e-RIGHTS

Enhancing Digital Rights in Nigeria

Digital Rights Reform Policy Guide

Co-funded by the European Union

CFLI/FCIL
Canada Fund for Local Initiatives
Fonds canadien d'initiatives locales

AVOCATS SANS FRONTIÈRES FRANCE

CITAD
CENTRE FOR INFORMATION TECHNOLOGY AND DEVELOPMENT

SPACES FOR CHANGE | S4C

Enhancing Digital Rights in Nigeria (e-RIGHTS) Project

The Enhancing Digital Rights in Nigeria Project, formally known as the e-RIGHTS project, is a project being implemented by Avocats Sans Frontières France in Nigeria, with support from the European Union in Nigeria.

The e-RIGHTS project is aimed at promoting the rights of Nigerians in the digital sphere, harnessing opportunities and addressing challenges provided by new technologies. The project will respond directly to the needs of Nigerian youths, activists, journalists, online news platforms, bloggers, social media influencers, human rights defenders, and active citizens to have access to a free and open internet

The e-RIGHTS project is implemented in partnership with Spaces for Change and Center for Information Technology and Development (CITAD).

e-RIGHTS
Enhancing Digital Rights in Nigeria

Objectives

01 Provide a safe online platform for human rights defenders, to report and monitor issues of digital rights breaches including data privacy breaches, cyber threats, internet shutdown and threat to the social media space and to ensure prompt response to cases reported.

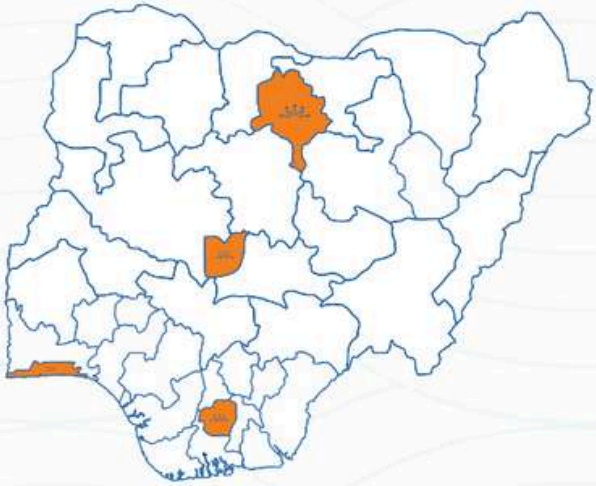
02 Establish a situation room of CSOs, lawyers, academics, tech platform providers and government partners for effective collaboration and coordination of digital rights issues.
Technical members of the situation room will also review and develop a policy guide for data rights and digital rights protection in Nigeria.

03 Work with its network of digital rights lawyers, to intervene in identifying cases of digital rights violations.

04 Build the capacity of CSOs, lawyers, journalists, activists and human rights defenders on digital rights and data security.

Implementation Areas

The action will take place in four (4) implementation areas including; the Federal Capital Territory - Abuja, Lagos State, Kano State and Imo State.



FCT
Lagos
Kano
Imo

Target Groups & Beneficiaries

- Students
- Lawyers & Judges
- Activists
- Private Sector
- e-RIGHTS
- Government Agencies
- Victims of Digital Threats
- Social Media Influencers
- Nigerian Internet users

Project Activities

- Capacity Building
- Technology Development
- Advocacy & Engagements
- Legal Assistance
- Raising Awareness

Target Outcomes

01 Human rights defenders recognize and are able to deal with the digital threats they face

02 An enabling environment for the enjoyment of digital rights is established in Nigeria

TABLE OF CONTENTS

LIST OF ACRONYMS

- ACHPR - African Charter on Human and Peoples' Rights
- AML - Anti-Money Laundering
- AI - Artificial Intelligence
- AR - Augmented reality
- CBDC - Central Bank Digital Currency
- CBN - Central Bank of Nigeria
- CFRN - Constitution of the Federal Republic of Nigeria
- CFT - Countering the Financing of Terrorism
- CFTC - Commodity Futures Trading Commission
- CSA - Cloud Security Alliance
- DeFi - Decentralized Finance
- DISPs - Digital Investments Service Providers
- DLT - Distributed Ledger Technology
- DRRPG - Digital Rights Reform Policy Guide
- ECHR - European Convention on Human Rights
- ECOWAS - Economic Community of West African states
- ER - Extended reality
- e-Rights - Enhancing Digital Rights in Nigeria
- EU - European Union
- FATF - Financial Action Task Force
- FinCEN - Financial Crimes Enforcement Network
- FTTx - Fiber to the Home

- GAID - General Application and Implementation Directive
- GDPR - General Data Protection Regulation
- ICCPR - International Covenant on Civil and Political Rights
- IoT - Internet of Things
- IRS - Internal Revenue Service
- ITU - International Telecommunication Union
- KYC - Know Your Customer
- MiCA - Markets in Crypto-Assets Regulation
- ML - Machine Learning
- NAIRA - National Artificial Intelligence Regulatory Authority
- NCA - Nigerian Communications Act
- NCAIR - National Centre for Artificial Intelligence and Robotics
- NCC - Nigerian Communications Commission
- NCPS - National Cybersecurity Policy and Strategy
- NDPA - Nigeria Data Protection Act
- NESREA - National Environmental Standards and Regulations Enforcement Agency
- NGO - Non-governmental Organization
- NITDA - National Information Technology Development Agency
- OSINT - Open-Source Intelligence
- PBOC - People's Bank of China
- SEC - Securities and Exchange Commission
- UDHR - Universal Declaration of Human Rights
- USPF - Universal Service Provision Fund
- VASPs - Virtual Assets Service Providers
- VR - Virtual reality

PREFACE

The unprecedented expansion of digital technologies has reshaped societies, economies, and individual lives, making digital rights a cornerstone of modern democracies. In Nigeria, where internet penetration has reached 45%, digital spaces have become integral to civic participation and democratic discourse. However, the rise of these platforms has equally brought new challenges, such as cyberbullying, misinformation, privacy violations, and state surveillance. These issues bring to the fore the urgent need for a balanced approach to digital governance—one that protects fundamental human rights while promoting technological innovation and addressing the complexities of emerging threats.

It is not in doubt that Nigeria has made considerable strides with legislative instruments like the Cybercrimes (Prohibition, Prevention, Etc.) Act 2015, the Nigerian Data Protection Act 2023, National Artificial Intelligence Strategy, National Blockchain Adoption Strategy and a host of other frameworks. Yet, these frameworks remain insufficient to address the evolving challenges of the digital age, particularly in protecting the rights of citizens from the overreach of state and corporate actors. Instances such as the profiling of #EndSARS, #EndBadGovernance protesters and the controversial Twitter ban highlight the fragility of digital rights in the face of political and institutional pressures. These events call for more rights-centric frameworks that safeguard citizens' freedoms and ensure accountability in the use of digital technologies.

This Digital Rights Reform Policy Guide (DRRPG) represents a critical intervention in this landscape. Commissioned by the Enhancing Digital Rights in Nigeria (e-RIGHTS) project, supported by the European Union, the DRRPG offers a roadmap for the development and strengthening of Nigeria's digital rights frameworks. It draws on lessons from global best practices, while contextualizing them for Nigeria's unique social, political, and technological environment. This guide goes beyond identifying gaps; it provides actionable recommendations across critical areas such as artificial intelligence, blockchain, data privacy, cybersecurity, telecommunications, and media freedom.

I am deeply aware of the tensions between innovation and regulation, particularly in countries like Nigeria, where the potential for technological advancement coexists with governance

challenges. The DRRPG reflects a commitment to bridging this divide, emphasizing a regulatory ecosystem that is inclusive, transparent, and aligned with international human rights standards. The DRRPG's emphasis on emerging technologies is particularly commendable. As innovations like artificial intelligence, blockchain, and the Internet of Things redefine the possibilities of digital ecosystems, Nigeria has an opportunity to position itself as a leader in responsible technology governance. However, this requires forward-thinking policies that address the ethical, social, and economic implications of these technologies.

Ultimately, the Digital Rights Reform Policy Guide is a call to action. It invites Nigerian policymakers, stakeholders, and citizens to envision a digital future that prioritizes inclusion, safeguards freedoms, and promotes equitable development. Implementing the recommendations outlined in this guide will definitely place Nigeria on a better pedestal to strengthen its digital rights frameworks, build public trust, and ensure that technological progress supports, rather than undermines, the fundamental rights of its people.

Victoria Ibezim-Ohaeri
Executive Director
Spaces for Change | S4C

EXECUTIVE SUMMARY

The rapid global evolution of digital rights has brought both unprecedented opportunities and challenges to the forefront of regulatory governance, especially in technologically advancing nations like Nigeria. With 103 million internet users and a 45% internet penetration rate, digital spaces in Nigeria have become hubs for information exchange and civic participation. However, these technological landscapes have also exposed vulnerabilities, creating a need for regulatory frameworks that balance innovation with the protection of fundamental human rights. While a plethora of regulatory efforts have been achieved in Nigeria so far, gaps persist in curbing the misuse of digital technologies by state and non-state actors, particularly in contexts of political dissent and activism.

The Enhancing Digital Rights in Nigeria (e-RIGHTS) project, supported by the European Union, responds to this pressing need through the development of the Digital Rights Reform Policy Guide (DRRPG). The guide seeks to serve as a model for strengthening Nigeria's digital rights framework. Drawing on lessons from global best practices, particularly from the European Union, the DRRPG builds on existing Nigerian legislation and policy frameworks while addressing gaps in areas such as artificial intelligence, blockchain technology, data privacy, cybersecurity, and new media. It also proposes actionable policy recommendations. The guide envisions a regulatory environment that ensures accountability, safeguards civic freedoms, and aligns technological advancements with the fundamental rights of citizens.

To chart a sustainable path forward, the DRRPG proposes a horizontal regulatory ecosystem, consistent with global best practice adopted by progressive jurisdictions, to oversee the complexities of emerging technologies like artificial intelligence, blockchain, IoT, and cloud computing. The key advantage of this approach is that it allows multiple agencies to work

collaboratively to promote responsible technology development and deployment while addressing dynamic issues associated with emerging technologies, such as data breaches, user safety, consumer protection, and compliance. Furthermore, the cross-border nature of digital technologies necessitates international cooperation to harmonize regulations and prevent regulatory arbitrage. A horizontal regulatory model is well suited to overcome these jurisdictional challenges and build a comprehensive framework that protects digital rights in an increasingly interconnected world.

1

INTRODUCTION

1 Digital rights are an extension of human rights in the digital age. Dheere (2017) described them as human rights as they are invoked in digitally networked spaces. They encompass the fundamental rights and freedoms that individuals are entitled to, both online and offline. Apart from the inherent nature of digital rights, the relationship between human rights and digital rights can be understood in several ways: digital rights conceptually extend the protection of human rights to new areas that emerged with the rise of technology.

1.1 The global evolution of digital rights has become a crucial fundamental discourse as the world embraces an increasingly interconnected and technology-driven era.[1] The statement bears stack relevance to the state of internet connectivity in Nigeria where internet users and social media users stand at 103.0 million users and 36.75 million users respectively, with 45% internet penetration.[2] These digital spaces and tools, once lauded for democratizing access to information and amplifying voices, have also exposed vulnerabilities in safeguarding individual freedoms.

1.2 As societies strive to protect rights like freedom of expression, privacy, assembly and access to information, the concept of "safe spaces" online is continually redefined[3] - reflecting a tension between enabling open digital platforms and mitigating harms

[1] *Quimbre F and Stockwell S. (2021) "The Implications for Human Rights in the Digital Age" Accessed 12/12/2024*
[2] *Kemp S. (2024) DataReportal – Digital 2024: Nigeria. Accessed 20/11/2024*
[3] *Tamakloe D. et al (2021) "Transitioning from Face-Face to Online Learning: Creating Safe Spaces for Academic Advisement in the Face of a Global Pandemic" Journal of Learning Spaces Volume 10, Number 3. Accessed 12/12/2024*

such as misinformation, cyberbullying, and digital surveillance with the "agreed minimum" of ensuring that technological innovation supports, rather than erodes, fundamental human rights.[4] The crux of digital technology regulatory efforts then lies at the intersection between protecting human rights and addressing power asymmetries, particularly those perpetuated by state actors and tech platforms, to ensure these online spaces do not become tools for victimization or marginalization of critical voices and communities.[5]

1.3 Nigerian regulatory efforts to strike this delicate balance have resulted in landmark legislation and policies. For instance, the Cybercrimes (Prohibition, Prevention, Etc.) Act 2015 aims to promote "cybersecurity and the protection of computer systems and networks, electronic communications, data and computer programs, intellectual property and privacy rights".[6] In 2023, the Nigerian Data Protection Act was enacted into law. Among other innovations, it aims to safeguard the fundamental rights and freedoms of data subjects, as guaranteed under the CFRN, 1999, and provide safe processing of personal data in the country. However, the law, like many other regulatory attempts, admits to some gaps in its ability to protect active citizens against the excesses of state actors, particularly in instances where digital rights intersect with political dissent or civic activism.

1.4 According to a report by Spaces for Change|S4C, the Nigerian government's humongous investment in the acquisition of surveillance technologies like the Elbit Systems' Open Source Intelligence (OSINT) solution and Circles have enhanced its

[4] United Nations Human Right Council Resolution 47/23 - https://documents.un.org/doc/undoc/gen/g21/192/18/pdf/g2119218.pdf Accessed 9/12/2024
[5] UN Global Digital Compact Rev. 1 (2024) https://www.un.org/techenvoy/sites/www.un.org.techenvoy/files/Global_Digital_Compact_Rev_1.pdf
[6] S. 1(c) Cybercrimes (Prohibition, Prevention, Etc.) Act 2015

capacity to spy on private communications of citizens and opposing voices.[7] The infamous ban on Twitter, and the indiscriminate profiling of Nigerian youths who participated in the nationwide #EndSARS protest against police brutality in 2020 and the #EndBadGovernance protests of 2024[8] are instances that often come to the fore when misuse of regulatory and policing powers in the digital spaces are in discuss.

1.5 Nonetheless, these recent advancements in digital technology, coupled with citizens' evolving experiences, present policymakers with a unique opportunity to craft policies that more effectively safeguard citizens' rights and protect the country's national interest. Achieving this demands visionary leadership, clear lines of accountability, appropriate systems, and consistent and fair application of rules.[9] Existing related frameworks are fraught with inconsistencies, lacking unified thrust and dated. The way forward requires more inclusive, rights-centric regulatory frameworks that guarantee safe and equitable digital spaces.

1.6 It is on this premise that the Enhancing Digital Rights in Nigeria (e-RIGHTS) project[10] supported by the European Union has commissioned the development of this Digital Rights Reform Policy Guide (DRRPG) to serve as a model for the Nigerian government to adopt for the development/strengthening of digital rights frameworks in the country. The DRRPG specifically address issues ranging from data protection, freedom of expression, and online privacy, to surveillance, among others.

---

[7] Spaces for Change (2024) The Proliferation of Dual-Use Surveillance Technologies in Nigeria: Deployment, Risks & Accountability. Accessed 11/11/2024

[8] *Closing Spaces Database (2024) - https://closingspaces.org/ Accessed 11/11/2024*

[9] *DRAFT DIGITAL GOVERNMENT POLICY FRAMEWORK, retrieved from https://www.dpsa.gov.za/dpsa2g/documents/egov/2024/ accessed on November 15, 2024*

[10] *The e-RIGHTS project is aimed at promoting the rights of Nigerians in the digital sphere, harnessing opportunities and addressing challenges provided by new technologies - https://www.avocatssansfrontieres-france.org/en/missions/e-rights/*

1.7 Drawing lessons from good practices implemented in the European Union and other jurisdictions, DRRPG builds on existing Nigerian legislations, strategies and policy directives on digital rights across various cluster issues, namely: (1) artificial intelligence, (2) blockchain technology and finance, (3) data privacy and cybersecurity, (4) new media and freedom of expression, (5) telecommunications, and (6) new and emerging technologies - revealing the existing gaps and providing policy recommendations that not only fill in these gaps but provide for other novel areas of digital technology that intersects with digital rights.

2

ARTIFICIAL INTELLIGENCE

2.1 The foundational years of Artificial Intelligence (AI) saw limited regulatory oversight, as the technology was largely in its infancy and confined to research labs.[11] Early discussions focused on theoretical frameworks, such as Isaac Asimov's "Three Laws of Robotics,"[12] which proposed ethical guidelines for robots. In the 2000s, as AI began to find practical applications (e.g., in search engines, recommendation systems), concerns emerged about privacy, data security, and algorithmic bias. However, regulation remained minimal and largely reactive.[13]

2.2 As AI development continues to evolve technologically, AI regulation has been approached with mixed feelings. High-profile incidents of AI bias, such as discriminatory hiring algorithms[14] and errors in facial recognition,[15] have ignited debates about the ethical implications of AI systems. These biases, often rooted in the data used to train AI models, emphasis the societal risks of perpetuating inequities through automated decision-making. AI's opacity compounds these challenges, raising concerns about accountability and fairness in its application. The need for

[11] *Nilsson, N.J. (2013) "The Quest for Artificial Intelligence" Cambridge University Press – Accessed 9/12/2024*
[12] *https://en.wikipedia.org/wiki/Three_Laws_of_Robotics#cite_note-IROBOT-1*
[13] *Nilsson op cite*
[14] *In 2018, Amazon abandoned an AI-based recruitment system that was found to discriminate against women. The system had been trained on ten years of hiring data, predominantly from men, and developed biases against resumes mentioning terms like "women" or activities at all-women colleges*
[15] *Briggs, C. and Briggs, R. (2024) "10 Case Studies in AI: Bias in Facial Recognition, Hiring, and Advertising," MIT Press, pp.173-191.*

explainable and unbiased AI has become a central theme in regulatory and ethical discussions.[16]

2.3 Additionally, the massive data requirements of AI systems have intensified scrutiny over data privacy, intellectual property ownership, and consent. Landmark regulations, like the EU's General Data Protection Regulation (GDPR), try to address some of these concerns to safeguard individuals' privacy rights. Military applications of AI, such as autonomous weapons and dual-use technologies, have further complicated the ethical landscape, prompting global calls for restrictions to prevent misuse by state and non-state actors.[17] These concerns reflect the urgent need for robust frameworks to address the multifaceted risks posed by AI while harnessing its potential responsibly.

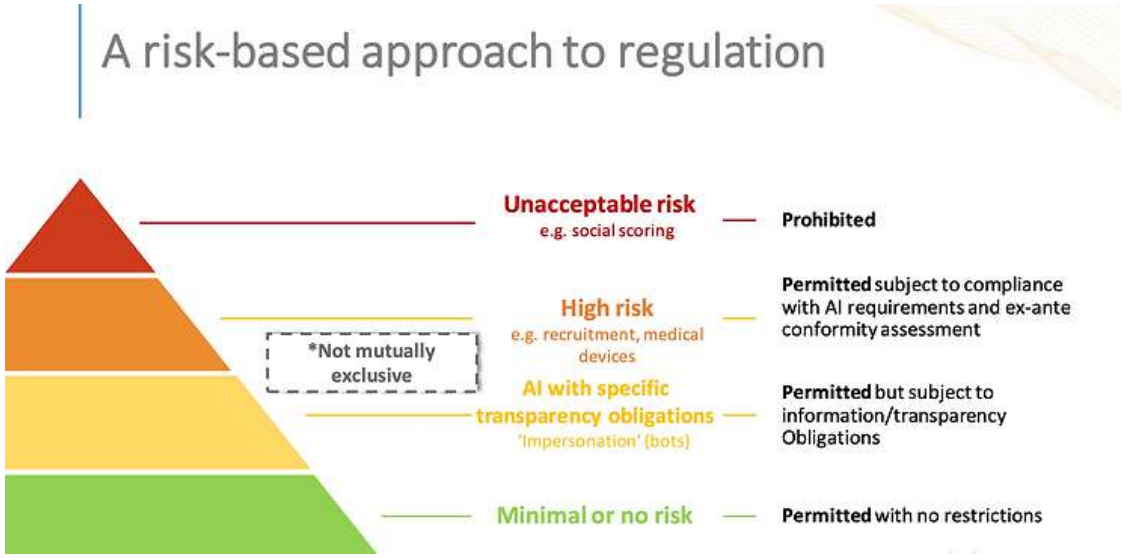
2.4 The European Union's AI Act 2024 stands out as a comprehensive framework designed to regulate AI systems based on their risk levels, with the goal of ensuring safety, transparency, and accountability.[18] The Act adopts a risk-based approach and categorizes AI applications into four tiers: ***unacceptable risk*** (banned uses like social scoring by governments), ***high risk*** (strictly regulated areas such as biometric identification and critical infrastructure), ***limited risk*** (requiring transparency measures, like disclosing AI use in chatbots), and ***minimal risk*** (subject to few restrictions).[19] The act mandates robust data governance, human oversight, and risk management for high-risk systems, while promoting innovation by exempting low-risk AI.[20] It also

---

[16] Pazzanese, C. (2020) "Ethical concerns mount as AI takes bigger decision-making role in more industries" The Harvard Gazzet. Accessed 10/12/2024

[17] Marwala, T. (2023) "Militarization of AI Has Severe Implications for Global Security and Warfare" – United Nations Univesity. Accessed 12/12/2024
[18] European Commission (2024) "AI Act Enters into Force". Accessed 12/12/2024
[19] Lawson, A. (2022) "The EU AI Act Explained: Tracking Developments for Responsible AI". Responsible Artificial Intelligence Institute. Accessed 12/12/2024
[20] ibid

establishes penalties for non-compliance and introduces a harmonized approach across EU member states, aiming to balance AI's potential with public safety and fundamental rights.[21]



Source: https://www.responsible.ai/the-eu-ai-act-explained-tracking-developments-for-responsible-ai/

2.5 In early 2019, the Council of Europe published a study entitled "Discrimination, Artificial Intelligence and Algorithmic Decision-Making."[22] The study proposed that "public and private organizations should be allowed to base decisions with far-reaching consequences for individuals on AI. In the public sector, AI should be permitted for use in rendering services like predictive policing or in decisions on the payment of pensions, housing benefits or unemployment benefits. In the private sector, its uses should extend to job recruiting. Banks should be permitted to use it to decide whether to grant credit to a consumer and to set the corresponding interest rate. These positions, however, did not entirely receive acceptance from the

[21] *ibid*
[22] *Borgesius, F. Z. (2019) Discrimination, Artificial Intelligence and Algorithmic Decision-Making – Council of Europe. Accessed 10/12/2024*

subsequent EU AI Act 2024. **What the EU AI Act 2024 Actually Allowed (Risk-Based Approach)[23]:**

The AI Act takes a *very* different approach. It categorizes AI systems based on risk, and the higher the risk, the stricter the regulations. Many of the applications suggested by the Council of Europe study would be considered "high-risk" under the AI Act and thus face significant restrictions or outright prohibitions.

- **Prohibited AI Practices:** The AI Act *prohibits* certain AI uses considered unacceptable, regardless of risk assessment. These include:
    - Real-time biometric identification in public spaces (with limited exceptions for law enforcement).
    - Manipulation of human behavior through subliminal techniques or exploitation of vulnerabilities.
    - Social scoring systems.
    - AI used to exploit the vulnerabilities of specific groups (e.g., children).

- **High-Risk AI Systems (Strict Regulations):** Many of the applications the Council of Europe study mentioned fall into this category. High-risk AI systems are subject to strict requirements, including:
    - Conformity assessments (demonstrating compliance with requirements).

[23] *https://digital-strategy.ec.europa.eu/en/policies/regulatory-framework-ai#:~:text=To%20ensure%20safe%20and%20trustworthy,transparency%20and%20copyright%2Drelated%20rules. Accessed 10/12/2024*

- Data governance and quality requirements.
- Technical documentation.
- Human oversight.
- Transparency and explainability (to a degree).
- Accuracy, robustness, and cybersecurity requirements.

- **Examples of High-Risk AI under the AI Act (and how they relate to the Council of Europe Study's suggestions):**
  - **Predictive Policing:** Highly regulated. While not outright banned, the AI Act places heavy scrutiny on its use due to the potential for bias and discrimination.
  - **Employment/Recruitment:** Also high-risk. AI used in hiring must be transparent and non-discriminatory. The Council of Europe's suggestion of *unrestricted* use is far from what the AI Act allows.
  - **Credit Scoring:** High-risk. The AI Act mandates safeguards to prevent discriminatory outcomes in lending. Again, the Council of Europe's suggestion of allowing banks free rein is not in line with the AI Act.
  - **AI for Essential Public Services (Benefits, etc.):** High-risk. These systems must adhere to strict requirements to protect fundamental rights and prevent discriminatory outcomes.

2.6 In the United States, AI regulation has been sector-specific and fragmented, with growing efforts like the ***Blueprint for an AI Bill of Rights*** and various federal agency initiatives signaling a shift toward more cohesive oversight.[24] In contrast, China adopts a dual approach that encourages rapid AI innovation while imposing stringent controls, particularly over AI-generated content and its alignment with "Socialist Core Values", while avoiding content that could subvert state authority.[25] Meanwhile, African countries are crafting AI frameworks that prioritize fairness, inclusivity, and local relevance,[26] often drawing inspiration from international guidelines like UNESCO's Recommendation on the Ethics of Artificial Intelligence.[27]

2.7 Recently, the African Union Executive Council endorsed the Continental AI Strategy during its 45th Ordinary Session in Accra, Ghana, on July 18-19, 2024.[28] The strategy document accentuates Africa's commitment to "an Africa-centric, development-focused approach to AI, promoting ethical, responsible, and equitable practices". [29] It calls for unified national approaches among African Union (AU) Member states to navigate the complexities of AI-driven change to strengthen regional and global cooperation and position Africa as a leader in inclusive and responsible AI development.[30]

2.8 Incidentally, Nigeria launched her AI Strategy in August 2024 (one month after the AU Strategy adoption), guided by principles that prioritize responsible and ethical

---

[24] *Fazlioglu, M. (2023) US Federal AI Governance: Laws, Policies and Strategies – Resource Centre. Accessed 12/12/2024*
[25] *Sheehan, M. (2023) China's AI Regulations and How They Get Made – Carnegie Endowment for International Peace. Accessed 10/12/2024*
[26] *Ogenga, F & Stanley, A. (2023) Regulating Artificial Intelligence in Africa: Strategies and Insights from Kenya, Ghana, and the African Union – Wilson Centre. Accessed 12/12/2024*
[27] *UNESCO (2021) Recommendation on the Ethics of Artificial Intelligence. Accessed 9/12/2024*
[28] *African Union (2024) Continental Artificial Intelligence Strategy. Accessed 9/12/2024*
[29] *ibid*
[30] *ibid*

conduct, inclusivity, and shared prosperity to ensure broad societal benefits.[31] The strategy emphasizes innovation and adaptation while promoting cooperation and partnerships among stakeholders for cohesive development. It adopts a human-centric approach, with specific focus on risk management and building resilience, to address challenges effectively. Additionally, it emphasizes the importance of data ethics and individual agency, which would ensure that AI systems respect privacy.[32]

2.9 The Strategy document is built on five key pillars aimed at advancing the nation's AI development and adoption while protecting the rights of regular citizens in the machine learning process. These pillars include:[33]

i. Building Foundational AI Infrastructure
ii. Building and Sustaining a World-class AI Ecosystem
iii. Accelerating AI Adoption and Sector Transformation
iv. Ensuring Responsible and Ethical AI Development
v. Developing a Robust AI Governance Framework

2.10 Pursuant to the ideals outlined in the National AI Strategy, a bill for an "Act to ensure Proper Control of Usage of Artificial Intelligence Technology in Nigeria and for Related Matters"[34] was introduced in the National Assembly to establish a legal framework for the development, deployment, and ethical use of AI technologies within the country.[35] At the core of the proposed legislation was the creation of the National Artificial Intelligence Regulatory Authority (NAIRA), tasked with overseeing the development

[31] *NITDA (2024) National Artificial Intelligence Strategy. Accessed 7/12/2024*
[32] *Article 1.2.2. ibid*
[33] *Article 1.4.1. ibid*
[34] *National Assembly (2024) Order Paper Wednesday, 27th November, 2024 - House of Representatives: Federal Republic of Nigeria*
[35] *ibid*

and implementation of AI systems in Nigeria.[36] The authority was to focus on ensuring that AI related technologies adhere to ethical guidelines, promote public safety, and protect citizens' rights and freedoms.

2.11 However, on 26 November 2024, the House of Representatives stepped down the proposed legislation.[37] Lawmakers observed that there are currently three bills related to AI under consideration by the legislative body and consequently resolved to step down the instant bill to allow for the consolidation of the three other bills.[38] This decision leaves Nigeria without a codified legal framework specifically for AI, with laws on the subject found across legal frameworks that bother on data privacy, intellectual property, cybercrime, consumer protection, and capital markets.[39]

2.12 In relation to digital rights, existing legal frameworks are found in the following:

1. **Nigeria Data Protection Act (NDPA) 2023 –** As the primary legislation on data protection in Nigeria, the Act restricts the exclusive use of automated decision-making processes for processing and profiling personal data that results in legal or similar effects on the data subject.
2. **General Application and Implementation Directive (GAID) 2024 –** Issued by the Nigeria Data Protection Commission (NDPC) to guide the implementation of the NDPA, the GAID specifically provides that, in regulating AI, controllers or processors should take into account the rights of data subjects not to be subjected to a decision based on automated processes as they put in place the technical and organizational parameters for their AI deployment in data processing. In doing so,

[36] *ibid*
[37] *Omolaoye, S. (2024) Reps Step Down Bill on Artificial Intelligence Regulation – The Guardian. Accessed 9/12/2024*
[38] *ibid*
[39] *Ibid*

they are also required to take into account the right to be forgotten, regulations on cross-border data transfers, safeguards for processing sensitive personal data, privacy by design, and safeguards for child rights and other vulnerable groups. In summary, the GAID requires controllers or processors to also take into consideration the provisions of the NDPA, the GAID itself, public policy, and other regulatory instruments issued by the NDPC.

3. **Cybercrimes Act 2015 –** The act provides that anyone who, without authorization, intentionally accesses, in whole or in part, a computer system or network for fraudulent purposes and obtains data that are vital to national security, commits an offence and is liable to punishments.[40] The provision aims to curb AI-powered system cyberattacks, which have been witnessed in some jurisdictions globally.

2.14 Existing gaps

1. Existing legislation focuses more on data privacy and protection, but that is only one part of artificial intelligence. Other aspects like algorithm biases, machine learning processes, misinformation and disinformation, among others, are areas in need of human rights-based legislation.

2. Age requirements for access to AI platforms is an essential provision that is missing among the legal frameworks for AI in Nigeria. The case of the Late Sewell Setzer, a 14-year-old who committed suicide after he was obsessed with AI[41] emphasizes the need for such measures.

[40] *Section 6 (1) Cybercrime Act of 2015,*
[41] *CNN Business (2024) This Mom Believes Character.Ai Is Responsible For Her Son's Suicide. Accessed 11/11/2024*

3. With cases of misinformation and disinformation, there are concerns over the proportionate application of laws that counter these while ensuring that digital rights are not eroded in the interest of 'national security'.

2.15 Policy Recommendations

1. AI systems should be transparent in design, implementation, and decision-making. Developers and institutions must establish accountability mechanisms to address AI-related concerns.[42]
2. AI development must comply with Nigeria's human rights and data protection standards, such as the NDPA 2023, ensuring citizens' personal information remains secure and private.
3. AI policy and regulatory framework should adopt a human rights approach. Such an approach should emphasize the protection of fundamental human rights in AI design, development and application. There should deliberate attempts to limit AI deployment in areas that may pose unacceptable risks to human rights, such as in surveillance and predictive policing, unless strict safeguards are in place.The legal framework around AI should require AI system developers and deployers to ensure that their systems are developed and deployed without bias, ensuring fair treatment across demographics. Algorithms and AI models should be evaluated and tested against unintended discriminatory outcomes, and should be monitored throughout the AI system lifecycle. .[43]

[42] *https://www.lumenova.ai/blog/ai-risk-management-importance-of-transparency-and-accountability/#:~:text=Developers%20and%20users%20of%20AI,ethical%20AI%20development%20and%20use.*
[43] *https://www.sciencedirect.com/science/article/pii/S2468227624002266*

4. AI applications, especially in sensitive areas like healthcare, finance, and law enforcement, must be rigorously tested for reliability, accuracy, and resilience against cyber threats.[44]

2.16 **Implementation Strategies**

1. Develop a comprehensive AI legal framework to guide AI researchers, developers, and users in ethical AI practices like the European Union Artificial Intelligence Act 2024, covering issues like consent, transparency, fairness, and accountability.
2. Establish a dedicated AI regulatory body, or strengthen the capacity of the National Information Technology Development Agency (NITDA) to lead AI regulation, initiatives and enforcement.
3. Form a national AI council consisting of government, academic, industry, and civil society representatives to oversee AI policy implementation.
4. Establish a National AI Fund to finance AI projects that align with Nigeria's development goals, especially in priority sectors like agriculture, healthcare, education, and governance.
5. Partners with progressive nations and institutions, particularly the European Union, to establish regional AI standards and share resources for AI development and regulation while leveraging their resources and best practices in AI governance.

[44] *Ibid*

3

BLOCKCHAIN TECHNOLOGY AND FINANCE

3.1 Blockchain is a distributed ledger technology (DLT) that creates secure, transparent, and immutable records of transactions. Its decentralized nature has revolutionized traditional financial systems by facilitating innovations such as cryptocurrencies (e.g., Bitcoin, Ethereum), decentralized finance (DeFi), and digital assets.[45] This technology basically ensures that transactions are publicly recorded on a ledger for the purpose of transparency and accountability.

3.2 A key advantage of the technology is its security, which is built with cryptographic techniques that protect data from fraud and tampering.[46] Blockchain also eliminates the need for intermediaries, such as banks or payment processors, thereby reducing transaction costs and speeding up processes.[47] These features has come to make blockchain technology a transformative force in most sectors, including the financial sector where it is driving more efficient and secure transactions with an unprecedented rate of adoption that is almost outpacing the development of regulatory frameworks for many governments and financial authorities worldwide.[48]

3.4 In the early stages, the lack of clear regulations led to the rise of unregulated platforms, which contributed to high levels of financial risk, fraud, and market instability. This

[45] *Tapscott, D. and Tapscott, A. (2016) Blockchain Revolution: How the Technology behind Bitcoin Is Changing Money, Business, and the World. Penguin, New York.*
[46] *ibid*
[47] *Mougayar, W. (2016). The Business Blockchain: Promise, Practice, and Application of the Next Internet Technology.*
[48] *O'Neill, A. (2023) Digital Assets: Will Technological And Regulatory Developments Unleash Institutional Blockchain Adoption? – S&P Global. Accessed 12/12/2024*

environment allowed for the proliferation of swindles, volatility, and illegal activities that raised concerns about the protection of investors and the broader financial system.[49] As cryptocurrencies and blockchain-based technologies gained mainstream attention, regulators began to take action, seeking to strike a balance between innovation and ensuring consumer protection. Efforts so far have focused on establishing clearer guidelines for anti-money laundering (AML), taxation, and investor safeguards while also integrating these new technologies into existing financial laws.[50] The challenge remains to create a regulatory framework that does not stifle innovation but still ensures market stability, security, and compliance with international standards.

3.5 Major regulatory approaches to blockchain and cryptocurrency have emerged through the efforts of the Financial Action Task Force (FATF) - an international standard setting body against AML and counter-terrorism financing (CTF). Recommendation 15 of its 40 Standards is specifically tailored to virtual assets and its service providers.[51] The FATF guideline aim to ensure that cryptocurrency platforms adhere to the same financial regulations as traditional financial institutions, which includes implementing Know Your Customer (KYC) procedures, monitoring transactions for suspicious activity, and reporting illegal practices[52] with the aim of mitigating the risks of cryptocurrencies being used for illicit activities, such as money laundering or funding terrorism.

3.6 In national contexts, the European Union's Markets in Crypto-Assets Regulation (MiCA) seeks to establish a unified regulatory framework for crypto assets across all member

---

[49] *Pazzanese, C. (2021) Regulators Put Cryptocurrency in Crosshairs – The Harvard Gazette. Accessed 12/12/2024*

[50] *ibid*

[51] *FATF's Recommendation 15 and its Interpretative Note 15 was updated in 2019 to apply AML/CFT measures to VA and VASPs - https://www.fatf-gafi.org/en/publications/Fatfrecommendations/targeted-update-virtual-assets-vasps-2024.html*

[52] *FATF Interpretative Note 15*

states.[53] The goal of the framework is to provide legal clarity and ensure the stability of the cryptocurrency market by setting consistent rules for the issuance, trading, and storage of digital assets.[54] MiCA covers various types of crypto assets, including stablecoins and utility tokens, and introduces measures for investor protection, market integrity, and financial stability. Provisions of the Regulation also cover AML and consumer rights issues, requiring mandatory crypto service provider's registration.

3.7 In the United States, the regulation of cryptocurrencies is fragmented among different agencies based on the nature of the assets. The Securities and Exchange Commission (SEC) regulates cryptocurrencies that are classified as securities, with compliance emphasis with extant securities laws and investor protection measures.[55] On the other hand, the Commodity Futures Trading Commission (CFTC) regulates cryptocurrencies like Bitcoin and Ethereum as commodities and oversees derivatives trading in the sector.[56] The Financial Crimes Enforcement Network (FinCEN) addresses anti-money laundering (AML) compliance for entities handling cryptocurrencies,[57] while the Internal Revenue Service (IRS) treats cryptocurrencies as property for tax purposes.[58] A new addition is the Infrastructure Investment and Jobs Act, which has introduced provisions to tax digital assets, as a revenue source from the growing cryptocurrency market.[59]

---

[53] *European Union - https://eur-lex.europa.eu/eli/reg/2023/1114/oj*

[54] ibid

[55] *Quatro Hive (2024) The SEC vs. Ripple Case: Setting Precedents for Crypto Regulations in the U.S. Accessed 12/12/2024*

[56] ***CFTC v. McDonnell**, 287 F. Supp. 3d 213 (E.D.N.Y. 2018). This case confirmed the CFTC's jurisdiction over fraud and manipulation in the cryptocurrency derivatives market and its broader authority to regulate spot markets for commodities in cases of fraudulent or manipulative conduct.*

[57] *FinCEN (2013) Application Of FinCEN's Regulations to Persons Administering, Exchanging, or Using Virtual Currencies. U.S. Department of the Treasury. Accessed on 13/12/2024*

[58] *IRS (2023) Notice 2023 – 34. Accessed on 13/12/2024*

[59] *Public Law No. 117-58 (11/15/2021) [117th Congress Public Law 58] [From the U.S. Government Publishing Office] - https://www.congress.gov/bill/117th-congress/house-bill/3684/text*

3.8 China has taken a more restrictive approach to cryptocurrencies, implementing a series of bans on crypto trading and mining activities within the country. The government has expressed concerns over financial stability, money laundering, and speculative trading, which have contributed to its decision to shut down crypto exchanges and prohibit financial institutions from engaging in cryptocurrency transactions.[60] In addition to these bans, China has actively promoted the development and adoption of state-backed digital currencies, such as the Digital Yuan. This digital currency, also known as the e-CNY, is issued and controlled by the People's Bank of China (PBOC), and its primary goal is to maintain governmental control over the monetary system while modernizing payment infrastructure.[61]

3.9 The regulatory measures taken by the Central Bank of Nigeria (CBN) so far appears to follow the China approach. The CBN had in a policy statement in 2017 warned local financial institutions against having any transactions in crypto or facilitating payments for crypto exchanges on grounds that "digital currencies such as bitcoin, Litecoin, and others are largely used in terrorism financing and money laundering.[62] In 2021, the Apex Bank directed all banks to desist from transacting in and with entities dealing in cryptocurrency and directed banks to close accounts of persons or entities involved in cryptocurrency transactions within their systems.[63]

3.10 Following up with the Chinese model, the CBN launched its CBDC - the e-Naira on October 25, 2021 as a digital equivalent of the naira as a medium of exchange and a store of value.[64] The CBDC was lauded as a means to facilitate payment efficiency in

---

[60] *Shin, F. (2022) What's behind China's cryptocurrency ban? - Europe Center, Atlantic Council. Accessed on 13/12/2024*
[61] *ibid*
[62] *Nwanisobi, O. (ed) (2021) Cryptocurrency Trading: CBN Orders Banks To Close Operating Accounts, CBN Update; ISSN No: 2695-2394 Vol. 3 No. 2 Accessed 10/12/2024*
[63] *CBN (2021) Letter to All Deposit Money Banks, Non-Bank Financial Institutions and Other Financial Institutions - dated 5 February 2021.*
[64] *Erezi, D. (2021) Nigeria Launches eNaira Digital Currency. The Guardian. Accessed 13/12/2024*

retail transactions compared to cash. However, adoption has been underwhelming, with most wallets reportedly inactive as of 2024.[65] Public concerns about data privacy, financial crime and widespread mistrust in government have dampened enthusiasm for the digital currency.[66]

3.11 In a policy direction turn, Nigeria's National Information Technology Development Agency developed the **National Blockchain Adoption Strategy** with the purpose of leveraging blockchain as a transition technology into a digital economy and public administration while driving efficiency, transparency, security and accountability in governance.[67] The Strategy document is built on the following 6 key initiatives:[68]

a. Establishment of Nigeria Blockchain Consortium.
b. Strengthening of the Regulatory and legal framework.
c. Focus of the provision of National Digital Identity.
d. Promotion of Blockchain digital literacy and awareness.
e. Creation of Blockchain business incentive programmes.
f. Establishment of a national blockchain sandbox for proof of concepts and implementation

3.12 In May 2023, NITDA further published the **National Blockchain Policy for Nigeria** with a focus "*to grow domestic talent in Blockchain solutions development, foster innovation and catalyze the adoption and use of Blockchain technology*" in the country.[69] The Policy document specifically recognized the potential of Blockchain technology to

[65] *Sohst, R. (2024). Leaving No One Behind: Inclusive Fintech for Remittances. Migration Policy Institute. Accessed 13/12/2024*
[66] *ibid*
[67] *NITDA (2023) National Blockchain Adoption Strategy. Federal Ministry of Communication and Digital Economy. Accessed 10/12/2024*
[68] *ibid*
[69] *NITDA (2023) National Blockchain Policy for Nigeria. Federal Ministry of Communication and Digital Economy. Article 3.0. Accessed 9/12/2024*

"transform financial services by providing secure, transparent and efficient transactions without the need for intermediaries".[70]

3.13 While the implementation of the Strategy and Policy are yet pending, these documents effectively outline the trajectory for the development and adoption of blockchain technology in Nigeria. The increasing adoption of digital assets prompted Nigerian SEC to publish the "**Framework on Accelerated Regulatory Incubation Program for the Onboarding of Virtual Assets Service Providers (VASPs) and other Digital Investments Service Providers (DISPs)** in June 2024"[71] - signaling the stock exchange and securities readiness to adopt Blockchain technologies in the financial and economic ecosystem of the country.

3.14 Consistent with s.38(1) of the Investment and Securities Act 2007, the new regulatory framework mandates registration for all VASPs and other digital investment service providers such as token issuers carrying out business activities in Nigeria or offer services to Nigerian consumer.[72] The regulation also requires registration of individuals and corporate persons "whose activities involve any aspect of DLT and virtual/digital assets services. Such services according to the regulation include; reception, transmission and execution of orders on behalf of other persons, dealers on own account, portfolio management, investment advice, custodian or nominee services, etc."[73]

3.15 By Article 6(i), the Regulation reserves onboarding to only companies and entities incorporated in Nigeria with an operating office and their Chief Executive

[70] *ibid*
[71] *https://sec.gov.ng/wp-content/uploads/2024/06/ARIP-Framework-for-the-Onboarding-of-VASPs_4624.pdf*
[72] *Article 5(a) ibid*
[73] *Article 5)e) ibid*

Officer/Managing Directors or its equivalent resident in Nigeria.[74] Considering the international ramification of blockchain technologies, these regulatory measures are rather restrictive and would stifle onboarding of potential international companies or services providers into the Nigerian market.

3.16 Existing gaps

1. There is no unified legal framework guiding the development and deployment of Blockchain technology in Nigeria. Consequently, there have been different policy thrust by different regulators and agencies of the government. While the CBN has maintained an absolute ban on the technology as far as banks and other financial institutions are concerned in the country, the NITDA has been very progressive in facilitating the off-take of the technology in the country. SEC, however back-tracks on the NITDA progress by enacting a protectionist regulatory framework that would on serve to discourage the development and deployment of the technology.
2. Cryptocurrencies in Nigeria by the CBN was based on security concerns about the potential for cryptocurrencies to facilitate illegal activities such as money laundering, terrorism financing, and tax evasion. Given that countries and other regions (including the E.U)[75] have developed certain laws that govern these platforms to prohibit such occurrences, and the ability to leverage these statutes to develop stringent laws to combat them, the continuation of the ban continues to cause difficulties and hindrances to Nigerians from enjoying basic economic rights offered by these technologies.

[74] *ibid*
[75] *Regulation - 2023/1113 - EN - EUR-Lex*

3. While the SEC's new rules offer guidelines for crypto exchanges providing services[76] in Nigeria seemly raising optimism that the country could embrace blockchain technology and cryptocurrencies, the protectionist approach coupled with the government's treatment of Binance executives is enough to scare away service providers from implementing the provisions of the SEC's new rules.

3.17 Policy Recommendations

1. Develop a unified legal framework guiding the development and deployment of Blockchain technology in Nigeria to clearly define the legal status of cryptocurrencies and blockchain-based assets. This law of the National Assembly should establish comprehensive guidelines, including licensing requirements for blockchain-based financial institutions and platforms. It should also outline the use of blockchain in public financial management, with a focus on anti-money laundering and combating the financing of terrorism.
2. Encourage the adoption of blockchain for low-cost, cross-border payments to improve financial inclusion. This can be achieved through targeted digital literacy campaigns that help citizens, especially in rural areas, understand and use blockchain-based financial tools, while collaborating with microfinance institutions to integrate blockchain technology into their operations to achieve this goal.
3. Nigerian government should lead initiatives to support the development of a National Blockchain Infrastructure, including public and private blockchain networks, to facilitate secure and scalable transactions. This will require substantial investment in research and development centers focused on blockchain innovations in finance.

[76] *Article 25 supra*

4. Mandate adherence to Nigeria's Data Protection Act for all blockchain applications with clearly defined cybersecurity standards for blockchain networks to protect users and prevent fraud.
5. Development of a strong collaboration between government institutions, the private sector, and academia to drive blockchain adoption in Nigeria as proposed in the National Blockchain Policy for Nigeria. This should encourage co-creation and implementation of pilot projects, such as blockchain-based identity management systems for financial transactions.

3.18 Implementation Strategies

1. Establish a national regulatory sandbox[77] to test blockchain applications for all relevant sectors of the country in a controlled environment before full deployment to minimize potential risks to the broader financial ecosystem. This approach also allows regulators to assess technology's compliance with existing laws and adapt regulations based on real-world usage and emerging challenges.
2. To encourage blockchain technology development and deployment, the Nigeria government should consider tax incentives and grants for startups developing blockchain solutions for financial services.
3. Education policy makers and professional training institutions should liaise with the relevant agencies to incorporate blockchain technology into educational curricula and provide specialized training programs for financial professionals.

[77] *https://www.investopedia.com/terms/c/crypto-regulatory-sandbox.asp*

4. In order to accelerate Nigeria's blockchain development, the country should develop partnership with international organizations such as the European Union and adopt relevant global standards including cross-border blockchain initiatives.

4

NEW MEDIA AND FREEDOM OF EXPRESSION

4.1 The emergence of new media—spanning digital platforms, social media, blogs, online news outlets, and other interactive technologies—has significantly transformed how people access, share, and consume information.[78] New media has empowered individuals with unprecedented opportunities for freedom of expression, enabling voices from marginalized communities to participate in global conversations.[79] However, the rapid development of these platforms has also posed challenges for governments, regulators, and societies, particularly concerning the regulation of freedom of expression.[80]

4.2 International frameworks universally affirm freedom of expression as a fundamental right, with global and regional instruments setting standards for its protection. The Universal Declaration of Human Rights (UDHR) guarantees freedom of opinion and expression[81], including the right to seek, receive, and share information without borders. Similarly, the International Covenant on Civil and Political Rights (ICCPR) reinforces this right but permits restrictions for public order, health, or morals.[82] Regionally, the African Charter on Human and Peoples' Rights (ACHPR) provides for the right to information and opinion[83] in Article 9, while the European Convention on

[78] *Benkler, Y., Faris, R., & Roberts, H. (2018). Network propaganda: Manipulation, disinformation, and radicalization in American politics. Oxford University Press.*
[79] *Smith, J. (2020). The digital voice: New media and freedom of expression in the 21st century. Media Studies Press.*
[80] *ibid*
[81] *Article 19 Universal Declaration of Human Rights 1948*
[82] *Article 19 International Covenant on Civil and Political Rights 1966*
[83] *Article 9 (2) African Charter on Human and Peoples' Rights 1981*

Human Rights (ECHR) allows freedom of expression under Article 10, with limitations necessary for a democratic society.[84]

4.3 In Nigeria, the 1999 Constitution (as amended) guarantees freedom of expression under Section 39, affirming every individual's right to hold opinions and share information without interference.[85] It also provides for the right to establish and operate media outlets, subject to regulatory laws.[86] However, these rights come with limitations. Expression that threatens national security, public interest, order and morality are often considered legitimate limitations to free expression.[87] Additionally, Nigeria's defamation laws and some provisions within the Cybercrime (Prohibition) Act, 2015—originally aimed at addressing cyberbullying and fraud—have raised concerns over their use to suppress dissent and restrict digital freedoms, particularly in online spaces.[88]

4.4 Historically, the right of freedom of expression has been a cornerstone for democracy, accountability, and individual liberty.[89] It is often enshrined in many national constitutions as part of their broader commitments to human rights and freedoms, though implementation and restrictions vary widely across countries. With the proliferation of the internet in the late 20th and early 21st centuries, new media disrupted traditional media monopolies, democratizing information production and

[84] *Article 10 European Convention on Human Rights*
[85] *Constitution of the Federal Republic of Nigeria 1999 (As amended), Section 39 (1)*
[86] *ibid*
[87] *sections 39(3) and 45 ibid*
[88] *Spaces for Change (2021) Security Playbook of Digital Authoritarianism in Nigeria. Action Group on Free Civic Space*
[89] *Benkler, Y., Faris, R., & Roberts, H. (2018) op cite*

distribution.[90] This shift amplified free expression but also blurred the boundaries of ethical journalism and accountability.[91]

4.5 Governments, civil society, and tech companies have engaged in debates on how to regulate new media to balance freedom of expression with other pressing concerns such as combating misinformation, hate speech, and threats to national security.[92] These debates often center on the need to preserve open digital spaces while addressing the potential harms of unregulated expression, including the spread of false information, incitement to violence, and the exploitation of platforms for extremist ideologies.[93] At the same time, questions about platform accountability, the role of algorithms in amplifying harmful content, and the ethical limits of censorship further complicate regulatory efforts.[94]

4.6 As the internet continues to evolve and the digital space experiences several changes and modifications, users have unfortunately experienced continuous interference and attacks against their ability to freely express themselves digitally.[95] Series of regulatory frameworks developed so far together with government policies that have sprung up over the years which are targeted at shrinking the online freedom of expression give credence to these fears.[96] Legislations like the Hate Speech Bill 2019, Social Media Bill 2019, Nigeria Broadcasting Code (6th Edition), and the recent Counter Subversion Bill 2024 periodically make their way into the Nigerian civic space to majorly curtail the online or digital freedom of expression.

---

[90] *ibid*
[91] *McChesney, R. W., & Nichols, J. (2010). The death and life of American journalism: The media revolution that will begin the world anew. Nation Books.*
[92] *ibid*
[93] *ibid*
[94] *Smith, J. (2020).Op cit*
[95] *Spaces for Change (2021). Op cit*
[96] *ibid*

4.7 Existing gaps:

1. Absence of a specific legislative provision guaranteeing the protection of online or digital freedom of expression. The existence of this gap allows for the periodic proposal of one bill after another that seeks to take advantage of this gap to restrict free expression or digital freedoms.
2. A comprehensive review of the Nigerian Broadcasting Commission Act to reflect progressive standards for regulating media practitioners and protecting the freedom of expression.
3. The lack of a human rights-based approach to the development of security laws is another contributing factor to the proliferation of laws that seek to curtail online or digital freedom of expression. The amendment of the controversial Section 24 of the Cybercrimes Act 2015 is a noteworthy example of the importance of a human rights-based approach in the lawmaking process of security laws.
4. Blasphemy and defamation laws are ambiguous and open to misuse, leading to the suppression of dissent, creative expression, and legitimate criticism.

4.8 Policy Recommendation

1. Every individual has the right to freely express opinions, ideas, and information without fear of censorship or retribution, as enshrined in international human rights frameworks.[97] Media outlets should be allowed more space to operate without undue interference from governmental, political, or economic entities.

[97] *Article 19 of the Universal Declaration of Human Rights*

2. While upholding freedom of expression, specific policies should address the spread of disinformation by promoting fact-checking, media literacy, and accountability mechanisms.
3. The right to free expression must and should extend to digital platforms. Everyone should have equitable access to the internet and digital tools to exercise their digital rights without fear and harm from state and non-state actors.
4. Journalists and media workers should be safeguarded against harassment, intimidation, and violence. Legal frameworks should clearly define "national security issues" and address impunity against media practitioners and active citizens.
6. Blasphemy and defamation laws should be clarified and reinterpreted with a progressive approach to safeguard freedom of expression while balancing the need to respect cultural and religious sensitivities. These laws are often vague and open to misuse, leading to the suppression of dissent, creative expression, and legitimate criticism.

4.9 Implementation Strategies

1. Enactment of the Digital Rights and Freedom Bill[98] currently on the floor of the National Assembly to protect online freedom of expression. This will unmistakably affirm the country's commitment to international human rights principles to the freedom of expression as enshrined in the Nigerian constitution and international treaties.

2. Establish a national framework for detecting, reporting, and addressing the spread of misinformation, fake news, and harmful content, ensuring these efforts do not infringe on legitimate freedom of speech with clear procedures for removing harmful content, with mechanisms for appealing such decisions to ensure fairness.

[98] https://www.thisdaylive.com/index.php/2024/04/04/nhrc-pi-call-for-accelerated-passage-of-digital-rights-bill-to-safeguard-online-freedoms/#google_vignette

3. Collaborate with technology companies, civil society, and fact-checking organizations to create a multi-stakeholder approach to countering online disinformation, and encourage social media companies to implement content moderation policies that align with Nigerian values, while adhering to principles of free speech.
4. Strengthen legal protections for journalists, bloggers, and online activists, ensuring they are free to express their views without fear of retaliation or censorship and create a safe environment for whistleblowers and individuals using new media to expose corruption or human rights abuses.

5

TELECOMMUNICATION

5.1 Telecommunication regulation seeks to oversee the operation and delivery of communication services, including telephone networks, internet connectivity, and broadcasting.[99] Regulations in the sector are designed to ensure the efficient and equitable management of telecommunication resources, with emphasis on fair access and usage for individuals and organizations alike[100] preventing monopolistic practices in favour of market dynamics that lead to improved service quality and innovation.[101] At the same time, regulatory measures protect consumers by addressing issues such as pricing fairness, data privacy, and service reliability, while also promoting universal access to bridge digital divides and support inclusive development.[102]

5.2 In the early days of telecommunication, services were predominantly provided through government-owned monopolies.[103] These state-controlled entities managed both the infrastructure and the delivery of services, with primary considerations of protecting their national security and providing public access to essential communication tools.[104] However, by the late 20th century, many countries began liberalizing their telecommunications sectors in response to evolving technological and economic demands.[105] Privatization of state-owned entities became a key strategy, opening

[99] *Kenny, C. (2001). Telecommunications regulation in developing countries. Cambridge University Press.*
[100] *International Telecommunication Union (2021). Regulation of Telecommunications and Information Technologies.*
[101] *Bauer, J. M., & Wildman, S. S. (2020) Telecommunications regulation and competition policy: A global perspective. Oxford University Press.*
[102] *ibid*
[103] *Huisman, J. (2014) The Role of Government in Telecommunications: A Historical Perspective. Telecommunications Policy, 38(9), 849-858.*
[104] *Nigeria Economic Submit Group (2000) National Policy on Telecommunication. Ministry of Communication. Accessed 13/12/2024*
[105] *ibid*

markets to competition and creating an environment where efficiency, innovation, and service quality could thrive thereby breaking the monopoly model and paving the way for dynamic, competitive telecommunications industries that better addressed the needs of consumers and businesses.[106]

5.3 These innovations also introduced new complexities, such as spectrum allocation, data privacy, and cybersecurity, necessitating the development of regulatory frameworks that would ensure equitable and efficient use of resources.[107] Simultaneously, globalization amplified the interconnectivity of networks across borders with renewed demands for global regulatory standards.[108] Countries began working through organizations like the International Telecommunication Union (ITU), which essentially facilitates cooperation on spectrum management, interoperability, and the development of unified policies for the sector.[109]

5.4 Regulatory frameworks in telecommunications always seek to establish clear guidelines for service providers to adhere to fair practices while maintaining high standards of service delivery.[110] Spectrum allocation, for instance, is managed to prevent interference and optimize the use of this finite resource, while taxation policies aim to balance revenue generation with affordability for providers and consumers.[111] Modern regulatory approaches increasingly emphasize "technological neutrality" - a principle that ensures regulations apply uniformly across different platforms without favoring one technology over another.[112]

---

[106] *Kenny, C. (2001) Op cit*
[107] *ibid*
[108] *ibid*
[109] *ibid*
[110] *Bauer, J. M., & Wildman, S. S. (2020) Op cit*
[111] *ibid*
[112] *ibid*

5.5 The Nigerian Communications Commission (NCC) is the primary regulatory authority for the telecommunications sector in Nigeria, with a mandate to ensure the effective management and development of the industry.[113] Established under the Nigerian Communications Act (NCA) of 2003, the NCC is tasked with creating an enabling environment for the growth and operation of telecommunication services while safeguarding the interests of consumers and other stakeholders.[114] One of its core responsibilities is licensing operators and ensuring that service providers meet set standards for quality and coverage.[115] The NCC also oversees the allocation and management of the national frequency spectrum.[116]

5.6 The NCC has introduced regulations and policies over the years to address issues such as network quality, consumer protection, and licensing of new technologies. In 2021, Nigeria issued a National Policy on 5G Networks for Nigeria's Digital Economy[117] and charged the Commission with issuing licenses for the deployment of the technology in Nigeria - which a major significant step towards next-generation connectivity. This has boosted internet speed, improved communication capabilities, and provided the foundation for emerging technologies such as the Internet of Things (IoT) and artificial intelligence full of-take in the country.

5.7 Existing gaps

1. Despite the Commission's commendable achievements, concerns persist regarding its role in facilitating digital rights violations, such as "directing network and internet

[113] *S.3 NCA 2003*
[114] *S.1(g) NCA 2003*
[115] *Section 4 NCA 2003 and NCC Licensing Regulations 2013*
[116] *Article 29 NCC Licensing Regulations 2013*
[117] *Federal Ministry of Communication and Digital Economy (2021) National Policy on 5G Networks for Nigeria's Digital Economy. Accessed 13/12/2024*

shutdowns", and consenting to surveillance operations and content moderation by platform operators, all of which impact citizens' privacy rights. While these actions are legally permissible under existing laws like the Nigerian Communications Act 2013,[118] the Lawful Interception of Communications Regulation 2019,[119] and the Cybercrimes Act 2015, the Commission has an opportunity to reassess the human rights implications of these legal measures. It could recommend amendments to the laws and policies to ensure a balance between legal compliance and the protection of fundamental rights.

2. Over the years, the implementation of the Universal Service Provision Fund (USPF) [120] by the Commission has focused less on the potential of community networks, which could contribute to the full realization of the fund's objectives and enhance digital inclusion for marginalized groups and communities. Community networks, locally owned and operated, are designed to provide affordable, reliable, and inclusive connectivity, particularly in underserved and rural areas where traditional commercial providers often deem operations unprofitable. These networks are typically developed, managed, and maintained by local communities, NGOs, or cooperatives, enabling them to customize services that directly address the unique needs of their regions.[121]

[118] *Section 70 NCA 2003*
[119] *https://www.ncc.gov.ng/accessible/documents/839-lawful-interception-of-comunications-regulations-1/file*
[120] *NCC (2007) Universal Access and Universal Service Regulations. Accessed on 10/12/2024*
[121] *Association for Progressive Communications (2024) Community networks newsletter: Why we need to rethink financing for connectivity to bridge the digital divide. Accessed 13/12/2024*

5.8 Policy Recommendation

1. Harmonization of Nigerian telecom policies with the African Union's Digital Transformation Strategy 2020 - 2030[122] and other international best practices[123] to strengthen the capacity of Nigerian Communications Commission to put people and civic rights at the center of the enforcing telecom laws and policies.
2. Fully implement the NDPA 2023 and establish a robust framework for data localization and cross-border data flows in alignment with global privacy standards.
3. Uphold the right to freedom of expression in online spaces, subject to lawful restrictions while combating cybercrimes without infringing on the fundamental rights of individuals.
4. Provide affordable access to ICT tools for marginalized groups, including women, youth, and persons with disabilities and invest in digital literacy programs to improve skills and awareness.[124]

4.9 Implementation Strategy

Ensure participatory decision-making processes by involving relevant government agencies, private sector players, civil society organizations, and international partners in policymaking and execution.

1. Review and amend existing laws to address emerging digital rights challenges.
2. Strengthen the judiciary's capacity to adjudicate cases related to digital rights and cybercrimes.
3. Provide tax incentives for telecom companies investing in digital inclusion projects.

---

[122] *https://au.int/sites/default/files/documents/38507-doc-dts-english.pdf*
[123] *European Declaration on Digital Rights and Principles, https://ec.europa.eu/newsroom/dae/redirection/document/94370, accessed 15 November 2024.*
[124] *Article 4, ibid*

6

PRIVACY PROTECTION AND CYBERSECURITY

6.1 Privacy protection encompasses a range of safeguards designed to prevent unauthorized access, disclosure, or misuse of individuals' personal information.[125] With the advancements in technology and the internet, the concept of privacy has evolved, and with it, the vulnerability of personal data to exploitation through cyber-attacks has also increased in both frequency and sophistication.[126] This growing threat accentuates the need for comprehensive regulations that will be able to address the complexities of the digital landscape and ensure stronger protection for citizens' data.[127]

6.2 Early discussions around privacy were prompted by the rise of computer systems in the 1960s and 70s that were increasingly capable of storing unprecedented amounts of personal data.[128] Governments and organizations began to collect personal data on individuals, which, while useful for administrative and commercial purposes, also raised new ethical and legal questions about the handling and protection of that data.[129] As a result, the need for privacy protection became more apparent, driving early efforts to regulate the use of personal information in the digital age.

6.3 Legal frameworks were introduced over the following decades. In 1974, the U.S. Privacy Act was passed, marking one of the earliest attempts to regulate how the U.S.

---

[125] *Solove, D. J. (2021). Understanding privacy (2nd ed.). Harvard University Press.*
[126] *ibid*
[127] *ibid*
[128] *U.S. Department of Health, Education, and Welfare. (1973) Records, Computers, and the Rights of Citizens: Report of the Secretary's Advisory Committee on Automated Personal Data Systems. U.S. Government Printing Office. Accessed on 13/12/2024*
[129] *Westin, A. F. (1967). Privacy and Freedom. Washington and Lee Law Review. Volume 25, Issue 1:m20*

government handled personal data. [130] By the mid-1990s, the European Union took a major step forward with the enactment of the Data Protection Directive in 1995,[131] which aimed to safeguard personal data within the EU and regulate its export to other regions.[132] This Directive was later replaced by the General Data Protection Regulation (GDPR)[133] in 2016, which further strengthened data privacy rights. The GDPR which largely informed the NDPA 2023, became the global standard for personal data protection, as it granted individuals greater control over their data and imposed stringent requirements on organizations to ensure compliance with privacy standards.

6.4 While privacy protection is primarily concerned with safeguarding personal data from unauthorized access and misuse, cybersecurity regulations focus on the broader security of systems, networks that store, and process this data.[134] Both areas are deeply interconnected, as a breach in cybersecurity can lead directly to privacy violations, compromising individuals' personal information. Conversely, poor data privacy practices can weaken the security of systems, making them more susceptible to cyber-attacks and increasing the likelihood of data breaches.

6.5 In Nigeria, the Cybercrime (Prohibition, Prevention, etc.) Act 2015 is the first federal legislation aimed specifically at criminalizing cybercrime and protecting critical infrastructure in Nigeria.[135] It was enacted at a time when crimes committed via computer systems were increasing. The Act was amended in February 2024, primarily to correct typographical errors and address some issues in the original document. The

[130] *Privacy Act of 1974, 5 U.S.C. § 552a*
[131] *Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data*
[132] *ibid*
[133] *Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)*
[134] *Section 1, Cybercrimes Act 2015*
[135] *Cybercrime (Prohibition, Prevention, etc.) Act 2015, No. 12, Laws of the Federation of Nigeria 2015.*

amendment also ensured compliance with the ECOWAS Court's decision, which found that Section 24 of the Cybercrime Act is inconsistent with Article 9 of the African Charter on Human and Peoples' Rights.[136] However, this amendment was not substantial enough to address the law's shortcomings, especially in light of Nigeria's evolving cyber threats and the increasing scale and sophistication of these threats.

6.6 It is also noteworthy that Nigeria acceded to the Council of Europe Convention on Cybercrime in July 2022. However, this will have no local effect until the Convention is domesticated in accordance with Section 12 of the Nigerian Constitution. Unfortunately, the African Union Convention on Cyber Security and Personal Data Protection has not been signed by Nigeria.

6.8 Existing gaps:

- The objectives of the Cybercrime Act 2015 are to:

  (a) provide an effective and unified legal, regulatory, and institutional framework for the prohibition, prevention, detection, prosecution, and punishment of cybercrimes in Nigeria;

  (b) ensure the protection of critical national information infrastructure; and

  (c) promote cybersecurity and the protection of computer systems and networks, electronic communications, data and computer programs, intellectual property, and privacy rights.

  However, a close examination of the Act's substantive provisions reveals that these objectives were not fully achieved. While several provisions address the first two objectives, the third objective appears to be met only through the assumption that

[136] *The Registered Trustees of Social Economic Rights Accountability Project (SERAP) v. Federal Republic of Nigeria (2022) suit number ECW/CCJ/APP/09/19*

prohibiting certain actions against information systems will promote cybersecurity. The Act lacks provisions that effectively operationalize this third objective.

- Section 3 of the Cybercrime Act allows the President, upon the recommendation of the National Security Adviser, to designate certain computer systems, networks, and information infrastructure as Critical National Information Infrastructure, vital to national security or the economic and social well-being of Nigeria. This designation must be published in the Federal Gazette. In June 2024, this designation order was finally gazetted, nine years after the Act's enactment, signaling a very slow implementation pace. Furthermore, the designation order lacks adequate minimum standards, guidelines, rules, or procedures, as anticipated in Section 3(2) of the Act. Instead, the responsibility for establishing these standards has been delegated to the Office of the National Security Adviser under the designation order.
- Part III of the Cybercrime Act contains the offences and penalties relating to cybercrime. These include:

  1. Offences against critical national information infrastructure
  2. Unlawful access to a computer. Unlawful interception of communications
  3. Unauthorized modification of computer program or data
  4. System interference
  5. Misuse of devices
  6. Computer-related forgery
  7. Computer-related fraud
  8. Identity theft and impersonation
  9. Child pornography and related offences
  10. Cyberstalking
  11. Cybersquatting

12. Cyberterrorism

13. Racist and xenophobic offences

14. Attempt, conspiracy, aiding and abetting

15. Corporate liability

Although the offences addressed by the Act were common at the time of its enactment, new cybercrimes have since emerged, and others continue to evolve. While some provisions of the Act could be extended to cover new methods of cybercrime, it is doubtful whether the Act is flexible and adaptive enough to address emerging threats like revenge porn, disinformation, deepfakes, and ransomware.

- Additionally, the penalties outlined in the Cybercrimes Act are not sufficiently dissuasive to prevent these crimes. Many fines are far lower than the potential damage caused to information systems and individuals by cybercrime.
- Moreover, the Act lacks adequate provisions for victim support in terms of psychological assistance for those affected by cyberstalking or online harassment. This is notably absent, although some provisions address issues relating to monetary compensation or restitution for victims.
- Part VII of the Act addressed issues of jurisdiction. Section 50 of the Cybercrime Act grants exclusive jurisdiction to the Federal High Court for offences prescribed under the Act. However, because Federal High Courts are not present in all areas, it can be difficult or inconvenient for victims of cybercrimes to access these courts, especially in remote locations.

6.9 Policy Recommendation

1. Amend Section 24 (Cyberstalking): This section has been repeatedly used against journalists and activists. Advocate for its amendment to:
    - Narrow the Definition: Redefine "cyberstalking" to require a *credible* threat of harm or a pattern of harassment that causes *substantial* emotional distress. Remove vague language that criminalizes legitimate expression. Base the definition on established international human rights standards regarding freedom of expression.
    - Raise the Threshold: Increase the burden of proof required for conviction. Require clear and convincing evidence of intent to cause harm, not just offense or annoyance.
    - Proportionality of Punishment: Ensure penalties are proportionate to the actual harm caused and not excessively harsh, discouraging legitimate reporting and criticism.
2. Amend Section 4 (Unlawful Access): This section can be misused against journalists investigating corruption or exposing wrongdoing. Advocate for:
    - "Public Interest" Defense: Introduce a "public interest" defense for journalists and researchers who access information systems without authorization *solely* for the purpose of uncovering and reporting on matters of public concern, provided they act responsibly and without causing undue harm.
    - Clarify "Authorization": Define "authorization" more precisely to avoid criminalizing legitimate journalistic practices. Distinguish between authorized access and access for legitimate journalistic purposes.
3. Repeal or Amend Section 26 (Offences Against Critical National Information Infrastructure) when used against Free Expression: This section is overly broad and can

be used to target individuals reporting on infrastructure vulnerabilities or government mismanagement. Advocate for:

- Precise Definitions: Specifically define what constitutes "critical national information infrastructure" to prevent its overbroad application.
- Intent Requirement: Require proof of *malicious intent* to cause harm to infrastructure, rather than simply accessing or reporting on it. Exclude journalistic activity aimed at exposing security flaws or holding government accountable.

Implementation Strategies:

1. Lobbying and Advocacy: Engage with legislators, policymakers, and government officials to advocate for the proposed amendments. Present research findings, case studies, and legal arguments to demonstrate the need for reform.
2. Legal Challenges: Support strategic litigation challenging the misuse of the Cybercrime Act in specific cases. This can help establish legal precedents and create pressure for legislative change.
3. International Advocacy: Engage with international human rights organizations and bodies to raise awareness about the issues and seek their support. International pressure can be effective in promoting legislative reform.
4. Coalition Building: Form a coalition of digital rights organizations, journalists' associations, civil society groups, and legal experts to advocate for these amendments. A united front amplifies the message and increases pressure on policymakers.

5. Public Awareness Campaign: Raise public awareness about the misuse of the Cybercrime Act through media engagement, social media campaigns, and public forums. Educate citizens about their digital rights and the importance of free expression.

7

NEW AND EMERGING TECHNOLOGIES

7.1 The digitization of societies and economies, fueled by advancements in connectivity, is generating unprecedented volumes of data.[137] Technologies like Fibre to the Home (FTTx) and fast mobile networks have revolutionized individuals and organizations interaction with digital activities, enabling innovations and efficiencies that were recently unimaginable.[138] Simultaneously, the proliferation of "smart" objects—devices connected to the internet that can send and receive data—has transformed industries, enhanced convenience, and opened new avenues for innovation.[139] This interconnected ecosystem of people and things has become a cornerstone of modern life.

7.2 Alongside these rapid technological advancements are challenges that are demanding regulatory responses in order to curb the potential associated risks to privacy, security, and societal ideals posed by these technologies. In other words, effective regulation must evolve in step with these developments to ensure that the benefits of digitization are harnessed responsibly.[140] Policies must strike a balance between protecting individuals and organizations from cyber threats and privacy

[137] *International Telecommunication Union (2020) "Global Connectivity Report". Accessed 13/12/2024*
[138] *ibid*
[139] *Evans, D. (2011) The Internet of Things: How the Next Evolution of the Internet is Changing Everything. Cisco Internet Business Solutions Group.*
[140] *United Nations Conference on Trade and Development (2022) Outcome Report: Data and Digitization for Development. eCommerce Week 22 – 25 April 2022. Accessed 13/12/2024*

breaches on one side and encouraging innovation and the adoption of transformative technologies on the other side.

7.3 The commendable efforts of the European Union's Artificial Intelligence Act 2024[141], the GDPR,[142] and the various Blockchain Technology Regulatory Frameworks in countries like Singapore[143] and Switzerland[144] exemplify attempts to create structured yet flexible guidelines for these technologies. International organizations, including the United Nations, OECD, and ITU, are also actively working to develop global norms and standards to address the transboundary nature of these innovations.[145] Despite these efforts, the regulatory landscape remains fragmented, with differing national approaches often leading to challenges in achieving global harmonization.[146]

7.4 In Nigeria, regulatory attempts have resulted in the development of the **National Cloud Computing Policy**, which primarily aims to *"develop an ongoing and iterative program of work which will enable the use of a range of cloud services, as well as changes in the way ICT is procured and operated, throughout the Nigerian public sector…creating an enabling environment for more investment in Cloud infrastructure and platforms."* [147] The framework, while focused on the public sector, recognizes that the private sector has largely adopted cloud to varying degrees across sectors and therefore encouraged it to continue utilizing cloud computing for IT deployment.[148]

---

[141] *Op cit*
[142] *Op cit*
[143] *Maeda, R. (2024) Singapore: A Crypto Hub at the Crossroads of Innovation and Regulation. Presto Research. Accessed on 13/12/2024*
[144] *Thoma, S. (2020) Switzerland Strengthens Fintech and Blockchain Sector. PWC. Accessed 13/12/2024*
[145] *ibid*
[146] *ibid*
[147] *NITDA (2019) National Cloud Computing Policy - Article 4.0*
[148] *ibid*

7.5 Additionally, The National Centre for Artificial Intelligence and Robotics (NCAIR) - a NITDA special purpose vehicles created to promote research and development on emerging technologies and their practical application in areas of Nigerian national interest is focused on researching into the development of AI, robotics, drones, Internet of Things and other emerging technologies in Nigeria.[149]

7.6 While Nigeria currently grasps in efforts to provide formal legislation on current trends and technologies, new ones are emerging. These new and emerging technologies cut across all the various areas of discussion in previous chapters. Some of these new and emerging technologies include:

1. Artificial Intelligence (AI) and Machine Learning (ML)
2. Generative AI (e.g., ChatGPT, DALL-E)
3. Quantum Computing
4. 5G Expansion and 6G Research
5. Edge Computing
6. Decentralized Infrastructure (Blockchain and Distributed Ledger Technology)
7. Extended Reality (XR): Virtual Reality (VR), Augmented Reality (AR), and the Metaverse
8. Sustainable and Green Technology
9. ClimateTech and Carbon Management
10. Cybersecurity Innovations (Zero-Trust Architecture, AI-driven Cybersecurity)
11. Internet of Things (IoT) and Smart Infrastructure
12. Biotechnology and Genomics (e.g., CRISPR Gene Editing)
13. Synthetic Biology

[149] *https://nitda.gov.ng/ncair/*

14. Blockchain Applications Beyond Cryptocurrency
15. Decentralized Finance (DeFi)

7.7 The DRRPG has, in this chapter, limited its policy focus on emerging technologies with cross-sector applications, specifically cloud computing, the Internet of Things, and smart robotics. Together, these technologies are reshaping industries, providing innovative solutions for global challenges, and driving the digital transformation of economies worldwide. However, challenges such as data privacy, security, data interoperability, and governance remain key burning issues in their widespread adoption and regulation.[150]

7.8 Cloud Computing

This technology offers scalable infrastructure and real-time analytics, supporting the integration of large-scale data storage and processing for IoT and robotics applications. It allows organizations to manage and analyze vast amounts of data efficiently, enabling smart decision-making and innovative services.

Challenges with cloud computing

1. Risk of data breaches and unauthorized access, especially in shared environments.
2. Downtime during service outages sometimes disrupt operations.
3. Vendor Lock-in makes it difficult for users to migrate their data or applications between providers.
4. Adhering to data protection laws and industry-specific regulations is sometimes complex.

[150] *Laura Romeo et al (2020): Internet of Robotic Things in Smart Domains: Applications and Challenges - https://www.mdpi.com/1424-8220/20/12/3355*

Policy Recommendations

1. Create a dedicated national cloud computing policy outlining roles, responsibilities, and regulations for stakeholders - aligning Nigerian regulations with frameworks like the Cloud Security Alliance (CSA) guidelines
2. Data sovereignty and full localization for sensitive government and critical industry data, while requiring regular audits and national certification programs for cloud service providers accessible in Nigeria.
3. Regulate Service Level Agreements (SLAs) and Vendor Practices to define minimum SLAs standards, including uptime guarantees, data recovery, and liability for breaches.
4. Provided clear enforcement guidelines on portability of data in NDPA 2023 to address vendor lock-in by service providers.
5. Conduct regular public education campaigns to inform organizations and individuals about cloud risks, rights, and opportunities.

7.9 Internet of Things

IoT connects physical devices and systems, facilitating data exchange and interaction. Its applications span numerous fields, from smart cities and agriculture to healthcare and industrial automation. IoT enables interconnected systems to function dynamically, leveraging real-time data for optimized performance.

Regulatory Issues and Gaps

1. Nigeria currently lacks a specific IoT-focused regulatory framework. Existing ICT and data protection laws, such as the NDPA 2023, Cybercrimes Act 2015, Nigeria's

National Cybersecurity Policy and Strategy etc, only partially address IoT-related risks.

2. IoT devices generate vast amounts of personal and sensitive data, often without clear data ownership or explicit user consent. There is currently limited enforcement of NDPA standards for IoT platforms, making users susceptible to data breaches and cyberattacks.

3. There is insufficient regulation addressing consumer rights in cases of device malfunctions, fraud, or harm caused by IoT-enabled systems.
4. E-waste from IoT devices poses environmental risks. Existing environmental regulations like NESREA guidelines inadequately address the disposal of IoT-related components.

Policy Recommendations

1. The NCC should collaborate with stakeholders to design an IoT-specific polic. This framework should align with global best practices like the EU's Cybersecurity Act and the US IoT Cybersecurity Improvement Act.
2. Update the NCPS and the Cybercrimes Act to include IoT-specific risks, with emphasis on threat modeling, incident response, and vulnerability management.
3. Amend the NDPA 2023 to explicitly cover IoT data processing and ensure stricter requirements for consent, encryption, breach reporting and penalties for non-compliance.
4. Update NESREA Act to include IoT devices and promote the recycling and safe disposal of IoT components.

7.10 Smart Robotics

Smart Robotics represents an evolution in robotics, integrating AI and machine learning to enhance autonomy and functionality. These systems can adapt to their environments, learn from interactions, and operate collaboratively, making them invaluable in healthcare, manufacturing, and other sectors.

Regulation of Smart Robotics

Isaac Asimov, a renowned science fiction writer, introduced the Three Laws of Robotics in his 1942 short story "Runaround" and expanded on them in later works.[151] These fictional principles were the foundational principles towards developing a regulatory framework to guide the behavior of intelligent robots for safe coexistence with humans.[152]

- 1st Law: A robot may not injure a human being or, through inaction, allow a human being to come to harm.
- 2nd Law: A robot must obey the orders given to it by human beings, except where such orders would conflict with the First Law.
- 3rd Law: A robot must protect its own existence as long as such protection does not conflict with the First or Second Law.

Regulatory Issues in Smart Robotics

1. Decision-making in autonomous systems (e.g., lethal autonomous weapons).
2. Bias and discrimination in AI algorithms: Human rights violations in surveillance robotics.

[151] *https://en.wikipedia.org/wiki/Three_Laws_of_Robotics#cite_note-IROBOT-1*
[152] *ibid*

3. Determining accountability and liability for errors or accidents involving robots.
4. Misuse of data collected by robotics for surveillance or commercial exploitation.
5. Risk of cyberattacks targeting connected robotic systems.
6. Job displacement due to automation in manufacturing, agriculture, and services.
7. E-waste management from discarded robotics.
8. Energy consumption of large-scale robotics systems.

Policy Recommendations

Develop a Comprehensive Robotics Policy aligned with international standards (e.g., ISO robotics standards) to guide robotics development, use, safety, and innovation. The proposed guideline should provide for:

1. Securing robotics systems against cyber threats.
2. Robotic safety standards and liability protocols for damages caused by autonomous systems.
3. Mandatory insurance for developers and users of high-risk robotics.
4. Require transparency in algorithm design to prevent biases.
5. Create an ethical committee to oversee AI and robotics deployments, particularly in surveillance, healthcare, and law enforcement.
6. Invest in educational initiatives to reskill displaced workers for tech-driven roles.
7. Encourage Local Innovation and promote local expertise.
8. Launch awareness campaigns to build public trust and understanding of smart robotics.
9. Ensure inclusivity by involving diverse stakeholders in policy design.
10. Create guidelines for recycling and disposing of robotics systems and promote energy-efficient designs in robotics manufacturing.

8

BRIDGING THE GAP AND CONCLUSION

8.1 All through the chapters above, various gaps have been spotted to highlight the shortcomings of available legislation towards the protection of digital rights in Nigeria. In proffering solutions to these issues, below are some recommendations to bridge the gaps:

1. **Human rights by design:** An important piece necessary in bridging the existing gaps in the protection of digital rights in Nigeria is the presence of a human rights-based approach. This approach should be included in lawmaking processes, regulatory directives, implementations and enforcement, among others.
2. **Judicial activism:** The fast-paced nature of evolving technologies and the slow lawmaking process may lead to a negative impact on rights holders and other stakeholders. In its place, a vibrant judiciary can step in via judicial precedence to provide a direction that would ensure that these emerging technologies are not adequately regulated to avoid breaches of digital rights.
3. Social media companies and Tech companies need to collaborate with the government to ensure they understand how to effectively manage risks and ensure people are protected and safe online.
4. Research, Advocacy and Education are important in the enactment of data and digital rights regulation.

5. With respect to the objectives of the Cybercrimes Act, to comprehensively meet the third objective, new, targeted laws will need to be enacted to address these areas systematically.
6. Clarity in the definition of offences is crucial in criminal law, and ambiguities that arise from stretching existing definitions to cover new crimes could impede justice.
7. To address the issue of jurisdiction for offences stemming from the Cybercrimes Act, it is recommended that jurisdiction be extended to include State High Courts to improve access to justice for victims across the country and reduce the burden on the Federal High Court system.
8. **Legal Reform**: Amend or repeal vague and overly broad provisions within existing laws, such as the Cybercrimes Act, to ensure they align with international human rights standards and promote freedom of expression.
9. **Enhanced Oversight**: Strengthen accountability mechanisms to oversee the implementation and enforcement of digital rights laws, thereby mitigating the risk of arbitrary enforcement and abuse of power.
10. **Public Awareness**: Foster public awareness campaigns to educate citizens about their digital rights and empower them to advocate for reforms that uphold civil liberties in the digital sphere.
11. **Stakeholder Engagement**: Facilitate dialogue and collaboration between government, civil society, and other stakeholders to develop inclusive policies that protect digital rights while addressing societal concerns.

8.2 Conclusion and Way Forward: Horizontal regulatory ecosystem

A horizontal regulatory ecosystem enables multiple agencies to jointly oversee various facets of emerging technologies, in order to ensure that their development,

deployment, and usage remain responsible and beneficial.[153] This framework is particularly effective for regulating complex technological innovations like artificial intelligence, IoT, and cloud computing[154] and ensures that issues such as user safety, data breaches, market monopolies, and compliance with technological standards are addressed in a coordinated manner.

Moreover, the cross-border nature of digital technologies makes collaboration and harmonization among regulatory jurisdictions almost mandatory. Internet-based innovations often transcend national boundaries, requiring regulators to align on principles and enforcement mechanisms.[155] For instance, harmonizing data protection rules will ensure seamless cross-border data flows, while dealing with challenges like jurisdictional overlaps in cybercrime cases. This will prevent regulatory arbitrage, where companies exploit inconsistencies between regions to bypass stringent regulations.[156]

[153] *OECD (2021) Practical Guidance On Agile Regulatory Governance To Harness Innovation. Accessed 26/11/2024*
[154] *ibid*
[155] *ibid*
[156] *Zaring, David. (1998). Regulatory Arbitrage. Texas Law Review, 82(6), 1423-1440.*

BIBLIOGRAPHY

- *African Charter on Human and Peoples' Rights 1981*
- *African Union (2024) Continental Artificial Intelligence Strategy.*
- *Association for Progressive Communications (2024) "Why We Need To Rethink Financing For Connectivity To Bridge The Digital Divide": Community Networks Newsletter:*
- *Bauer, J. M., & Wildman, S. S. (2020) Telecommunications regulation and competition policy: A global perspective. Oxford University Press.*
- *Benkler, Y., Faris, R., & Roberts, H. (2018). Network propaganda: Manipulation, disinformation, and radicalization in American politics. Oxford University Press.*
- *Borgesius, F. Z. (2019) Discrimination, Artificial Intelligence and Algorithmic Decision-Making – Council of Europe.*
- *Briggs, C. and Briggs, R. (2024) "10 Case Studies in AI: Bias in Facial Recognition, Hiring, and Advertising," MIT Press, pp.173-191.*
- *CBN (2021) Letter to All Deposit Money Banks, Non-Bank Financial Institutions and Other Financial Institutions - dated 5 February 2021.*
- *CFTC v. McDonnell, 287 F. Supp. 3d 213 (E.D.N.Y. 2018).*
- *Closing Spaces Database (2024) - https://closingspaces.org/*
- *CNN Business (2024) This Mom Believes Character.Ai Is Responsible For Her Son's Suicide.*
- *Constitution of the Federal Republic of Nigeria 1999 (As amended)*
- *Cybercrime (Prohibition, Prevention, etc.) Act 2015, No. 12, Laws of the Federation of Nigeria 2015.*
- *Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995*
- *Erezi, D. (2021) Nigeria Launches eNaira Digital Currency. The Guardian.*
- *European Commission (2024) "AI Act Enters into Force".*
- *European Convention on Human Rights*
- *European Union Agency for Cybersecurity (2022) Cybersecurity Regulation in the EU: Protecting Networks, Systems, and Data.*
- *Evans, D. (2011) The Internet of Things: How the Next Evolution of the Internet is Changing Everything. Cisco Internet Business Solutions Group.*
- *FATF's Recommendation 15 and its Interpretative Note 15 was updated in 2019 to apply AML/CFT measures to VA and VASPs*
- *Fazlioglu, M. (2023) US Federal AI Governance: Laws, Policies and Strategies – Resource Centre.*
- *Federal Ministry of Communication and Digital Economy (2021) National Policy on 5G Networks for Nigeria's Digital Economy.*
- *FinCEN (2013) Application Of FinCEN's Regulations to Persons Administering, Exchanging, or Using Virtual Currencies. U.S. Department of the Treasury.*
- *https://en.wikipedia.org/wiki/Three_Laws_of_Robotics#cite_note-IROBOT-1*
- *Huisman, J. (2014) The Role of Government in Telecommunications: A Historical Perspective. Telecommunications Policy, 38(9), 849-858.*
- *International Covenant on Civil and Political Rights 1966*
- *International Telecommunication Union (2020) "Global Connectivity Report".*
- *International Telecommunication Union (2021). Regulation of Telecommunications and Information Technologies.*

- *IRS (2023) Notice 2023 – 34.*
- *Kemp S. (2024) DataReportal – Digital 2024: Nigeria.*
- *Kenny, C. (2001). Telecommunications regulation in developing countries. Cambridge University Press.*
- *Laura Romeo et al (2020): Internet of Robotic Things in Smart Domains: Applications and Challenges - https://www.mdpi.com/1424-8220/20/12/3355*
- *Lawson, A. (2022) "The EU AI Act Explained: Tracking Developments for Responsible AI". Responsible Artificial Intelligence Institute.*
- *Maeda, R. (2024) Singapore: A Crypto Hub at the Crossroads of Innovation and Regulation. Presto Research.*
- *Marwala, T. (2023) "Militarization of AI Has Severe Implications for Global Security and Warfare" – United Nations Univesity.*
- *McChesney, R. W., & Nichols, J. (2010). The Death and Life Of American Journalism: The Media Revolution That Will Begin The World Anew. Nation Books.*
- *Mougayar, W. (2016). The Business Blockchain: Promise, Practice, and Application of the Next Internet Technology.*
- *National Assembly (2024) Order Paper Wednesday, 27th November, 2024 - House of Representatives: Federal Republic of Nigeria*
- *NCC (2007) Universal Access and Universal Service Regulations.*
- *NCC Licensing Regulations 2013*
- *Nigeria Economic Submit Group (2000) National Policy on Telecommunication. Ministry of Communication.*
- *Nilsson, N.J. (2013) "The Quest for Artificial Intelligence" Cambridge University Press*
- *NITDA (2019) National Cloud Computing Policy*
- *NITDA (2023) National Blockchain Adoption Strategy. Federal Ministry of Communication and Digital Economy.*
- *NITDA (2023) National Blockchain Policy for Nigeria. Federal Ministry of Communication and Digital Economy.*
- *NITDA (2024) National Artificial Intelligence Strategy.*
- *Nwanisobi, O. (ed) (2021) Cryptocurrency Trading: CBN Orders Banks To Close Operating Accounts, CBN Update; ISSN No: 2695-2394 Vol. 3 No. 2*
- *OECD (2021) Practical Guidance On Agile Regulatory Governance To Harness Innovation.*
- *Ogenga, F & Stanley, A. (2023) Regulating Artificial Intelligence in Africa: Strategies and Insights from Kenya, Ghana, and the African Union – Wilson Centre.*
- *Omolaoye, S. (2024) Reps Step Down Bill on Artificial Intelligence Regulation – The Guardian.*
- *O'Neill, A. (2023) Digital Assets: Will Technological And Regulatory Developments Unleash Institutional Blockchain Adoption? – S&P Global.*
- *Pazzanese, C. (2020) "Ethical concerns mount as AI takes bigger decision-making role in more industries" The Harvard Gazzet.*
- *Pazzanese, C. (2021) Regulators Put Cryptocurrency in Crosshairs – The Harvard Gazette.*
- *Privacy Act of 1974, 5 U.S.C. § 552a*
- *Public Law No. 117-58 (11/15/2021) [117th Congress Public Law 58] [From the U.S. Government Publishing Office] - https://www.congress.gov/bill/117th-congress/house-bill/3684/text*
- *Quatro Hive (2024) The SEC vs. Ripple Case: Setting Precedents for Crypto Regulations in the U.S.*
- *Quimbre F and Stockwell S. (2021) "The Implications for Human Rights in the Digital Age"*
- *Regulation - 2023/1113 - EN - EUR-Lex*
- *Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016*

- *Sheehan, M. (2023) China's AI Regulations and How They Get Made – Carnegie Endowment for International Peace.*
- *Shin, F. (2022) What's behind China's cryptocurrency ban? - Europe Center, Atlantic Council.*
- *Smith, J. (2020). The digital voice: New media and freedom of expression in the 21st century. Media Studies Press.*
- *Smith, J. A. (2020). Cybersecurity and Data Protection: Regulations and Challenges. Cambridge University Press.*
- *Sohst, R. (2024). Leaving No One Behind: Inclusive Fintech for Remittances. Migration Policy Institute.*
- *Solove, D. J. (2021). Understanding privacy (2nd ed.). Harvard University Press.*
- *Spaces for Change (2021) Security Playbook of Digital Authoritarianism in Nigeria. Action Group on Free Civic Space*
- *Spaces for Change (2024) The Proliferation of Dual-Use Surveillance Technologies in Nigeria: Deployment, Risks & Accountability.*
- *Tamakloe D. et al (2021) "Transitioning from Face-Face to Online Learning: Creating Safe Spaces*
- *Tapscott, D. and Tapscott, A. (2016) Blockchain Revolution: How the Technology behind Bitcoin Is Changing Money, Business, and the World. Penguin, New York.*
- *The Registered Trustees of Social Economic Rights Accountability Project (SERAP) v. Federal Republic of Nigeria (2022) ECW/CCJ/APP/09/19*
- *Thoma, S. (2020) Switzerland Strengthens Fintech and Blockchain Sector. PWC.*
- *U.S. Department of Health, Education, and Welfare. (1973) Records, Computers, and the Rights of Citizens: Report of the Secretary's Advisory Committee on Automated Personal Data Systems. U.S. Government Printing Office. Accessed on 13/12/2024*
- *UN Global Digital Compact Rev. 1 (2024) https://www.un.org/techenvoy/sites/www.un.org.techenvoy/files/Global_Digital_Compact_Rev_1.pdf*
- *UNESCO (2021) Recommendation on the Ethics of Artificial Intelligence.*
- *United Nations Conference on Trade and Development (2022) Outcome Report: Data and Digitization for Development. eCommerce Week 22 – 25 April 2022.*
- *United Nations Human Right Council Resolution 47/23 - https://documents.un.org/doc/undoc/gen/g21/192/18/pdf/g2119218.pdf*
- *Universal Declaration of Human Rights 1948*
- *Westin, A. F. (1967). Privacy and Freedom. Washington and Lee Law Review. Volume 25, Issue 1:m20*
- *Zaring, David. (1998). Regulatory Arbitrage. Texas Law Review, 82(6), 1423-1440.*

Digital Rights Reform Policy Guide

The e-RIGHTS is co-funded by the European Union, Canada Fund for Local Initiatives (CFLI) and UNESCO, 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).