivery of a document by e-mail – a method habitually used by businessmen, lawyers and civil servants – should be regarded as essentially different from communication by post, fax or telex."
[13] See Digital Rights Lawyers Initiative v. National Identity Management Commission Appeal Number CA/IB/291/2020; Olatokunbo Oladapo v. Polaris Bank Limited (Suit No. FHC/L/CS/5842/2021).

Protecting the Digital Square

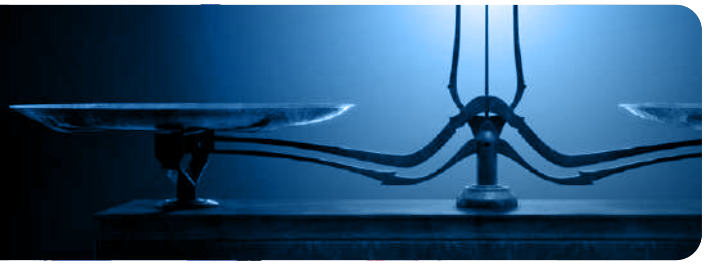
Expression, Assembly, and Non-Discrimination

Beyond the individual, the Constitution also safeguards the collective democratic process through Freedom of Expression (Section 39), Assembly (Section 40), and Non-Discrimination (Section 42). Application of these rights have found new meaning in the digital sphere as the new "public square". Section 39's right to "impart ideas... without interference" would directly challenge the legality of internet shutdowns, while Section 40 validates virtual mobilisation as a legitimate form of assembly. Furthermore, Section 42's prohibition of discrimination based on ethnicity or origin, would apply to algorithmic decisions.

However, enforcing these rights face the stiffest resistance from the State. For example, the "cyberstalking" provisions of the Cybercrimes Act appears to have been weaponised to criminalise "imparting of ideas", potentially creating a chilling effect on digital journalism (e.g., the Agba Jalingo case).[14] Similarly, as Nigeria adopts AI in sectors like banking, antidiscrimination faces a new test: Algorithmic Bias. If an automated system denies loans based on data proxies on any of the protected attributes, it would violate the spirit of non-discrimination even if no human is involved. Thus, the implementation of Chapter IV in a digital environment requires a vigilance against both overt censorship and covert algorithmic exclusion.

The Derogation

Section 45



Yet, these digital protections are not absolute; they are structurally limited by Section 45, which permits derogation in the interest of "defence, public safety, public order...." This section provides the legal basis for national security legislation, including the Cybercrimes Act 2015 and the various mandates of the National Information Technology Development Agency (NITDA), and other agencies.

However, it is notable that while the State can limit rights for security purposes, Section 45 requires that any such law be "reasonably justifiable in a democratic society." The friction arises because national security is often invoked broadly to justify digital repression (like the Twitter Ban)[15] without satisfying the strict requirements of necessity and proportionality. The future of digital rights in Nigeria will be impacted by the manner of enforcing the justifiability standard of Section 45 against government overreach.

[14] See Global Freedom of Expression, SERAP v. Federal Republic of Nigeria (Case of Agba Jalingo) https://globalfreedomofexpression.columbia.edu/cases/serap-v-federal-republic-of-nigeria-case-of-agba-jalingo/#:~:text=Facts,and%20the%20Criminal%20Code%20Act accessed 10 January 2026.

[15] PLAC, "Information minister and the Twitter ban" (29 June 2021). https://placng.org/Legist/information-minister-and-the-twitter-ban/ accessed 10 January 2026.

The Limits of Judicial Transposition

The judiciary plays a very important role in transposing the traditional human rights provisions to the digital sphere. The case of Digital Rights Lawyers Initiative v. National Identity Management Commission[16] exemplifies this approach, where the Court of Appeal ruled that the right to privacy under Section 37 of the 1999 Constitution encompasses the protection of personal information. However, relying solely on the transposition of traditional provisions is structurally limited by the fundamental disconnect between analog and digital realities. Traditionally, constitutional texts were drafted in a language that envisages physical tangibility, exemplified by phrases like the "inviolability of the home" or "secrecy of correspondence". But these provisions struggle to encompass modern intangible threats and assets, such as algorithmic profiling, metaverse, metadata collection, or neuro-technological interference, where no physical trespass occurs.

Consequently, the transpositional approach may create a protection gap where citizens are left defending themselves with "analog shields against digital swords," unable to challenge harms inconceivable to the Constitution's original drafters. This inadequacy has necessitated a move beyond mere interpretation toward explicit structural reforms in legal frameworks.

To bridge this protection gap, several jurisdictions have diverged in their approaches: some amended their constitutional frameworks and others enacting specific legislation. Greece, for example, explicitly amended its Constitution in 2001 to include the right to participate in the information society, placing an obligation on the State to facilitate access,[17] while Portugal enacted a Charter of Human Rights in the Digital Age that codifies digital rights in a specific law.[18] In contrast, Nigeria has not pursued a constitutional amendment but has instead adopted an approach of enacting specific laws like the Nigeria Data Protection Act (NDPA) to address the impact of digitalization in various domains.

The following section will evaluate these specific instruments to determine how effectively they have advanced digital rights.

2.2. Key Statutory Frameworks Around Digital Rights

Although the Constitution provides the doctrinal foundation for digital rights governance, the operational realities are defined by several statutory instruments. These laws determine, for example, how personal data is processed, how the digital space is policed, how consumers are protected, how access to public information is regulated, among others. Some of these laws will be discussed below.

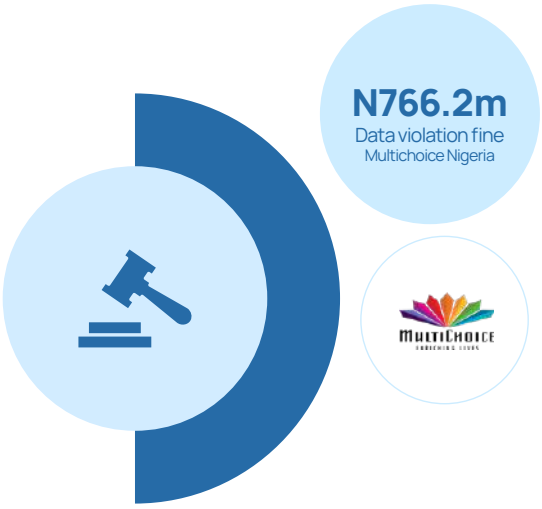
[16] Appeal Number CA/IB/291/2020. See also Olatokunbo Oladapo v. Polaris Bank Limited (Suit No. FHC/L/CS/5842/2021) where the Federal High Court explicitly extended the constitutional right to privacy to data protection principles.
[17] See Article 5A of the Greek Constitution as amended.
[18] Carta Portuguesa de Direitos Humanos na Era Digital (Lei n.º 27/2021) (Portuguese Charter of Human Rights in the Digital Era (Law 27/2021 of May 17). It is primarily principle-based rather than prescriptive. See also the Spain Charter of Digital Rights which is not regulatory in nature but rather a guide intended to frame the interpretation of existing laws and future regulations https://portal.mineco.gob.es/RecursosNoticia/mineco/prensa/noticias/2021/SPAIN_Charter-of-Digital-Rights.pdf accessed 10 January 2026.

2.2.1. The Nigeria Data Protection Act (NDPA) 2023

The enactment of the NDPA in 2023 represented the most significant legislative advancement for digital rights in Nigeria's history. It transitioned the country from a patchwork of regulations to a comprehensive primary statute on data protection.

The Act established the Nigeria Data Protection Commission (NDPC) as an independent supervisory authority,[19] thereby aligning Nigeria with global practices like the GDPR. Crucially, it introduced extraterritorial jurisdiction, meaning foreign entities processing Nigerian data, even if they have no physical infrastructure in Nigeria, are bound by its provisions. The Act contains a "bill of rights" for data subjects, including the right to erasure, data portability, and protection from automated decision-making, among others,[20] which are relevant for the digital era. Recently, the General Application and Implementation Directive (GAID)[21] was issued by the Commission to further clarify compliance requirements, signaling a maturing regulatory environment.

Undoubtedly, the NDPA has demonstrably strengthened citizens' ability to seek legal remedies, evidenced by an uptick in both litigation and complaints to the supervisory authority regarding personal data and privacy violations.[22] This legal weight has empowered individuals and civil society organisations to actively challenge both private entities and government bodies suspected of violating the NDPA's mandates. The variety of cases underscores this trend and reflects a new willingness to use the law to seek justice. Crucially, these legal actions are expected to establish significant precedents, thereby shaping how the Act is interpreted and applied, and cementing its status as a vital instrument for protecting digital rights within the country.



However, a significant enforcement gap remains, primarily because the NDPC appears to apply the NDPA selectively. While the Commission has actively sanctioned private sector entities, such as the **N766.2 million** fine levied against Multichoice Nigeria for data violations,[23] it has noticeably hesitated to impose similar punitive sanctions on government institutions. For instance, despite the March 2024 investigation into the National Identity Management Commission (NIMC) following allegations that unauthorised third-party sites were selling citizens' National Identity Numbers (NINs) for as low as **N100,** no comparable financial penalty or public sanction has been issued against the agency.[24] This uneven application of the law suggests that government agencies are not subject to the same strict oversight as private corporations. This perception could diminish the Act's effectiveness.

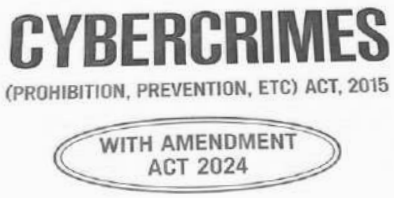
[19] The NDPC replaced the Nigeria Data Protection Bureau (NDPB), which was set up by the Federal Government in 2022 following the issuance of the Nigeria Data Protection Regulation (NDPR) in 2019.
[20] See Part VI of the NDPA.
[21] https://ndpc.gov.ng/wp-content/uploads/2025/07/NDP-ACT-GAID-2025-MARCH-20TH.pdf accessed 10 January 2026.
[22] The NDPC Report 2024 indicates that the NDPC is investigating 213 cases and the subject matter of these investigations are diverse ranging from behavioural profiling to unlawful use of CCTV. See https://ndpc.gov.ng/resources/ accessed 19 January 2026.
[23] "NDPC fines MultiChoice 766m for data privacy violations" Punch (6 July 2025) https://punchng.com/ndpc-fines-multichoice-%E2%82%A6766m-for-data-privacy-violations/ accessed 20 January 2026. Other private institutions fined by the Commission include: Fidelity Bank PLC and Meta. It has also issued compliance notices to banks, insurers, pension and gaming firms. See Ayodeji Adegboyega, "NDPC issues compliance notices to banks, insurers, pension and gaming firms" Premium Times (2025) https://www.premiumtimesng.com/business/816603-ndpc-issues-compliance-notices-to-banks-insurers-pension-and-gaming-firms.html accessed 20 January 2026.
[24] Ladi Patrick-Okwoli, "NDPC investigates alleged Privacy Breach at NIMC" Business Day (18 March 2024) https://businessday.ng/news/article/ndpc-investigates-alleged-privacy-breach-at-nimc/

Furthermore, a lack of transparency plagues the Commission's investigative processes, as detailed reports required to evaluate the findings are not made public. The sheer scale of data protection issues is evidenced by the 213 cases investigations according to the NDPC 2024 report.[25] Addressing this requires a major push for public awareness, including detailed reports on how these investigations are resolved.

A notable development is the NDPA amendment bill[26] currently before the National Assembly, which aims to strengthen accountability by mandating social media platforms, data controllers, and processors to establish physical offices within Nigeria.[27] This is a welcomed development as that will bring these actors within the reach of both regulators and citizens.

2.2.2 The Cybercrimes Act 2015

If the NDPA is the "shield" for citizen data, the Cybercrimes (Prohibition, Prevention, etc.) Act of 2015 is the state's "sword" for policing the digital domain.



Enacted toprotect critical infrastructure and combat fraud, the Act criminalises a broad spectrum of offenses ranging from identity theft and child pornography to cyber-terrorism. It was amended in February 2024, specifically addressing issues raised by the ECOWAS Court regarding the controversial "cyberstalking" provisions of section 24.[28]

However, despite this amendment, the Act suffers from a legislative lag. Drafted in an era of simple phishing scams, does not seem robust enough to structurally handle the nuance of modern threats such as AI-generated deepfakes or digital likeness appropriation. Although some of its provisions might be interpreted to cover new cyber offenses, such stretching may face definitional challenges leading to legal ambiguity. Furthermore, the Act remains focused on State security (critical infrastructure) rather than victim recovery. It lacks adequate provisions for supporting cyber victims who suffer financial, psychological or reputational ruin from cybercrime and attacks.

The Act inadequately addresses the full scope of cybersecurity,[29] particularly failing to mandate proactive measures and comprehensive protection beyond designated Critical National Information Infrastructure (CNII). This leaves sectors not classified as critical, such as SMEs and non-essential private organisations, vulnerable. These entities, which often hold sensitive data and contribute significantly to the economy, lack specific mandated baseline security requirements or support mechanisms in the legislation. This gap in addressing these "weakest links" compromises the nation's overall digital ecosystem, necessitating a holistic reform of the digital security chain.

It is notable on the international front that Nigeria acceded to the Council of Europe Convention on Cybercrime in July 2022.[30] It has also recently in Hanoi, signed the UN Convention against Cybercrime in October 2025. However, these international treaties will have no local effect until they are domesticated in accordance with Section 12 of the Nigerian Constitution.

[25] See https://ndpc.gov.ng/resources/ accessed 19 January 2026.
[26] Nigeria Data Protection Act (Amendment) Bill, 2024 (SB 650).
[27] Aluko & Oyebode, "Commentaries on the Nigeria Data Protection Act Amendment: Social Media Platforms and Data Controllers/Processors Local Office Registration Requirement" (March 2025) https://www.aluko-oyebode.com/wp-content/uploads/2025/03/Commentaries-on-the-Nigeria-Data-Protection-Act-Amendment-Social-Media-Platforms-and-Data-Controllers-Local-Office-Registration-Requirement.pdf accessed 10 January 2026.
[28] " Recall that the ECOWAS court found Section 24 of the Cybercrime Act in violation of the African Charter on Human and Peoples' Rights. See ECW/CCJ/APP/09/19. Following the 2024 amendments, SERAP filed a new suit (ECW/CCJ/APP/03/2025) in early 2025 challenging the new, amended law, stating that the authorities continue to use it to stifle free speech.
[29] See Iheanyi Nwankwo and Angela Uzoma - Iwuchukwu, "Policy brief: Reforming Cybersecurity Regulation in Nigeria" (July 2025) https://gkrjynvdzvwwvekrrlif.supabase.co/storage/v1/object/public/publication-files//Policy%20Brief_final.pdf accessed 10 January 2026
[30] Council of Europe, "Original instrument confirming Nigeria's accession to the Convention on Cybercrime received" (28 August 2022) https://www.coe.int/en/web/cybercrime/-/original-instrument-confirming-nigeria-s-accession-to-the-convention-on-cybercrime-received accessed 10 January 2026
[31] United Nations Treaty Collections, "Status of Signatories as at 10.01.2026" https://treaties.un.org/Pages/ViewDetails.aspx?src=TREATY&mtdsg_no=XVIII-16&chapter=18&clang=_en accessed 10 January 2026.

2.2.3 The Nigerian Communications Act (NCA) 2003

The Nigerian Communications Act (NCA) of 2003, which governs the physical and logical infrastructure of the communications sector, is one legislation at the heart of digital rights in Nigeria.

Originally created to regulate the telecommunications sector, this Act now significantly influences how Nigerians access the internet, communicate digitally, and exercise associated freedoms. It is pivotal in determining accessibility to the digital gateway.

The NCA has been leveraged to anchor initiatives aimed at expanding broadband penetration in Nigeria. The Universal Service Provision Fund,[32] for example, supports network expansion in rural and underserved communities, growth in mobile and internet penetration, and improved affordability of basic communication services. Such initiatives directly advance access to the internet and digital technologies, and support participation in the digital economy.

The Nigerian Communications Commission (NCC) has equally operationalized consumer protection through the Consumer Code of Practice,[33] which mandates transparency and fair complaint mechanisms. This Code establishes standards to protect, inform, and empower telecom users, ensuring they can make informed decisions in the marketplace. The Commission has also established an Industry Consumer Advisory Forum (ICAF) to advise it on issues concerning the interests and concerns of consumers of ICT products and services, including older adults and persons with Special Needs.[34]

However, it is important to highlight that the NCC "dual role" makes it operate in a structurally conflicted position. While tasked with defending consumer rights and ensuring quality service, the NCC is simultaneously responsible for enforcing mandates, such as lawful interception and compulsory SIM registration.[35] This means that some of its regulatory actions—often justified for national security purposes—can unintentionally facilitate mass surveillance or result in digital exclusion, for instance, through the blocking of unlinked lines. The Commission, thus, has a daunting task to ensure a right balance is struck between digital rights and national security within its constitutional mandates.

2.2.4 The Central Bank of Nigeria (CBN) Act

While the NCC regulates the infrastructure of connectivity, the CBN regulates the value flowing through it. The CBN's mandate focuses on the financial ecosystem and it is bestowed with the authority to, among others, regulate all financial activities and transactions occurring within the digital space, including mobile money, digital payments, and fintech operations.

[32] " https://www.uspf.gov.ng/ accessed 10 January 2026.
[33] Nigerian Communications (Consumer Code of Practice) Regulations, 2024.
[34] NCC, ICAF Charter, https://consumer.ncc.gov.ng/consumer-advocacy/icaf accessed 10 January 2026.
[35] See the e-RIGHTS Digital Policy Guide.

This role makes the CBN a critical stakeholder in discussions concerning consumer protection, and digital rights, particularly regarding financial data privacy, access to digital banking, security of financial transactions and the governance of cryptocurrencies or other novel digital assets.[36]

The CBN's most profound impact on digital rights lies in its National Financial Inclusion Strategy,[37] which treats access to digital financial services as a prerequisite for modern citizenship. Through frameworks like the Guidelines for Mobile Money Services (2021) and the Agent Banking Guidelines (2025), the CBN has lowered the barrier to entry for underserved populations. And by licensing fintechs and Payment Service Banks (PSBs), it has expanded the digital economy beyond traditional brick-and-mortar banking. This transforms financial inclusion from an economic policy into an access to participate.

Unlike the general data protection framework, the financial sector operates under a stricter, sector-specific regime where consumer protection and cybersecurity are enforced via direct supervision. The Consumer Protection Framework (2016) and the Risk-Based Cybersecurity Framework (2024) mandate that financial institutions not only secure data (using standards like ISO 27001 and PCI DSS) but also provide transparent redress mechanisms. The CBN enforces a clear escalation matrix: consumers have a right to resolve disputes with their bank, and if unsatisfied, can appeal directly to the CBN. This structure arguably offers a practical enforcement mechanism of digital remedy than going through the full judicial system which is time consuming.

Despite the existing framework for consumer redress, significant operational issues within Nigeria's digital finance sector frequently leave consumers frustrated and vulnerable. These service gaps include the persistent problem of service downtimes and dispense errors, as well as opaque data-sharing practices between fintechs and third parties like loan recovery agents and loan applications.[38] The frequency of service outages for essential digital financial services, such as payment gateways and mobile banking platforms, is a major concern. These disruptions severely impede commerce and daily life, thereby eroding trust in the reliability of the digital finance infrastructure. Furthermore, the process for resolving dispense errors—particularly those involving Automated Teller Machines (ATMs) and Point-of-Sale (POS) terminals—is often cumbersome. Consumers also continue to report unethical practices from loan apps, despite recent regulatory efforts to govern their conduct. Addressing these persistent operational flaws, especially concerning service reliability and transparency, is essential to realising the promise of a secure and rights-respecting digital economy.

[36] Chioma G. Nkechika, "Digital Financial Services and Financial Inclusion in Nigeria: Milestones and New Directions" Central Bank of Nigeria Economic and Financial Review (December 2022) https://www.cbn.gov.ng/Out/2024/RSD/Digital%20Financial%20Services%20and%20Financial%20Inclusion%20in%20Nigeia,%20Milestones%20and%20New%20Direction.pdf accessed 11 January 2026.
[37] See CBN, National Financial Inclusion Strategy (Revised 2022). See also the Guidelines for Mobile Money Services in Nigeria (2021).
[38] See Lorrita Ogu et al., "Rights and challenges impacting the protective framework for financial technology consumers in Nigeria" IJEBM Vol:1, Issue:1 (2024); Blaise Udunze, "Erosion of Trust: How hidden charges, downtime erode confidence in Nigerian banks" Business247 (28 October 2025); FCCPC, "Service disruptions: FCCPC warns banks against violation of customer's rights" (29 October 2024) https://fccpc.gov.ng/service-disruption-fccpc-warns-banks-against-violation-of-customers-right/ accessed 19 January 2026.

2.2.5 Federal Competition and Consumer Protection Commission

The Federal Competition and Consumer Protection Commission (FCCPC) Act mandates the Commission to promote fair business practices and consumer interest, including ensuring that a wide variety of quality products are provided at competitive prices and adopting measures that guarantee goods and services are safe for their intended or normal use.

FCCPC mandate has evolved to include defending the citizens against predatory online practices.

The FCCPC's most significant intervention in the digital space has been its regulation of the digital lending sector, where it redefined consumer protection to include protection from privacy-based harassment. Previously, unregulated Loan Apps utilized non-consensual contact scraping to publicly shame borrowers, a practice that violated both privacy and human dignity.[39] In response, the FCCPC coordinated a Joint Regulatory and Enforcement Task Force (JRETF), an inter-agency enforcement coalition to address consumer harms related to digital money lenders.[40] It also issued the Digital, Electronic, Online, or Non-Traditional Consumer Lending Guidelines 2025 to require the compulsory registration of lending apps and explicitly prohibit the weaponisation of personal data for debt recovery. This intervention demonstrates regulatory agility by forcing app stores (Google/Apple) to delist non-compliant apps.

Beyond the money lending sector, the FCCPC functions as the arbiter of fairness by protecting consumers from manipulative interface designs and opaque digital contracts. Through its surveillance and investigation units, the Commission monitors online marketplaces to prevent misleading advertising, hidden charges, and the sale of unsafe digital goods. The FCCPC operates an online complaint handling system (including a web portal and a mobile app) which allows consumers to register complaints about digital products or services and track their complaints with a unique code.[41]

Furthermore, the FCCPC acts as a force multiplier for other regulators by integrating compliance into its registration processes. For example, it has made compliance with the Nigeria Data Protection Act a mandatory prerequisite for registration of digital lenders.[42] It requires platforms to disclose exactly how personal data is used and to obtain meaningful consent before operation. Apart from issuing fines, which it successfully did in the case of Meta,[43] the FCCPC can threaten the commercial existence of a company by blocking its market entry.

[39] FCCPC, "Digital lending: FCCPC tackles abuses, issues landmark regulations" https://fccpc.gov.ng/digital-lending-fccpc-tackles-abuses-issues-landmark-regulations/ accessed 11 January 2026.
[40] Frontier Africa Reports, "FCCPC, ICPC, EFCC, NITDA, NHRC and CBN to jointly investigate rights violations in money-lending industry" https://news.frontierafricareports.com/article/fccpc-icpc-efcc-nitda-nhrc-and-cbn-to-jointly-investigate-rights-violations-in-money-lending-industry accessed 11 January 2026.
[41] FCCPC, "Complaint handling procedure" https://fccpc.gov.ng/consumers/complaint-handling/ accessed 11 January 2026.
[42] See the Digital, Electronic, Online, or Non-Traditional Consumer Lending Guidelines 2025.
[43] ICLG, "Nigeria and Meta agree to settle USD 32.8 million data protection dispute" (7 October 2025) https://iclg.com/news/23143-nigeria-and-meta-agree-to-settle-usd-32-8-million-data-protection-dispute accessed 11 January 2026.

Despite progress, the enforcement framework faces significant institutional, operational, and systemic challenges, notably due to overlapping or even conflicting regulatory responsibilities.[44] The FCCPA includes provisions that potentially overlap with the statutory mandates of other agencies such as the Standards Organisation of Nigeria (SON) in the area of consumer protection. [45] This also includes functions of sectoral regulators that possess specialized expertise and practices, meaning this overlap could lead to administrative friction, ultimately negatively impacting both consumers and industry stakeholders.[46] These may breed conflicts that affect discharge of duties effectively.

The complexity of the digital marketplace presents a substantial challenge for regulatory bodies globally, and Nigeria's FCCPC is no exception. A critical issue is the FCCPC's apparent limitation in both resources and specialized technical expertise, which hinders its ability to effectively navigate and address the sophisticated dynamics inherent in digital markets. This resource and knowledge deficit becomes particularly pronounced when juxtaposed with well-established and highly funded international counterparts, such as the Federal Communications Commission (FCC) in the United States, which possess significant institutional depth in digital regulation. The disparity is felt when the FCCPC attempts to engage with or take regulatory action against major global technology companies ("big tech"). [47]

These multinational corporations leverage vast legal, technical, and lobbying resources, often requiring a level of digital forensics, data analysis, and regulatory sophistication that currently strains the capacity of the Nigerian regulator. This gap affects the FCCPC's effectiveness in ensuring fair competition and safeguarding consumer rights in the rapidly evolving digital economy.

2.2.6 Other Relevant Instruments

Apart from the legislation highlighted above, there are several other instruments that promote digital rights in various forms, both directly and indirectly. These include:

- **The Evidence Act 2011,** which facilitates the admissibility and presentation of digital evidence in court, directly impacting dispute resolution in cases involving digital transactions or activities.

[44] See for example, Chinonso Ekuma, "Regulatory Overlap Between the FCCPC and the NCC in Tackling Anti-competitive Practices in the Nigerian Telecommunications Sector" https://www.kennalp.com/articles/regulatory-overlap-between-the-fccpc-and-the-ncc-in-tackling-anti-competitive-practices-in-the-nigerian-telecommunications-sector accessed 19 January 2026.
[45] Kasarahchi Aniagolu, "Reform FRSC, NAFDAC, FCCPC, SON, others having overlapping mandate, CPPE tells Tinubu" The Whistler (30 June 2024) https://thewhistler.ng/reform-frsc-nafdac-fccpc-son-others-having-overlapping-mandate-cppe-tells-tinubu/ accessed 19 January 2026.
[46] Jackson, Etti and Edu, "Key Takeaways – The Changing Landscape: Federal Competition and Consumer Protection Act" (2019) https://jee.africa/insights/key-takeaways-the-changing-landscape-federal-competition-and-consumer-protection-act accessed 11 January 2026.
[47] A notable example is the dispute between the FCCPC and Meta. The regulator conducted a two-year investigation that concluded Meta was liable for multiple consumer rights breaches, resulting in a $220 million fine. In response, Meta issued a threat to withdraw its services from Nigeria. See Sarah Laniyan and Chimgozirim Nwokoma, "Meta threatened to exit Nigeria over $220m fine but two months after deadline, services are still running" (2 September 2024) https://techpoint.africa/insight/meta-and-fccpc-continue-tussle/ accessed 19 January 2026.

- **The National Information Technology Development Agency (NITDA) Act 2007** gives NITDA the mandate to regulate IT development, which often includes setting standards and guidelines relating to digital security and infrastructure, laying the groundwork for digital rights protections.

- **The Freedom of Information Act 2011** guarantees the right of access to public records, which, in the digital age, extends to electronically held information.

- **The National Health Act 2014** contains provisions regarding patient information and confidentiality, which translates into an essential protection for digital health data privacy.

- **The Nigeria Startup Act 2022** represents a pivotal legislative advancement for digital rights by directly addressing the fundamental barrier of accessibility and seeks to lower entry barriers to the digital ecosystem through substantial investment in capacity building and talent development programmes.

- **The Copyright Act 2022** modernizes copyright protection and covers enforcement of copyright in the digital environment in Nigeria. It prohibits the circumvention of technical protective measures implemented to protect copyright, as well as contains provision relating to takedown of online infringing content.

These laws have wide-ranging effects, from indirectly incorporating protections through regulatory compliance to directly governing how both private businesses and public institutions process personal data. However, one conclusion emerging from the discussions above is that Nigeria's digital rights governance features a complex, multi-sectoral landscape involving various government agencies, each operating under distinct legislation and mandates. While this framework offers potentially comprehensive coverage, it leads to a fragmentation where multiple bodies address interrelated aspects of digital rights.

A critical need, therefore, is a robust mechanism for inter-agency coordination. Without a clear, collaborative, and cohesive framework, the system faces significant risks. These include administrative conflicts, such as conflicting regulatory interpretations or enforcement actions, which generate uncertainty for citizens and digital service providers, as well as the wasteful duplication of resources.

Nevertheless, the relentless speed of digital innovation perpetually tests established human rights and legal structures, highlighting the ongoing necessity for legislative reforms and forward-looking new laws. For example, the emergence of AI technologies introduces fresh challenges to core principles like privacy, non-discrimination, fairness, and accountability. Current legislation may not adequately regulate the ethical implementation and use of AI to effectively protect digital rights. Therefore, sustained legislative effort is vital to keep abreast of developments in the digital sphere. We will now highlight several relevant bills currently before the National Assembly to determine their potential in bridging these existing gaps.

2.2.7 Bills Relevant to Digital Rights

The Nigerian National Assembly is demonstrating a growing legislative commitment to digital rights, a response to the current regulatory gap. This commitment is evidenced by the various bills under consideration, all of which aim to either directly or indirectly solidify and advance these rights, signaling a determined effort to keep pace with the rapidly evolving digital landscape.

A landmark digital rights bill was first proposed in 2019, but despite being passed by the National Assembly, it did not become law as the President withheld assent.[48] Although attempts have been made to reintroduce it, the bill has not yet been successfully enacted. Beyond this foundational effort, a variety of other subject-specific bills have been proposed, covering areas such as hate speech, the digital economy, artificial intelligence, combating internet falsehood and manipulation, among others.

Several bills currently before the National Assembly have the potential to reshape the digital rights landscape. Key among them include: the reintroduced Digital Rights and Freedoms Bill (HB 1739), which seeks to explicitly safeguard online expression, assembly, and privacy, and the Child Online Access Protection Bill (HB 244), which has passed the House, introduces a framework to protect minors from cyberbullying and online exploitation. In the realm of emerging technology, the National Artificial Intelligence Commission Bill (SB 731) aims to establish a regulatory authority for AI deployment, while the Control of Usage of Artificial Intelligence Technology in Nigeria Bill (HB 942) aims to regulate the deployment and use of AI technologies to prevent misuse and harm. [49]

However, the pace of these legislative developments does not match the rate of technical innovation, suggesting an urgent need to reduce the timeline and duration for passing these bills. There is also the need to improve the public and civil society engagement in the process of enacting these laws, the specialized knowledge required to understand their complexities. Furthermore, prioritising public access to information about the status and progress of these bills is essential. Currently, draft copies are often difficult to locate, which hinders researchers and civil society from analysing and providing informed input into the legislative process.

Due to limitations in space and time, a detailed individual analysis of these bills is not possible. Nevertheless, some of these bills need to be harmonised in terms of definitions, authorities they establish, subject matter, numbering, etc.[50] Furthermore, as these bills advance through the legislative process, it is advised that sufficient time be allocated for public commentary. Utilizing an accessible digital medium for this purpose will allow the procedure to benefit from the "knowledge of the crowd."

[48] Oyewole Oladapo and Ayo Ojebode, "Nigeria Digital Rights Landscape" (2021) https://pdfs.semanticscholar.org/12d3/0a0d33aab6a32e9331c906f9be85e0f5896a.pdf accessed 12 January 2026.
[49] A table listing pending bills is available in Appendix A.
[50] For example, the definition of an AI system differs between HB 942 and HB 1810. The regulatory authority they establish differs too irrespective of the fact that both bills address similar subject matter.

THEMATIC ANALYSIS

Evaluating the Protection, Promotion and Fulfillment of Digital Rights Across Themes

This section offers a thematic review of the current status and existing gaps of specific digital rights in Nigeria. The examination is structured around five key thematic areas.

3.1. Rights Focusing on Access and Participation in the Digital Space

Access to the internet represents the foundational layer upon which the entire structure of digital rights is built. Without meaningful connectivity and the requisite digital literacy and competence to utilize it effectively, all other rights pertinent to the digital environment remain theoretical abstractions. While Nigeria has achieved significant telecommunication penetration, access to the internet has not yet been elevated to a fundamental enforceable right.

Digital inclusion in Nigeria today is significantly affected by the cost of connection, urban-rural divide and electricity deficit.[51] High data costs remain a prohibitive barrier for low-income households.[52] A study indicates that 40% of open learners cite connectivity costs as a primary obstacle.[53] When internet access consumes a disproportionate share of daily income, the digital public square becomes an exclusive club for the urban elite. More critically, the divide is physical: recent data from the NCC reveals that while urban internet access stands at approximately 57%, rural access lags significantly at just 23%—leaving nearly 77% of the rural population effectively disconnected.[54] The concentration of digital services (e.g., e-commerce, e-health) in urban cities leaves rural populations effectively "offline," exacerbating existing inequalities.[55] Furthermore, unreliable power supply forces citizens to rely on expensive power generators, thereby increasing the cost of digital access.

[51] Benjamin OO and Foye VO, Inclusion, organisational Resilience, and Sustainable Development in Nigeria: The Role of Digital Innovations (2022) 2; Okonkwo SN, Digital Inclusion in Africa: Bridging the Divide (2025) 1; ANI JI and Batisai K, Promoting Digital Inclusion through Public-Private Partnerships for Older Adults in Nigeria: A Review (2024) 2.
[52] Njoku NA et al, Opportunities Presented by Digital Infrastructure and Internet Access for Nigeria's Economic Growth (2025) 69.
[53] ibid, 257.
[54] Juliet Umeh, "Only 23% of rural communities have internet access in Nigeria — NCC" Vanguard (22 October 2025)
[55] Benjamin OO and Foye VO, Inclusion, Organisational Resilience, and Sustainable Development in Nigeria: The Role of Digital Innovations (2022) 2.

Even where physical access exists, a profound digital literacy gap creates a second-level divide, distinguishing those who can merely consume digital content from those who can create value with it. A significant portion of the population lacks the basic skills to navigate e-governance platforms or secure their data. This deficit highlights that digital education should be formalised at all levels. While the government has launched high-profile initiatives like the 3 Million Tech Talents (3MTT) Programme[56] to train youth, older demographics and persons with disabilities remain largely excluded from these interventions. Advancing the economic utility of youth should be balanced with the digital inclusion of the elderly, disabled, and women to ensure that the digital divide does not exacerbate existing social inequalities.

Citizens' engagement through e-Governance platforms has largely focused on digitising bureaucracy (efficiency and service delivery). Less progress has been made on using digital platforms to enhance democratic participation and secure the right to public participation by digital means. This leaves citizens as passive users rather than active stakeholders.[57] While platforms like the NIMC have streamlined identity services, platforms for citizen engagement in policy-making remain nascent or non-existent. The digital space is not adequately leveraged to consult citizens on policy; instead, it is often used to announce policy. This top-down approach creates a situation where citizens perceive digital platforms merely as tools for state extraction rather than avenues for their voice to be heard. To bridge this trust gap, the State must move beyond "Service Portals" to "Deliberative Platforms" where digital policy is co-created with citizens and civil society.

For Nigeria to realise its aspiration of a digitally-enabled society and ensure all citizens can fully exercise their digital rights, it must move beyond focusing solely on high internet penetration rates. The nation needs to formally recognise and guarantee universal, affordable, quality internet access, as well as the right to digital non-exclusion. Access to the internet should be managed as an essential utility, on par with electricity to ensure that the majority of the population will benefit in the information society.

3.2. Rights Focusing on Personality, Digital Identity and Inheritance

Personality rights are a fundamental form of recognition that extends beyond simple privacy. They are essential to a citizen's intrinsic capacity to maintain control over their digital existence and identity.

This encompasses the right to resist unwarranted attempts to remove anonymity without a clear, lawful justification, and the ability to manage one's identity against any form of manipulation or unauthorised appropriation.

[56] https://3mtt.nitda.gov.ng
[57] Adediran M et al, Bridging the Digital Divide: A Business Case for Digital Inclusion in Nigeria (2025) 45.

While the enactment of the NDPA in 2023 marked a legislative milestone to a robust statutory framework on data protection, it falls short in addressing the profound new threats associated with the comprehensive digitization of the self such as digital likeness appropriation facilitated by deepfakes and synthetic data. Advances in generative AI have democratized the capacity to clone the voice, appearance, and mannerisms of any individual—living or dead—with near-perfect realism, for profit or damage to dignity, with ease and at low cost. [58]

AI cloning and deepfakes go beyond mere data theft; they are an appropriation of a person's very being. This technology seizes the fundamental, intrinsic markers of identity, such as the unique sound of a voice, subtle facial expressions, and manner of walking, and bends them to an external will. The creation of an AI-generated video showing a person uttering words they never said is a profound violation, not just of their data, but of their intrinsic dignity and integrity.

The current Nigerian digital rights landscape is inadequately equipped to tackle these sophisticated, identity-level threats. The statutory framework must evolve rapidly to establish specific and enforceable protections against the unauthorised exploitation of digital identity, voiceprints, and likeness. This necessitates an urgent legislative intervention that explicitly defines and sanctions the creation and distribution of malicious or deceptive synthetic media.

A related but equally critical area requiring legislative attention is the recognition of digital heritage within the nation's succession law framework. As lives become increasingly intertwined with digital assets—from cryptocurrencies and online accounts to intellectual property and social media presences—the question of how these elements are managed, accessed, and distributed after death remains largely unanswered in Nigerian jurisprudence.[59] Modernizing succession law to include clear provisions for digital inheritance is essential to ensure continuity of property rights and respect for the deceased's digital legacy.

[58] See Siwei Lyu, "Deepfake Leveled up in 2025 – Here's What's Coming Next" (Emmetsburg, 23 Dec. 2025), https://www.emmetsburgnews.com/premium/theconversation/stories/deepfakes-leveled-up-in-2025-heres-whats-coming-next,154987 accessed 2nd January 2026.
[59] See Chuks Okoriekwe, "Reflections: dealing with legal issues of digital afterlife" (July 2017) https://lelawlegal.com/add111pdfs/Article_34_Reflections-Dealing_with_Legal_Issues_of_Digital_Afterlife1.pdf accessed 19 January 2026; Trusted Advisors, "Securing Your Legacy: Estate Planning for Digital Assets in the Digital Age" (4 December 2023)

3.3. Rights Focusing on Expression in the Digital Space

As earlier noted, the Nigerian Constitution guarantees the right to freedom of expression. A critical facet of this right involves the liberty to seek, receive, and impart information and ideas online without fear of censorship, reprisal, or undue restrictions. This protection extends to both individual citizens and the organized press. In contemporary Nigeria, the digital space has evolved into the primary arena for political discourse and citizen journalism, making the protection of this right paramount for democratic health.

The constriction of the digital space in Nigeria has a profound and demonstrable "chilling effect" on the exercise of constitutionally guaranteed rights, particularly freedom of expression and press freedom. This manufactured climate of fear fundamentally undermines democratic discourse and fosters an environment of pervasive self-censorship. Both individual citizens and established media outlets are compelled to proactively limit the scope and critical nature of their online activity, including social media posts, investigative reports, and opinion pieces, to mitigate the risk of arbitrary and punitive State action.

A central mechanism enabling this digital repression is the deliberate weaponisation of key provisions within the Cybercrimes Act of 2015. Among these, Section 24, ostensibly designed to curb "Cyber-stalking," has been systematically repurposed. The law, which should serve as a tool for ensuring online safety and combating genuine harassment, has been routinely employed to justify the warrantless arrest, prolonged detention, and malicious prosecution of journalists, bloggers, and civil society activists.[60]

By creatively interpreting critical commentary, investigative journalism, or political dissent as "cyber-stalking" or "offensive" speech, the government effectively transforms a digital safety statute into an potent and accessible instrument of political censorship and legal harassment. This misuse erodes public trust in the rule of law and signifies a broader trend towards shrinking the civic space, both online and offline, by making the cost of exercising fundamental rights prohibitively high.

Beyond State actors, the role of intermediary service providers—the platforms through which digital freedom of expression is exercised—is equally pivotal. There are several instruments addressing the various aspects of intermediaries action, including the Copyright Act, the Cybercrime, Case law, and the NITDA Code of practice for interactive computer service Platforms/ internet intermediaries (2022). However, despite these frameworks, there is unclear rule on how these intermediaries ensure accurate information and transparency when moderating content. It is important that the framework on intermediary governance evolves to integrate human rights standards, and a balanced approach necessary to ensure that platforms are neither granted blanket immunity that permits the proliferation of harmful content nor subjected to disproportionate liability that chills legitimate innovation. Importantly, platforms must establish robust and accessible complaint mechanisms that allow citizens to seek redress and formally challenge decisions regarding the removal, restriction, or demotion of their content. Crucially, this process must be transparent, timely, and free of undue cost.

[60] See Maureen Okpe, "How Cybercrime Act is Weaponised to Intimidate Journalists, Suppress Press Freedom" Global Sentinel (15 January 2026) https://globalsentinelng.com/how-cybercrime-act-is-weaponised-to-intimidate-journalists-suppress-press-freedom/ accessed 19 January 2026.

3.4. Rights Focusing on Remedy and Due Process

Often overlooked but critically important in the digital rights space is the guarantee of access to effective justice and redress when digital rights are violated, regardless of whether the infringement is done by State actors or non-state entities.

Traditionally, access to justice is seen in light of the opportunity for an individual to bring a claim before a court and have it adjudicated based on principles of fairness, ensuring just and equitable legal outcomes. [61]

Unlike the offline world, private entities known as "online gatekeepers" hold significant power in the digital space, capable of directly affecting individual fundamental rights in ways that mirror the operations of nation-states.[62] This dynamism brings a new dimension to the nature of remedy; it shifts the locus of justice from solely public courts to private adjudication systems. While traditional due process focuses on minimizing State arbitrariness, the emerging principle of "due process online" recognises that powerful private companies make decisions regarding content moderation and account suspension that directly curtail users' rights.[63] Consequently, legal standards must evolve to govern their actions.

Digital platform policies are often designed by these gatekeepers with broad discretion, leading to opaque and inequitable practices, from business competition to content moderation, that may affect marginalised groups. Regulators are now requiring these entities to operate with transparency and accountability. For example, the EU's Digital Services Act (DSA) introduces a tiered enforcement and redress framework designed to ensure effective procedural safeguards for users affected by platform moderation decisions. After an initial platform decision, such as the removal or restriction of content, users must be provided with access to a mandatory internal complaint-handling mechanism that is accessible, reasoned, and subject to human review (Article 20 DSA). If the dispute is not resolved at this stage, users may refer the matter to an independent and certified out-of-court dispute settlement body, with which platforms are required to cooperate in good faith (Article 21 DSA). This framework operates without prejudice to the right of users to seek judicial remedies before national courts. By combining internal review procedures, independent external dispute resolution, and preserved access to courts, the DSA seeks to rebalance power asymmetries between platforms and users, reduce the risk of arbitrary or opaque moderation decisions, and enhance consistency, accountability, and due process in digital content governance.

[61] Majekodunmi et al, Issues and Challenges concerning Access to Justice in Nigeria: Clinical Legal Education Aid as a Panacea (2024).
[62] Okocha, Udoh & Harikrishnan, Social Media Regulation in Nigeria and the Implications on Digital Rights in a Democracy (2021); Adetunji & Okuonghae, Challenges of Copyright Protection in the Digital Age: The Nigerian Perspective (Library Philosophy & Practice, 2022).
[63] Ekpo, Okokon & Akpakpan, Data Protection in the Digital Age: A Comparative Analysis of Nigeria's NDPA and the EU's GDPR (ICTD Conference, 2024).

Nigeria's current digital rights landscape lacks the necessary institutionalization of key protections and administrative safeguards, which poses a significant barrier to citizens seeking redress for online harms. A crucial first step toward rectifying this deficit is the establishment of a dedicated national complaint bureau for online matters. This independent body would serve as an essential mechanism for citizens to escalate issues, particularly in instances where platform-internal remedies have proven ineffective or non-existent. Furthermore, a comprehensive legislative overhaul is imperative. This must involve either a significant reform of existing relevant laws or, more effectively, the passage of the proposed Digital Rights and Freedom of Information Bill and formalizing these protections through law, coupled with a robust administrative oversight body like the aforementioned complaint bureau.

3.5. Rights Focusing on Cybersecurity

Security and integrity in the digital realm are essential for safeguarding individuals, organisations, and the nation from cyber threats. Cybersecurity constitutes the collective tools, policies, and safeguards designed to protect computer systems from unauthorised actions that threaten the confidentiality, integrity, and availability (CIA) of such systems.

A compromised system can lead to significant financial loss, identity theft, and erosion of public trust.

Nigeria's current legal framework has not yet evolved to guarantee every citizen a "right to cybersecurity." While the Cybercrimes Act primarily focuses on criminalising unauthorised access and cyber-terrorism, it did not establish a right against cybercrime or cybersecurity. The Act also does not provide mandatory security standards for the entire supply chain. Consequently, there is a pressing need for an overarching, horizontal cybersecurity instrument that would mandate that both public and private entities maintain appropriate security measures to guarantee the integrity of their services.

Another critical aspect of the cybersecurity ecosystem that remains significantly underdeveloped in Nigeria is the cyber victim support system and post-breach remediation.[64] The current regulatory frameworks are notably deficient in adequately addressing the necessary victim compensation, psychological support, and post-breach remedies such as mandatory credit monitoring services and identity theft insurance for individuals whose data and privacy have been compromised. This absence reflects a broader oversight where the focus has historically been on punishment, rather than comprehensive victim recovery and restitution.

[64] See Lateef Adeleke and Zainab Oluwo, "The legal regime of cyberbully and victim protection in Nigeria" Fountain University Law Journal (2025) 2(4).

The immediate consequence of this systemic deficiency is that when a data breach or a significant cyber incident occurs, affected individuals are almost invariably forced to cater for these remedial costs themselves. This vacuum highlights a need for regulatory reform that shifts the responsibility for victim recovery back to the entities—whether public or private—that failed to protect the data in the first instance. A mature digital society requires not only strong data protection laws but also robust, accessible, and mandated mechanisms for recovery and compensation when those protections inevitably fail.

Protection of children from online exploitation and abuse is similarly not optimised. While statutes, such as the Child's Rights Act (CRA), the Cybercrimes Act, and the NDPA, contain provisions protecting children's dignity, they are often fragmented and insufficient for the digital age. The complexity of modern digital threats, including algorithmic grooming and exposure to harmful content, demands a dedicated legal instrument for children's online protection. Such specific legislation would place a "duty of care" on platform operators to proactively assess the risks to children, incorporating preventative safety measures into their system.

It is a welcomed development that the Child Online Access Protection Bill (HB.244) is progressing in the Parliament.[65] The bill seeks to establish a comprehensive legal framework to protect children from online threats such as cyberbullying, grooming, exploitation, and exposure to harmful or illegal content. It will also require accountability from internet service providers and digital platforms to proactively restrict or remove harmful content, enforce age-appropriate access, and promote digital literacy and safety.[66] As of December 2025, the House of Representatives has passed the bill at its third reading, marking a significant step forward. The bill now awaits consideration by the Senate before it can be signed into law by the President. Civil society organisations and child rights advocates have widely praised the bill as a critical move toward aligning Nigeria's children digital safety standards with global best practices.[67]

Beyond legislation, there is also a need for widespread education and awareness.[68] This approach requires integrating cybersecurity components into national education curricula to provide younger generations with essential digital literacy skills. Crucially, this education must extend to parents and guardians, as they play a central role in monitoring their children's online activities and fostering responsible behavior.[69] This ties into the broader necessity of promoting public awareness for society as a whole. Despite the existence of cybercrime laws, insufficient public information renders many individuals susceptible to phishing assaults and social engineering-occasioned fraud. Thus, robust public awareness campaigns are essential to instruct citizens on identifying fraud and adopting best practices, thereby creating a human firewall to complement legal and technical safeguards.

[65] Oscar Yakwen, "National Assembly Passes Historic Child Online Protection Bill (HB.244)" 4 December 2025 https://naltf.gov.ng/hb-244/ accessed 15 January 2026.
[66] Ibid.
[67] Fortune Eromonsele, "Rep passes Child Online Safety Bill to protect minors in digital space" (Premuim Times 8 December 2025) https://www.premiumtimesng.com/health/health-news/841607-rep-passes-child-online-safety-bill-to-protect-minors-in-digital-space.html accessed 15 January 2026.
[68] Iheanyi Nwankwo and Angela Uzoma - Iwuchukwu, "Policy brief: Reforming Cybersecurity Regulation in Nigeria" (July 2025).
[69] Akeusola, Social Media and the Incidence of Cyberbullying in Nigeria (2023).

EMERGING ISSUES

Artificial Intelligence, Digital Rights, and Regulatory Frontiers



AI is a rapidly advancing, multipurpose technology that offers vast benefits across sectors, including manufacturing, healthcare, education, and entertainment. However, its "dual-use" nature presents significant risks: while it is a powerful force for good, malicious actors can exploit it to cause systemic harm. Generative AI is a prime example of this paradox.

As discussed in Section 3.2 on digital identity, the widespread use of deepfakes and sophisticated synthetic media has severely complicated online verification and authenticity, creating opportunities for public deception. This was evident during Nigeria's 2023 electoral period, which saw a significant surge in deceptive content, such as false endorsements and misattributed statements. [70] The speed and ease with which this content was created and disseminated amplified its harmful potential, resulting in a volatile information environment and profoundly eroding public trust in genuine media reporting and political discourse.

Beyond disinformation, bad actors are utilizing AI to escalate cybersecurity threats and fraud. NITDA issued a public warning regarding the increasing sophistication of AI-generated job scams, which lure unsuspecting individuals with seemingly legitimate offers to extract processing fees.[71] Furthermore, AI can empower cybercriminals to overwhelm traditional defences by developing highly sophisticated attacks. AI-driven tools, for example, can craft bespoke, highly personalised phishing attacks that are far more effective than generic attempts, or create polymorphic malware that evades detection.[72] These capabilities allow attackers to identify and exploit vulnerabilities in large systems at machine speed, presenting a significant threat to individuals and institutions alike.

As the application of AI technologies matures in Nigeria, the key question is what regulatory framework will be required to prevent undue infringement on digital rights.[73] There are signs of the government reacting to the societal impacts of AI by adopting a national strategy that aims to leverage AI for development while mitigating potential risks. However, this needs to be supported by legislation and defined implementation strategy.

[70] Chiagozie Nwonwu & Fauziyya Tukur, "Nigerian elections 2023: False claims and viral videos debunked" BBC (23 February 2023) https://www.bbc.com/news/world-africa-64797274; Jochen Luckscheiter, "Bots and biases: the role of social media in Nigeria's elections" Heinrich-Böll-Stiftung, https://ng.boell.org/en/2022/10/26/bots-and-biases-role-social-media-nigerias-elections accessed 18 January 2026:
[71] Microsoft, "Three AI scams Nigerians need to watch out for in 2025" https://news.microsoft.com/source/emea/features/three-ai-scams-nigerians-need-to-watch-out-for-in-2025/#:~:text=Just%20six%20months%20ago%2C%20Nigeria's,fraudulent%20offers%20harder%20to%20detect; https://marketingedge.com.ng/stay-vigilant-as-cybercriminals-utilize-ai-in-attacks-nitda-warns-nigerians/ accessed 18 January 2026.
[72] Tope Aladenusi, "Nigeria cybersecurity outlook 2025" Deloitte https://www.deloitte.com/ng/en/services/consulting-risk/perspectives/Nigerias-cybersecurity-landscape-in-2025.html accessed 18 January 2026.
[73] See the National Artificial Intelligence Strategy (September 2025) https://ncair.nitda.gov.ng/wp-content/uploads/2025/09/National-Artificial-Intelligence-Strategy-19092025.pdf accessed 17 January 2026.

The National Assembly has introduced several legislative bills that aim, among others, to establish educational institutions to advance AI studies and implement controls for the ethical, risk-based deployment of AI technology.[74] However, the timing and pace of these legislative, and other regulatory developments are critical and needs urgent consideration given the unprecedented novelty, rapid speed, and broad societal impact of AI adoption and diffusion across various sectors in the country to prevent regulatory gaps.

Below, we consider some pivotal developments in detail, analysing their scope, effectiveness, and future implications for the digital rights landscape in Nigeria.

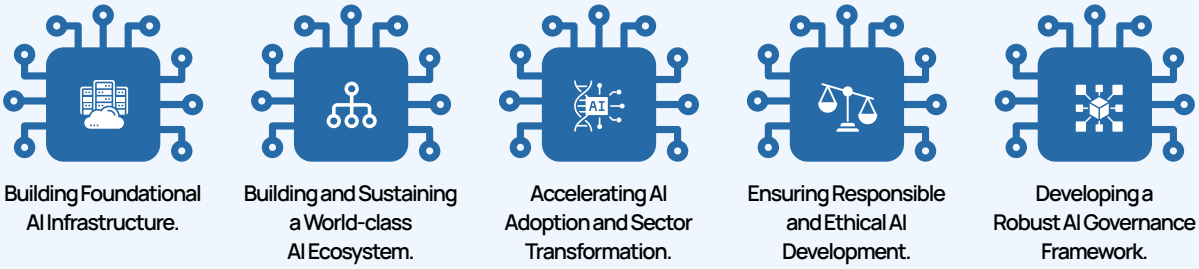
4.1. Regulatory Framework of Artificial Intelligence in Nigeria

Artificial intelligence, having been in development for over half a century, is not an entirely new concept. Consequently, its impact can be addressed in inappropriate instances using existing legal frameworks. For example, a perpetrator who uses AI to create a phishing email resulting in fraud can be prosecuted under current criminal and cybercrime laws, regardless of the AI involvement. However, the innovative capabilities of AI and its potential for broad deployment create novel scenarios that may challenge existing laws. This difficulty explains why various nations are currently developing specific AI regulations within both civil and criminal law frameworks to manage these emerging threats.

Nigeria is yet to adopt an overarching law that regulates the entire gamut of AI development and deployment like the EU's AI Act. However, the Federal Ministry of Communications, Innovation and Digital Economy (FMCIDE) is leading the way on AI policy development and innovation. The Ministry published a draft National AI Strategy in 2024, outlining a roadmap for leveraging AI for development and societal benefits while simultaneously addressing potential risks. Now released in September 2025, the National Strategy represents the most dedicated AI-focused document indicating the government's position on AI governance.[75]

[74] See Section 2 above.
[75] See the National Artificial Intelligence Strategy (September 2025) https://ncair.nitda.gov.ng/wp-content/uploads/2025/09/National-Artificial-Intelligence-Strategy-19092025.pdf accessed 17 January 2026.

The National AI Strategy articulates five key pillars that will guide government's actions to achieving the nation's AI vision:



It is important to note that the National AI Strategy is a foundational, high-level policy document. As such, it acts as a governmental blueprint, detailing strategic intent rather than providing the granular, prescriptive detail needed to fully address the nuanced human rights implications of AI or to institute immediate, definitive regulatory frameworks. Crucially, the document itself anticipates a future adoption of specific legislation. This subsequent legislation will be essential for translating the high-level policy goals into enforceable legal standards to effectively manage the complex ethical and regulatory dimensions of AI implementation.

While this future legislation is awaited, the NDPA is arguably the most relevant existing law addressing AI implications for personal data processing. This significance stems from the law's technology-neutral approach and the fact that developing and deploying most AI systems typically necessitates the processing of personal data. As such several provisions of the NDPA can impact AI system development and deployment once personal data is processed, including but not limited to:

- **Section 24** which requires data controllers and processors (e.g., AI system developers and deployers) to comply with the principles of personal data processing when building their systems.
- **Section 28** which mandates conducting a Data Protection Impact Assessment (DPIA) when a data processing operation presents a high risk to the rights and freedoms of individuals.
- **Section 37** which grants data subjects the right not to be subject to a decision based solely on automated processing (including profiling) if that decision produces legal or similarly significant effects. This provision is a crucial tool for addressing algorithmic bias, offering recourse to victims of biased AI outputs.
- **Section 30** which is triggered when sensitive personal data is processed, placing stricter rules around consent or legal authorisation.

A fortiori, all the rights granted to the data subjects by NDPA, such as the right to be informed, the right to object, the right to rectification, the right to erasure, among others, inherently apply to personal data processing, regardless of the technology employed.

So far, the integration of AI into the operational frameworks of Nigerian government agencies is gaining considerable momentum, signaling a proactive approach to addressing entrenched national challenges using AI. A notable example is the CBN, which is actively exploring and encouraging the deployment of AI technologies to address challenges such as Anti-Money Laundering (AML) and combating the Financing of Terrorism (CFT), given AI's superior capability in processing vast amounts of data and identifying suspicious patterns.[76] This governmental encouragement of AI usage underscores a growing understanding of its potential as a strategic national asset for security and economic stability.

In sum, Nigeria is currently in the early stages of establishing a comprehensive regulatory framework for Artificial Intelligence. However, as previously mentioned, the National Assembly is actively working on several AI-related bills, including those with implications for human rights. The following section will examine how other jurisdictions are approaching AI regulation.

4.2 Emerging Global Approaches in Regulating AI: Moving from Reactive to Proactive Regulation

Given the global nature and often unprecedented effects of AI on human rights, it is crucial to examine international trends to inform Nigeria's approach to AI regulation. Worldwide, various strategies are being adopted to manage the complex and evolving implications of AI technologies. These global approaches include:

Extending Existing Laws

This approach involves the judiciary actively interpreting current legislation and constitutional provisions and extending their application to new situations and challenges presented by AI.[77] This heavily relies on the flexibility and progressive nature of the judicial system.

Amending Existing Laws

This entails making specific, targeted changes or updates to existing statutes to explicitly incorporate digital rights protections, address new harms occasioned by AI, or clarify the application of established legal principles in this context.[78] This is often a quicker route than crafting entirely new legislation but may be limited to the scope of the original law.

[76] CBN, "Baseline standards for automated anti-money laundering (AMLI) solutions" (May 2025) https://www.cbn.gov.ng/Out/2025/CCD/Exposure%20Draft%20on%20Baseline%20Standards%20for%20Automated%20AML%20Solutions.pdf accessed 17 January 2026.

[77] In Moffatt v. Air Canada (2024 BCCRT 149), British Columbia Civil Resolution Tribunal found that Air Canada's online AI chatbot provided incorrect information to a passenger about the airline's bereavement fare policy. However, since the representation had a legal effect, the airline could not escape liability for it. This underscores that companies cannot treat automated agents as separate from their legal obligations when those agents interact with consumers in a commercial context

Crafting New Laws

This involves the development and enactment of entirely new, comprehensive legislation specifically designed to regulate the development and deployment of AI technologies.[79]

Using Administrative Guidelines and Directives

Government agencies, regulatory bodies, and specialized commissions often issue administrative guidelines, regulations, standards, or codes of conduct regarding the development and deployment of AI.[80] These non-legislative instruments provide practical instructions, offer speed and technical specificity in areas requiring rapid response or specialized expertise.

Promoting Self-Regulation and Co-Regulation

This involves encouraging private sector actors, particularly technology companies, to develop and enforce their own ethical guidelines, content policies, and transparency mechanisms (self-regulation), sometimes in collaboration with government oversight (co-regulation).[81] This can leverage industry knowledge but requires robust accountability measures.

These approaches are not mutually exclusive, they have been combined in several jurisdictions to achieve the desired aims. Currently, Nigeria's regulatory approach is more visible within the administrative approach. As AI applications are being integrated across sectors of the nation's economy and public life, it becomes more imperative to have a clear, ethical, and regulatory framework backed by legislation.
While these legislative efforts are ongoing, it is suggested that they be based on defined principles, strategic and be proactive focused. A well-defined strategy must address key pillars, including:

Ethics and Governance

Establishing clear ethical guidelines to ensure AI systems are fair, transparent, accountable, and non-discriminatory, particularly in relation to digital rights.

Infrastructure and Capacity Building

Investing in the necessary digital infrastructure (e.g., high-speed internet, data centres) and developing a skilled local workforce capable of creating, deploying, and maintaining AI technologies.

Regulation

Adopting flexible regulatory regime that encourages innovation while protecting citizens' rights and preventing misuse of AI.

Data Policy

Developing robust national data policies that govern the collection, storage, and utilization of data with a strong emphasis on sovereignty and privacy.

[78] Denmark offers a relevant model through its amended Copyright Law, which addresses the exploitation and digital appropriation of likeness via generative AI. Under the proposed amendments, each person would effectively have copyright-style control over their own body, facial features, voice and likeness, allowing them to demand takedowns of AI-generated content that depicts them without consent and to seek legal remedies, while still permitting exceptions for parody and satire. See Miranda Bryant, "Denmark to tackle deepfakes by giving people copyright to their own features" The Guardian (27 June 2025) https://www.theguardian.com/technology/2025/jun/27/deepfakes-denmark-copyright-law-artificial-intelligence accessed 19 January 2026.
[80] See for example, the EU's Ethics Guidelines for Trustworthy Artificial Intelligence, https://digital-strategy.ec.europa.eu/en/library/ethics-guidelines-trustworthy-ai accessed 20 January 2026.
[81] See for example, Industry-Led AI Ethics Codes such as Google AI Principles, https://ai.google/principles/ accessed 20 January 2026.

International collaboration and lessons are essential to strengthening the framework for digital rights in Nigeria, particularly given the transnational nature of the digital space and the shared challenges faced by nations globally. By engaging with international bodies, civil society organisations, and foreign governments, Nigeria can access best practices, technical assistance, and support crucial for developing a robust and rights-respecting AI regulatory framework.

KEY FINDINGS AND RECOMMENDATIONS

Charting the Path Forward: A Multi-Stakeholder Agenda

Nigeria's digital rights landscape is at a critical turning point, as revealed by the analysis in this report and the findings of the e-RIGHTS Project. While the country has established the pillars of a digital society, particularly regarding personal data processing, significant structural gaps remain. The 'dual-use' paradox continues to threaten civic space, and the legal framework struggles to keep pace with the velocity of technological innovation.

5.1. Key Findings

01 The Pace of Legislative Interventions

Nigeria has made considerable strides in developing legislative instruments that affect digital rights, including the Cybercrimes Act, the NDPA, the Startup Act, and a range of complementary regulatory frameworks. Collectively, these instruments reflect a deliberate effort by the government to establish a foundational legal architecture for Nigeria's digital space. However, this progress has not kept pace with the rapid and accelerating evolution of technology, nor with the emergence of new and complex threats arising from both public and private actors operating online.[82] The tempo of legislative intervention remains misaligned with the urgency required to effectively govern these changes.

This gap is illustrated by the slow amendment cycle of key legislation. For example, it took nine years for the Cybercrimes Act to undergo its first amendment. Despite this extended interval, the amendment did not adequately address several novel categories of cybercrime and digitally enabled harms that had emerged and proliferated since the Act's original enactment.[83] As a result, significant regulatory blind spots persist, limiting the law's effectiveness in responding to contemporary digital risks.

Looking ahead, the trajectory of technological development suggests that new tensions and unprecedented legal complexities will continue to surface.

[82] See the e-Rights Digital Policy Guide.
[83] Examples of cybercrimes not covered in the Act include but not limited to: AI-powered and synthetic content crimes, Blockchain and decentralized finance crimes, data encryption/hostage-taking and cyber extortion model crimes, etc.

Existing laws are likely to face increasing strain as they are applied to scenarios for which they were not originally designed, often leaving affected individuals without clear or effective legal remedies. A salient example is the growing use of Generative AI for malicious or criminal purposes, including the unauthorised appropriation and manipulation of individuals' digital likenesses through deepfakes. The speed and adequacy of legislative responses to such high-impact, rapidly evolving threats remain uncertain.

Notwithstanding these challenges, there are emerging signs of a potential shift toward a more responsive legislative posture. The recent amendment of the NDPA, undertaken just two years after its initial adoption, represents a notable departure from earlier patterns of prolonged legislative inertia. This comparatively expedited reform process suggests that a more adaptive and time-sensitive approach to digital rights legislation may be feasible, offering a pathway to avoid the extended delays that have historically characterized reform in this area.

In parallel, a review of the current parliamentary docket reveals a growing risk of duplication and overlap among bills addressing similar subject matter and policy objectives.[84] Strategic consolidation of related bills into fewer, more comprehensive legislative instruments could streamline parliamentary deliberation, reduce fragmentation, and shorten the time required for enactment and implementation. Such procedural refinement would constitute a practical step toward closing existing legal gaps more efficiently.

Given the inherent and temporary vacuums created by the lag between technological innovation and legislative response, the burden of interpreting and applying existing principles to novel situations falls heavily upon the judiciary. In the absence of clear and up-to-date statutory guidance, courts are required to apply existing legal principles to novel digital contexts, often through precedent-setting test cases that gradually shape the contours of digital rights jurisprudence.[85] The development of digital rights law in Nigeria therefore reflects an ongoing and dynamic interplay between incremental legislative reform and judicial interpretation, with the latter frequently acting as a stopgap mechanism in periods of regulatory uncertainty.

02

The Use of New Media and Public Perception

The migration of human interaction and communication into the digital realm has fundamentally reshaped public discourse. While new media platforms have significantly expanded opportunities for free expression and civic engagement, they have also blurred long-standing boundaries around ethical journalism, accountability, and responsibility. This tension lies at the heart of global digital rights debates, which grapple with how to preserve open, democratic online spaces while addressing the substantial harms that can arise in largely unregulated environments. Such harms include the rapid spread of misinformation and disinformation, the incitement of violence, and the exploitation of digital platforms by extremist groups for recruitment, coordination, and propaganda.

[84] See Table 1 in Section 2 above
[85] An example is the recent Falana v Meta where the public debate has been whether the NDPA covers platform liability for infringing material published by third parties.

Within Nigeria, governmental responses to these challenges have been met with sustained criticism from CSOs. Many CSOs contend that regulatory interventions have tended to prioritise control over online expression rather than the promotion of responsible digital conduct. Legislative initiatives such as the proposed Hate Speech Bill (2019) and the Social Media Bill (2019), among others, have been widely interpreted as efforts to expand state authority over online discourse, with the potential to suppress dissent and limit legitimate public scrutiny of government actions.

These concerns are reinforced by the practical application of existing laws, particularly the Cybercrimes Act. Although the Act was enacted with legitimate objectives: combating cyberbullying, financial fraud, and other cyber-enabled crimes, it has increasingly been perceived as a tool for constraining digital expression.[86] Its routine invocation by state actors in cases involving journalists, activists, and online commentators has deepened public skepticism regarding the government's commitment to protecting digital rights. Collectively, these trends contribute to a growing sense of a shrinking civic space, raising broader questions about the resilience of democratic participation and public trust in Nigeria's evolving digital environment.[87]

From a policy perspective, this dynamic has significant implications. The growing mistrust surrounding digital regulation risks undermining public confidence in lawmaking institutions. For legislators and regulators, the finding underscores the need for public engagement and institution of clear safeguards against abuse, and transparent enforcement mechanisms that distinguish between harmful online conduct and protected expression. Without such recalibration, regulatory efforts aimed at addressing online harms may continue to be perceived as threats to democratic participation rather than as legitimate tools for promoting a safe, inclusive, and rights-respecting digital public sphere.

03

Public Engagement and Multistakeholders Participation in Digital Governance

Nigeria's digital governance framework remains predominantly characterized by a top-down policy and implementation model, with limited institutionalized avenues for meaningful public, civil society, and private-sector engagement. As a result, the country has yet to fully harness the benefits of an inclusive, collaborative digital governance ecosystem grounded in co-creation. The absence of structured multistakeholder participation constrains the ability to draw on civil society expertise, private-sector innovation, and citizen input in the design, implementation, and oversight of digital governance policies and systems.

Although Nigeria has made notable progress in deploying digital platforms across multiple tiers of government, the underlying design logic of these systems prioritises administrative efficiency and service delivery over democratic engagement. Existing e-governance platforms are largely configured as government-to-citizen (G2C) service channels, facilitating access to information and public services, but offering limited functionality for public consultation, participatory policymaking, or collaborative problem-solving.

[86] See documented cases in https://closingspaces.org
[87] Ibid.

This structural orientation has important implications for the role of citizens within the digital governance architecture. Rather than being recognised as active stakeholders in the digital transformation process, citizens are primarily positioned as end-users—recipients of services or applicants within automated systems. Such an approach narrows opportunities for public input, weakens mechanisms for accountability, and limits the capacity of civil society and other non-state actors to contribute diverse perspectives, technical expertise, and rights-based analysis. It risks entrenching a form of digital governance that is insufficiently democratic.

Deliberate bottom-up approach to embed participation, transparency, and co-creation into digital governance frameworks in Nigeria is necessary not only for its potential to strengthen democratic accountability and public trust, but also to enable meaningful stakeholder engagement, and reposition citizens as partners—rather than passive beneficiaries—in the governance of Nigeria's digital future.

04

The "Rights-Resource " Tension in Nigeria's Digital Landscape

The effective realisation of digital rights in Nigeria is shaped not only by legal and regulatory considerations, but also by underlying economic and infrastructural constraints. Digital inclusion challenges extend beyond basic connectivity to encompass broader utility concerns, particularly the availability, reliability, and affordability of supporting physical infrastructure. Addressing these challenges requires sustained investment in robust, accessible, and affordable foundational systems.

At present, internet access is not treated as an essential public utility on par with water or electricity. This policy posture has significant implications, as the reliability of electricity supply directly affects both the cost and availability of digital access. In large parts of the country, inconsistent power supply compels individuals, businesses, and internet service providers to depend heavily on backup energy sources to remain connected. This reliance substantially increases the cost of providing and accessing internet services.

Higher operational costs for service providers are passed on to consumers, producing an inflated "power-plus-data" cost structure that functions as a powerful economic filter. For a significant proportion of the population, particularly those in rural communities, these combined costs sharply limit sustained and meaningful participation in the digital economy. This structural reality highlights a need for substantial, front-loaded public investment in nationwide fibre-optic networks, satellite and alternative broadband solutions, last-mile connectivity for underserved areas, and, critically, large-scale upgrades to the national power grid.

This finding aligns Nigeria's experience with broader international debates on whether internet access should be treated as an essential public utility. In several jurisdictions, access to affordable and reliable internet is increasingly framed as a prerequisite for the enjoyment of economic, social, and political rights, and is integrated into universal service obligations, national infrastructure plans, and public investment strategies. Countries that have adopted this approach have typically paired rights-based commitments with sustained State-led investment in broadband infrastructure and energy reliability, often complemented by public–private partnerships.

For Nigeria, the implication is clear: digital rights aspirations must be deliberately synchronised with infrastructure, energy, and fiscal policy planning. Without such alignment, efforts to recognise or expand digital rights, particularly the right to internet access, risk remaining largely aspirational. Bridging the rights–resource gap therefore requires coordinated, cross-sector action that treats connectivity as critical national infrastructure, ensuring that legal commitments are matched by the material conditions necessary for their effective and equitable realisation.

5.2. Key Recommendations

The Legislature

Adopt Value-Guided and Strategic Legislative Architecture

The legislature occupies a central role in advancing and safeguarding digital rights in Nigeria. To discharge this responsibility effectively, digital legislation should be grounded in a value-guided, strategic, and principles-based architecture. Such an approach would provide a coherent normative framework to guide policymaking and regulatory action across all arms of government, reducing fragmentation and inconsistency.

Nigeria can draw instructive lessons from international models such as the EU's Declaration on Digital Rights and Principles, which is explicitly anchored in fundamental human rights and organized around a clear set of eight core principles. Within the Nigerian context, the Digital Rights and Freedoms Bill offers a viable foundation for embedding shared values into the country's digital governance framework. Positioned as a foundational statute, the Bill can serve as a reference point for future legislation, regulation, and enforcement in the digital environment.

Adopt a More Proactive and Coordinated Legislative Approach

Given the speed and complexity of technological change, a shift from reactive to anticipatory lawmaking is essential. Digital rights are no longer governed by isolated statutes but by an interconnected regulatory ecosystem involving multiple institutions and oversight bodies. Legislative interventions should therefore explicitly promote inter-agency coordination, clarify institutional mandates, and reduce regulatory overlap.

To ensure continued relevance, digital legislation should incorporate mandatory periodic review clauses. These provisions should assign responsibility to designated regulatory authorities to conduct impact assessments, publish public reports, and recommend legislative or regulatory adjustments in response to emerging risks and technological developments. In addition, all future technology-related bills should be systematically assessed for their potential human rights impacts, helping to prevent unintended infringements and ensuring alignment with constitutional and international obligations.

Leverage Research and Expertise to Keep Pace with Change

To strengthen evidence-based lawmaking, the National Assembly should institutionalize the use of expert research, foresight studies, and policy analysis on digital rights and emerging technologies. Targeted parliamentary studies, such as evaluations of the effectiveness of existing digital rights-related laws, can help identify gaps, unintended consequences, and areas requiring reform.

In this regard, the establishment of a Nigerian Observatory on Digital Rights (NODR), in partnership with civil society and academic institutions, would provide a dedicated platform for sustained monitoring and analysis. The Observatory could track legislation, policies, regulatory practices, and judicial decisions; maintain a centralized repository of resources; and publish periodic and annual reports on the state of digital rights in Nigeria to inform legislative oversight and public debate.

Prioritise Key Digital Rights Legislation

Legislation with direct and significant implications for digital rights should be prioritised for harmonization, sequencing, and expedited passage. This includes foundational instruments such as the Digital Rights and Freedoms Bill, as well as sector-specific legislation such as the Children Online Safety Bill, the Cybersecurity Bill, and proposed laws addressing accountability in the development and deployment of emerging technologies, including artificial intelligence systems.

By clearly identifying and sequencing priority digital rights legislation, the legislature can create a more predictable and stable legal environment—one that protects fundamental rights while simultaneously supporting responsible innovation, investment, and trust in Nigeria's digital ecosystem.

The Executive and Regulatory Agencies

Strengthen Inter-Agency Coordination and Close Enforcement Gaps

The Executive arm must move beyond ad-hoc committees to address the persistent coordination deficits within Nigeria's digital governance ecosystem. Rather than loose working groups, the Presidency should mandate the execution of a binding Memorandum of Understanding (MoU) between key regulators such as the NDPC, NCC, FCCPC, CBN, among others.

This MoU should clearly delineate jurisdictional boundaries to prevent regulatory overlap (e.g., between consumer protection and data privacy) and establish a unified protocol for joint enforcement actions. By institutionalizing this collaboration through a binding framework, the Executive can close the regulatory blind spots that currently undermine the effective protection of digital rights.

Ensure Consistent and Impartial Enforcement Across Public and Private Sectors

Regulatory enforcement relating to digital rights, particularly in areas such as privacy, data protection, and consumer protection, must apply equally to private actors and public institutions. Where violations implicate fundamental rights, enforcement actions should be firm, transparent, and impartial, regardless of the identity of the offending party.

In particular, breaches involving government agencies or public-sector data processing require heightened accountability. Sanctions for unlawful data collection, processing, or disclosure by public institutions should be public, proportionate, and effectively enforced. Such an approach is essential to ending perceptions of impunity, strengthening regulatory credibility, and rebuilding public trust in State institutions responsible for digital governance.

Prevent Misuse of Cybercrime Laws Against Journalists and Civic Actors

To curb the misapplication of cybercrime legislation, the Federal Ministry of Justice should issue clear and binding prosecutorial guidelines on the interpretation and enforcement of the Cybercrimes Act. These guidelines should explicitly reaffirm constitutional guarantees of freedom of expression, press freedom, and due process, and clarify that cybercrime enforcement must not be used as a mechanism for harassment, intimidation, or repression of journalists, activists, or other civic actors.

The issuance of prosecutorial guidance should be complemented by regular, mandatory training for law enforcement officers and prosecutors on digital rights, constitutional protections, and applicable human rights standards. Together, these measures would help reorient cybercrime enforcement toward its legitimate objectives—protecting individuals and systems from harm—while safeguarding Nigeria's democratic space and civic freedoms.

The Judiciary

Build Judicial Capacity for Digital Rights Adjudication

As the final arbiter of rights and constitutional interpretation, the Judiciary occupies a central position in bridging the gap between analog legal frameworks and rapidly evolving digital realities. In the presence of legislative lag and emerging technological harms, judicial interpretation increasingly shapes the practical content and enforcement of digital rights in Nigeria.

To discharge this responsibility effectively, sustained and institutionalized capacity development for judicial officers is essential. The National Judicial Institute (NJI) should develop, formalize, and regularly update a specialized curriculum on digital technologies and digital rights. This curriculum should combine foundational technical literacy with deeper engagement on non-technical dimensions, including human rights standards and proportionality in remedies in the digital environment.

Regular training and continuous professional development in these areas would strengthen judicial reasoning, enhance consistency in decision-making, and improve the quality of remedies available to rights holders. From a policy perspective, such investment in judicial capacity is critical to ensuring that courts remain responsive to contemporary digital rights challenges and are equipped to provide effective oversight of both State and private actors in the evolving digital ecosystem.

Civil Society and Media

Strengthen Public Resilience Through Digital Literacy and Strategic Litigation

CSOs and the media play a critical role in strengthening societal resilience within Nigeria's digital ecosystem. As digital risks become more complex and pervasive, these actors are central to building a societal "human firewall" capable of withstanding disinformation, digital manipulation, and rights abuses. To this end, CSOs should scale up advanced digital literacy and civic education initiatives that go beyond basic technical skills and focus on cultivating critical digital citizenship.

Such programmes should equip individuals to identify and respond to emerging threats such as misinformation, disinformation, and deepfakes; understand their rights relating to data protection, privacy, and freedom of expression; and adopt sound cybersecurity practices. Media institutions have a complementary responsibility to support these efforts through responsible reporting and public-interest journalism that demystifies digital technologies, explains regulatory developments, and foregrounds rights-based implications for citizens.

In parallel, civil society should continue to deploy strategic litigation as a core accountability mechanism in the digital space. By deliberately testing laws, policies, and enforcement practices before the courts, CSOs can contribute to clarifying the scope and limits of state authority and private-sector obligations in relation to digital rights. Strategic cases serve not only to redress individual harms but also to shape jurisprudence and guide future policy and regulatory action. Landmark decisions, such as SERAP v. Federal Government of Nigeria,[88] demonstrates the potential of public-interest litigation to establish judicial precedents that strengthen the protection and enforcement of digital rights.

[88] See ECW/CCJ/APP/09/19 and ECW/CCJ/APP/03/2025.

Private Sector

Embed Human Rights, Transparency, and Accountability in Platform Design and Operations

Private sector actors, particularly technology companies and digital platforms that increasingly function as gatekeepers of the digital public sphere, play a decisive role in shaping how rights are exercised online. As such, they bear a responsibility to integrate human rights considerations into both system architecture and business operations. Technology companies operating in Nigeria, including startups and established platforms, should adopt a "rights by design" approach that embeds privacy, data protection, safety, and security safeguards at the earliest stages of product development, rather than treating these obligations as retrospective compliance requirements.

Beyond system design, platforms should strengthen and localize grievance redress mechanisms to ensure users have access to clear, accessible, and timely avenues for remedy. Effective mechanisms should allow users to appeal content moderation decisions, account suspensions, and data-related complaints without being compelled to resort to litigation. To be credible and trusted, such processes must be transparent, culturally and linguistically appropriate, and aligned with international human rights standards, including the provision of clear explanations, predictable timelines, and independent review where appropriate.

Private sector actors also have a responsibility to address disinformation and harmful online content in ways that are proportionate and respectful of freedom of expression. Platforms should pursue collaborative approaches that involve independent fact-checkers, civil society organisations, academic institutions, and local experts to identify and respond to misinformation, hate speech, and coordinated manipulation. Content moderation policies, algorithms, and automated systems should be context-sensitive, transparent, and subject to regular audits to ensure they do not disproportionately suppress legitimate political speech or marginalise vulnerable communities.

Conclusion

Nigeria is at a pivotal stage in its digital development. As this report highlights, the nation has evolved from merely consuming technology to becoming an increasingly influential and active centre for digital innovation. However, this advancement has created a persistent "dual-use" paradox: the very digital infrastructure that promotes economic opportunity, civic participation, and innovation is simultaneously being co-opted for human rights abuses, including surveillance and censorship.

The findings of the e-RIGHTS project underscore that, while Nigeria's foundational legal architecture continues to expand, it is constrained by a pronounced legislative lag. The pace and scale of technological change now consistently outstrip the ability of existing laws and institutions to provide effective protection for citizens' digital rights. This mismatch creates systemic vulnerability, leaving individuals to confront digital-era harms with legal safeguards designed for an analog world—effectively relying on "analog shields against digital swords."

At the same time, the promise of digital rights remains largely theoretical for a significant portion of the population that are not yet connected. Significant disparities in access—particularly between urban and rural communities—expose a fundamental "rights–resource" tension. A digital society cannot be meaningfully democratic if the "new public square" is accessible only to a section of the populace—the connected urban elites. Bridging this divide requires a deliberate policy shift: the State should recognise affordable and reliable internet access not as a discretionary service or luxury, but as essential public infrastructure underpinning the enjoyment of fundamental rights.

Addressing these intersecting challenges demands more than incremental legislative reform. It requires a fundamental reorientation of digital governance—from reactive responses to technological harms after they occur, toward proactive, rights-respecting frameworks capable of anticipating and shaping the deployment of emerging technologies. Such an approach must integrate lawmaking, regulation, infrastructure investment, and capacity-building into a coherent strategy.

Ultimately, the success of Nigeria's digital transformation should not be measured solely by innovation metrics or economic growth, but by the safety, dignity, and freedom experienced by Nigerians in the digital sphere. By implementing the recommendations outlined in this report, Nigeria has an opportunity to chart a digital future that is not only technologically advanced, but also just, inclusive, and secure.

Appendix A

List of Bills Related to Digital Rights in Nigeria[89]

Bill Name	Objectives of the Bill	Status
National Digital Economy and E-Governance Bill, 2025 (SB 498)	To establish a comprehensive legal framework for Nigeria's digital economy and e-governance, including recognition of electronic transactions, digital signatures, public sector digital transformation, data governance, cybersecurity, and emerging technologies (including AI).	Passed Second Reading (Senate); at Committee Stag
Digital Economy Mainstreaming Bill, 2025 (HB 2538)	To integrate digital technologies across key sectors of the Nigerian economy and promote the adoption of digital tools for productivity, innovation, and inclusion.	First Reading (House)
Digital Rights and Freedoms Bill 2024 (Reintroduced) (HB 1739)	Strengthens protections for online freedoms and privacy. Safeguard online expression, communications, and assembly; provide legal redress for digital rights violations	Awaiting 2nd Reading
Blockchain Technology Bill, 2025 (HB 2539)	To provide a regulatory framework for blockchain technologies, distributed ledger systems, and related digital infrastructure in Nigeria.	First Reading (House)
Digital Health Services Bill 2025 (HB 2198)	To regulate the provision of digital health services, including standards for digital platforms, protection of patient data, interoperability, and security of health information systems.	Committee Stage
Hate Speech Bill 2019 (HB 246)	To promote national cohesion and integration by outlawing unfair discrimination and hate speeches.	No public record available beyond first reading
Protection from Internet Falsehoods and Manipulations and Other Related Matters Bill 2019 (SB 132)	To regulate the transmission of false or manipulative information online and proposes penalties and enforcement mechanisms to address such speech.	Committee Stage

[89] The information presented is based on publicly available data at the time of this report and should not be considered exhaustive. It is possible that some relevant bills were not included due to data inaccessibility.

Appendix A

List of Bills Related to Digital Rights in Nigeria

Bill Name	Objectives of the Bill	Status
Bill to Amend the Nigeria Data Protection Act, 2023 (Social Media Platforms & Digital Service Providers) (SB 650)	To require certain social media platforms and digital service providers to establish physical offices or verifiable presence in Nigeria, to enhance regulatory oversight, data accountability, and enforcement.	Passed Second Reading; referred to Committee on ICT/Cybersecurity
Digital Television Services (Pay-Per-View) Subscription Bill, 2023 (HB 981)	Introduce and regulate a pay-per-view subscription model for digital television services; ensure transparent, consumer-centric billing.	Awaiting Second Reading
Chartered Institute of Digital Forensics of Nigeria (Establishment) Bill 2023 (HB140 / HB1491)	Establishes a statutory professional body regulating digital forensics practice, professionalizes digital forensics, regulates standards, accreditation of labs, enhance digital evidence handling.	Passed by the house
Chartered Institute of Digital and Educational Technology (Establishment) Bill 2023 (HB 2365)	Establishes an institute to regulate digital education and technology professionals. Standardise and regulate digital technology education; professional capacity building.	Awaiting 2nd Reading
Nigeria Digital Literacy Management Office Establishment Bill 2023 (HB 1251)	Establishes national office to coordinate digital literacy initiatives, Promote digital literacy across Nigeria; coordinate training and outreach; enhance access to digital skills.	Awaiting 2nd Reading
Nigerian Digital Sovereignty and Fair Data Compensation Bill 2025 (SB722)	Creates framework for data sovereignty and compensation for data use, Protect individual data rights; promote fair compensation for personal data use; define data ownership principles.	Awaiting 2nd Reading
Child Online Access Protection Bill, 2023 (HB 244)	Establish a comprehensive legal framework to protect children from online harms, including cyberbullying, online exploitation, exposure to illegal or harmful content; impose obligations on technology platforms for content moderation, safety-by-design measures, and sanctions for non-compliance.	Passed by the House, awaits Senate.
National Artificial Intelligence Commission (Establishment) Bill, 2025 (SB 731)	Establish a national regulatory authority to oversee, coordinate, and set standards for the development and use of artificial intelligence in Nigeria.	Awaiting Second Reading

Appendix A

List of Bills Related to Digital Rights in Nigeria

Bill Name	Objectives of the Bill	Status
National Institute of Artificial Intelligence and Robotic Studies (Establishment) Bill, 2025 (HB 2243)	Promote research, training, and capacity development in artificial intelligence and robotics.	Awaiting Second Reading
Establishment of the Artificial Intelligence Management and Finance Institute (AIMFIN) as a Professional Body 2025 (HB 2063)	Regulate and professionalise AI management and finance practices through ethical and professional standards.	Awaiting Second Reading
Control of Usage of Artificial Intelligence Technology in Nigeria Bill, 2023 (HB 942)	Regulate the deployment and use of AI technologies to prevent misuse and harm.	Awaiting Second Reading
National Artificial Intelligence and Robotic Sciences (Establishment) Bill, 2023 (HB 601)	Establish an institutional framework for AI and robotic sciences regulation and development.	Awaiting Second Reading
Federal Artificial Intelligence Institute (Establishment) Bill, 2023 (HB 377)	Create a federal institute to support AI research, innovation, and skills development.	Awaiting Committee Report
National Institute for Artificial Intelligence and Robotic Studies, Somolu, Lagos State (Establishment) Bill 2023 (HB 143)	Establish a specialised AI and robotics institute with regional focus.	Awaiting Second Reading
Artificial Intelligence Academy Omuo-Ekiti, Ekiti State (Establishment) Bill, 2025 (SB 763)	To create a specialised centre in Omuo-Ekiti focused on artificial intelligence (AI), innovation, and related technologies.	Awaiting Committee Report
National Artificial Intelligence Regulatory Authority Bill, 2024 (HB 1810)	To establish a statutory framework for the governance, oversight, and ethical deployment of artificial intelligence in Nigeria.	Second Reading

Funded by the European Union

IN PARTNERSHIP WITH

The e-RIGHTS is funded by the European Union, and implemented by Avocats Sans Frontières France in Nigeria, in partnership with Spaces for Change (S4C), and the Centre for Information Technology and Development (CITAD).

The contents of this publication are the sole responsibility of ASF France, and do not necessarily reflect the views of the donor.