

Assessing the Need for a

National Action Plan

for Digital Rights
in Nigeria



Assessing the Need for a National Action Plan on Digital Rights in Nigeria


Executive Summary

Digital rights, whether considered an extension of human rights or an independent right, are gaining significant prominence, especially with rapid advances in technology worldwide. Today's rapidly evolving digital landscape in developing and developed nations means that protecting and promoting these valuable rights has become significant to promoting democracy, human rights, and the rule of law. As Nigeria's digital economy continues to expand with several initiatives to improve its internet and broadband penetration, the challenges in protecting and promoting digital rights, such as the right to privacy and data protection, freedom of expression, access to information, and protection against surveillance, continue to expand. The country must now find a way to ensure adequate protection of these rights, especially considering that human rights online should be given as much prominence as human rights offline to safeguard democracy.

This report critically evaluates the necessity and urgency of developing a National Action Plan on Digital Rights in Nigeria. The report emerged against the backdrop of the challenges encountered in coming up with a binding legislation, such as the Digital Rights and Freedom Bill, which was refused assent by the President for reasons. Therefore, the essence of this study is to assess the necessity and feasibility of a National Action Plan and evaluate current legal and institutional frameworks, identify key gaps, examine global best practices, and engage with the lived experiences of citizens and key stakeholders on the issues.

Key Findings

- **Growing Threat to Digital Rights and Freedom:** The report revealed that digital rights are increasingly threatened in Nigeria despite a growing population who are aware of these rights. The most threatened rights include the right to privacy and data protection and the



right to freedom of expression online. The report also highlights that some digital rights, such as the right to digital literacy and access to the internet, may not be easily realizable given Nigeria's current socio-economic situation.

- **Fragmented Legal and Policy Framework:** The study finds that while several laws are relevant to the digital environment, the landscape regarding digital rights remains patchy, fragmented, and uncoordinated. Many Laws and Policies are not rights-based in that the people are not at the heart of these laws; they seem to protect those in power.
- **The Importance of a sui generis Digital Rights Law:** The study also finds that despite skepticism, especially in some quarters, on the viability and feasibility of a binding Digital Rights Law, it is one of the most effective ways of overcoming the challenge of digital rights in Nigeria. There is a need to think more seriously about surmounting the difficulties of enacting a binding law.
- **A National Action Plan as a First Step:** As a first step towards tackling the challenges of digital rights protection, there is a need for a National Action Plan. The study, however, finds that a NAP should not be considered as an end in itself but as a means towards an end. The idea should be towards a binding law on digital rights

Recommendations

- **More Awareness on Digital Rights Enforcement:** The study recommended more awareness among people on digital rights. Although the survey revealed that the level of understanding is relatively high, many people did not know where to complain, or did not bother to try to complain. Therefore, people need to understand the importance of not remaining silent in the face of apparent digital rights violations.
- **Strengthen Legal Protection:** Existing legislation and policies should also be reviewed to streamline digital rights. Likewise, proposed guidelines, strategies, and laws dealing with aspects of technology must also give due credence to digital rights protection.
- **A National Action Plan:** A properly thought-out National Action Plan on Digital Rights should be made, which adopts short lifecycles. This NAP should prioritize two things: coordinating the fragmented legal regime and transitioning to a binding law on digital rights. The process culminating in the NAP must be an all-inclusive process with the participation of all the critical stakeholders
- **Ownership by Government:** The government must acknowledge that digital rights or any initiative towards its protection, including a NAP, should not be considered an anti-government initiative. They need to own it and direct its course.

Conclusion

As Nigeria strives to harness technology for economic growth and enhance its people's well-being, it must find a way to balance this with digital rights protection. The efforts to advance technological development must be carried out alongside an obligation to protect freedom, rights, and justice, especially in the digital sphere. It is only by aligning innovation with human rights protection, democracy, and the rule of law that Nigeria can earn genuine recognition within the global human rights community as a nation committed to these values in the 21st century. While binding legislation is essential for digital rights protection, a National Action Plan is necessary to chart the path towards binding legislation. A National Action Plan could also provide an opportunity for the people to be part of the process of determining how their digital rights should be protected.



Abbreviations

- AI – Artificial Intelligence
- CBN – Central Bank of Nigeria
- CSO – Civil Society Organization
- DRFB – Digital Rights and Freedom Bill
- DRLI – Digital Rights Lawyers Initiative
- FOI – Freedom of Information
- KIIs – Key Informant Interviews
- MRA – Media Rights Agenda
- MoJ – Ministry of Justice
- NAP – National Action Plan
- NCC – Nigerian Communications Commission
- NDPA – Nigeria Data Protection Act
- NDPC – Nigeria Data Protection Commission
- NHRC – National Human Rights Commission
- NITDA – National Information Technology Development Agency
- ONSA – Office of the National Security Adviser
- PIN – Paradigm Initiative



Authors

Lukman Adebisi ABDULRAUF is an Associate Professor in the Department of Public Law at the University of Ilorin, Nigeria. He is also an Honorary Research Fellow at the School of Law, University of KwaZulu-Natal, and at the Institute for International and Comparative Law in Africa, University of Pretoria, South Africa. He holds an LL.D from the University of Pretoria, an LL.M from the University of Ilorin, and an LL.B from Ahmadu Bello University, Zaria. His research focuses on Digital Rights as well as Technology Law and Policy. He has published widely in these areas.

Basheerat Adedolapo Adedayo is an Associate at Aqua Advisories, Ilorin, where she provides legal and policy support on technology-driven regulatory issues. She holds an LL.B from the University of Ilorin, Nigeria. Her professional and research interests focus on Data Protection Law, Digital Rights, and the regulation of emerging technologies. In addition to her practice, she advises and conducts research for start-ups on compliance and innovation challenges in the fintech sector, with particular emphasis on Nigeria's rapidly evolving digital economy.

Ruqayyah Olaitan Farinu is a Legal Intern at the Ministry of Justice, Osun State, Nigeria. She holds an LL.B from the University of Ilorin, Nigeria. Her research interests lie in Intellectual Property Law and Digital Rights, with a particular focus on how these fields are developing within the Nigerian legal landscape.

Reviewers

Khadijah El-Usman: Senior officer programmes (Anglophone West Africa)

Moussa Waly SENE: Programmes Officer (Francophone Africa)

CHAPTER 01

Introduction

In an increasingly digitized world, the protection and promotion of digital rights is becoming a central issue in the broader discourse on human rights.¹ From the right to privacy and freedom of expression to access to information and protection against online surveillance, digital rights represent the intersection of technology and civil liberties. Because of the significance of digital rights, some have now described them as a new generation of human rights - the so-called fourth generation.² Nigeria, like several other developing democracies, faces unique challenges: rapid technological growth, uneven internet penetration, authoritarian tendencies in content regulation and surveillance for law enforcement and national security, and a fragmented legal framework.³ Despite an expanding digital landscape fueled by innovation, activism, and social media engagement, Nigeria has no coordinated or comprehensive approach for realising digital rights. Existing protections are dispersed across multiple legal instruments and policies, many of which were not designed with the complexities of the digital era in mind. There is also confusion as to institutional mandates over digital rights. The broader issue of effective enforcement and compliance with existing laws and policies on digital rights is also an increasing concern associated with the Nigerian landscape. As a result, the country

continues to witness frequent cases of rights violations, ranging from breaches of individuals' data, arbitrary internet shutdowns, and online surveillance to digital censorship.

Against this backdrop, this study seeks to examine the legal and policy landscape of digital rights in Nigeria and explore pathways towards their practical realisation, paying particular attention to the potential of a National Action Plan on Digital Rights in Nigeria. Its specific objectives are to:


- a. Review existing laws, policies, and institutional frameworks regarding digital rights in Nigeria;
- b. Identify overlaps, contradictions, and implementation gaps in the existing framework on digital rights in Nigeria
- c. Conduct empirical engagements with key stakeholders and digital citizens or digital rights subjects;
- d. Develop viable recommendations and propose a model for a context-specific, suitable, and sustainable National Action Plan (NAP) for Nigeria.

This study is unique because it does not just stop at a textual or doctrinal analysis of digital rights. It combines qualitative and quantitative

¹ B Wagner et al 'The Politics of Digital (Human) Rights' (2023) Oxford Research Encyclopedia of International Studies <https://doi.org/10.1093/acrefore/9780190846626.013.694>

² M Risse 'The Fourth Generation of Human Rights: Epistemic Rights in Digital Lifeworlds' (2021) 8(2) Moral Philosophy and Politics 351-378. See also Y Shany 'Digital Rights and the Outer Limits of International Human Rights Law' (2023) 24(3) German Law Journal 461-471. Although some have also vehemently rejected the idea that digital rights are a new generation of human rights. For example, according to Olumide Babalola, 'Contrary to the impression given in some quarters that digital rights are a new sets of rights, they are rather, the replication of legal rights on the Internet and on digital platforms.' See S Okedara, O Babalola & I Chukwukelu Digital Rights in Nigeria: Through the Cases (2022, Noetico Repetum Inc. & Global Macron Pace Limited, Lagos) 9.

³ MM Maseko 'Understanding Digital Rights in An Era of Digital Politics in Africa' (2024) 3(1) Digital Policy Studies Journal 58-72.



research methods, making it more robust, informed, and evidence-based. Indeed, much of digital rights' scholarly and regulatory discourse remains in abstract legal principles or normative frameworks. The empirical landscape, though very crucial, remains uncharted and unengaged.⁴ There is a total dearth of empirical studies that provide context on the perception of digital rights users on their rights, how to effectively protect them, and the critical insights of stakeholders on more effective protection of these unique rights. Given the relative novelty of these rights, empirical studies are indeed very crucial to enable one to understand the terrain properly. This study aims to fill this critical gap. Therefore, informed by the perspectives of key stakeholders and the lived experiences of Nigerian digital users, the study seeks to understand the current landscape, challenges, and opportunities for strengthening digital rights protections. The goal is to provide evidence-based insights that will guide policymakers, civil society, and other actors in assessing the need and feasibility of a national action plan to secure digital rights, promote digital inclusion, and build trust in Nigeria's digital ecosystem. The resulting report will contribute to academic understanding and practical and evidence-based policymaking in this emerging and crucial area.

The study is organised into nine parts. After this introduction providing context to the study, the second section reviews relevant literature, laws, and policy on digital rights in Nigeria. The aim is to provide a high-level assessment of the state of scholarship and an overview of the legal and policy framework. This section also considers the international and regional frameworks and the extent of their application to Nigeria. The third section outlines the methodology for the study, specifically detailing the approaches towards data collection and analysis. Other important issues covered in this section include ethical considerations and limitations of the method. The fourth section briefly summarises the key findings of the empirical research (i.e., both the qualitative and quantitative data).

The fifth section analyses and discusses the key findings from the field investigation. The sixth and seventh sections provide actionable recommendations and a conclusion for the study.

⁴ While there are some empirical studies in related areas, they do not cover digital rights generally. For example, one study merely covers the human rights issues associated with the digital ID system and the people's trust in the government with these IDs. See D Eke et al 'Nigeria's Digital Identification (ID) Management Program: Ethical, Legal and Socio-Cultural Concerns' (2022) 11 Journal of Responsible Technology 100039.

CHAPTER

02

Literature and Policy Review

The scholarly and legal landscapes on digital rights in Nigeria have been growing in recent years, marked by an expanding body of literature and the emergence of new laws and policies. Academic debates now cover various issues relating to digital rights' scope, interpretation, and implementation. At the same time, civil society organisations and policymakers continue to shape discourse and practice through advocacy, policy formulation, and legislative action. Though only occasionally called upon to address questions in this field, the courts at both national and regional levels have made modest contributions that are both relevant and noteworthy. The rapid evolution of digital technologies has further intensified scholarly engagement and legal development, making the field increasingly dynamic. What emerges from this review is a picture of a vibrant and diverse community of actors—academic, legal, and policy-oriented—actively engaging with the challenges and opportunities of digital rights in Nigeria. This section evaluates the literature and the legal–policy landscape in two parts, before presenting a preliminary conclusion on the state of the field.

2.1 Literature Review

Literature on digital rights can be broadly categorised thematically into five or six groups. These are conceptual frameworks, the state's digital rights protection in Nigeria, general or specific recognition and protection of digital rights, institutional and judicial role and mandate in protecting digital rights, and strategies and pathways towards digital rights protection. We will take each one in turn

2.1.1. Conceptual and Theoretical Framework

The concepts of 'Digital Rights' or 'Digital

Human Rights' may be used interchangeably to refer to rights exercisable in the digital age, due to the rise of technology and technological advancements.⁵ To Pangrazio and Sefton-Green, "digital rights are human and legal rights that allow citizens to access, use, create, and publish digital content on devices such as computers and mobile phones, as well as in virtual spaces and communities."⁶ Mathiesen contends that digital rights are not only a set of rights in and of themselves but are also related to other human rights, particularly freedom of expression and the right to privacy in online and digital environments.⁷

Certain scholars have conceptualised these rights as an extension of traditional human rights into the digital environment, including

5 It may appear that both concepts are different, considering the distinct development of 'digital human rights'. Scholars have associated the development of digital human rights to the international human rights context. See Y Shany 'Digital Rights and the Outer Limits of International Human Rights Law' (2023) 24(3) International Law and Digitalization 461-472.

6 Pangrazio, L., & Sefton-Green, J. (2021). Digital rights, digital citizenship and digital literacy: What's the difference? *Journal of New Approaches in Educational Research*, 10(1), 15–27. <https://doi.org/10.7821/NAER.2021.1.616>

7 Mathiesen, K. (2014). Human rights for the digital age. *Journal of Mass Media Ethics*, 29(1), 2–18. <https://doi.org/10.1080/08900523.2014.863124>, Seubert, S., & Becker, C. (2021). The democratic impact of strengthening European fundamental rights in the digital age: The example of privacy protection. *German Law Journal*, 22(1), 31–44. <https://doi.org/10.1017/glj.2020.101>

the right to freedom of expression, privacy, data protection, and access to information, all taking on new significance in an online setting.⁸ However, there is controversy on whether these rights should be treated as distinct from existing human rights or merely as a continuation of them as they evolve in changing times, which may necessitate a legal framework to protect them. MacKinnon⁹ contends that digital and offline rights are inextricably linked. This viewpoint aligns with Nigerian authors such as Babalola,¹⁰ who claim that digital rights are not “new rights” but preexisting rights that have been given new expression in the digital realm. From this perspective, the central challenge is not recognition but the effective translation of these rights into enforceable online protection.

Other scholars, however, stress that digital rights have distinct features that justify their treatment as a separate category. Dror-Shpoliansky and Shany,¹¹ notes that the rapid development of digital platforms has given rise to new risks not thought of by conventional human rights law, such as algorithmic manipulation and content moderation techniques. According to Hintz and Dencik,¹² digital rights are “emerging rights” that address the distinct social and political dynamics of digital technology. This school of thought suggests that recognising digital rights as distinct allows for targeted policy responses, particularly in societies with fragile democratic institutions. Therefore, some scholars contend that the advent of digital technologies necessitates a reexamination of legal frameworks,¹³ Others assert that current constitutional protections, when properly construed, are adequate to protect people’s digital rights online.¹⁴

The debates regarding whether digital rights are an extension of existing human rights or a distinct category of rights have not really materialised in the Nigerian context. However, Adegoke¹⁵ is one of the Nigerian authors who identifies these nuances in conceptualisation. He rightly notes that

if I was going to define digital rights a few years ago, I'd define it as the contextual application of the rights guaranteed by International, regional and national human rights instruments, in the use of existing, emerging and future digital technologies, including the internet. In today's reality, this definition would rather be naive and would be a total misrepresentation of the reality of the majority of the world's population where access to the internet, affordability of devices, digital gender-divide, cost of data etc are still key and pending issues affecting the realisation of fundamental rights.

2.1.2. The state of digital rights (protection) in Nigeria

A few works have assessed the state of digital rights protection in Nigeria. Most of these works are reports from notable civil society organisations working in the space. One of the most common is Paradigm Initiatives Londa-Nigeria Digital Rights and Inclusion Report.¹⁶ This report provides a broad overview of digital rights and inclusion in Nigeria, with the latest being in 2021. The report considers the state in five themes: digital infrastructure and prioritisation of ICT, freedom of expression

8 Kurbalija J, An Introduction to Internet Governance (7th edn, DiploFoundation 2016).

9 MacKinnon R, Consent of the Networked: The Worldwide Struggle for Internet Freedom (New York: Basic Books 2012).

10 O Babalola 'Digital Rights Explained' in KA Adeyemo et al, Pursuit of Legal Education (A Book of Readings by the Faculty of Law, Lead City University, Ibadan)

11 Chukwuma C, 'The Nigeria Data Protection Act 2023: Advancing Privacy Rights in the Digital Era' (2023) 11 Journal of Information Technology Law 87.

12 Hintz A and Dencik L, Digital Citizenship in a Datafied Society (Cambridge: Polity Press 2019).

13 Hintz A and Dencik L, Digital Citizenship in a Datafied Society (Cambridge: Polity Press 2019).

14 Babalola O, 'Data Protection and the Right to Privacy in Nigeria' (2023) https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4625918 accessed 18 August 2025.

15 B Adegoke 'The Five-Point Digital Rights Agenda for Nigeria's New Government' https://paradigmhq.org/the-five-point-digital-rights-agenda-for-nigerias-new-government/?utm_source=chatgpt.com

16 Paradigm Initiative Londa https://paradigmhq.org/wp-content/uploads/2022/06/Londa-Nigeria-Report-2021-lr.pdf?utm_source=chatgpt.com

on the internet, privacy, digital identity and surveillance, internet disruptions, and Artificial Intelligence in Nigeria. Another critical report on digital rights is the Global Freedom on the Net Report, which carries out inadequate studies with country rankings on digital rights protection. The most recent is the 2024 report, which rated Nigeria as partly free with a 59 out of 100 score.¹⁷ This shows a slightly worsening state compared to 2023, when Nigeria scored 60 out of 100.¹⁸

It is important to note that these reports merely detail the nature and type of digital rights violations in Nigeria without going into details on the legal and policy frameworks.

Other emerging works still consider specific digital rights challenges in relation to recent initiatives. One such initiative has to do with digital identification management. Eke et al,¹⁹ for example, empirically examined ethical, legal, and socio-cultural concerns associated with the government's Digital Identification Management Program. They conclude that applying such a program could enable breach of fundamental human rights, including unreasonable surveillance of citizens, for reasons that can be defined only by the government if there are no legal remedies that can protect the citizens.' In the same vein, Itanyi²⁰ examines the data privacy implication of the emerging digital economy in Nigeria arguing that 'the growth in the digital economy and its continuous use to drive businesses have continued to breed a rise in cybercrime and data privacy breaches.'

2.1.3. General and specific recognition and protection of digital rights

Isin and Ruppert²¹ state in their work that digital rights may be understood through five core principles: "expression", which protects against internet censorship; "access", which promotes universal, fast, and affordable internet connectivity; "openness", which ensures the internet remains a free and open network for communication and information sharing; "innovation", which safeguards the freedom to create and innovate without undue permission; and "privacy", which defends an individual's right to control their data and devices. With this, digital rights may take a variety of forms, including but not limited to the right to privacy, the right to freedom of expression, and the right to assembly and association. There are no comprehensive discussions on digital rights in Nigeria. Most of the available scholarships focus on specific rights. A few exceptions are Okedara et al.²² and Babalola.²³ Although the former claims to deal with digital rights generally, it focuses on just data privacy and freedom of expression. Although the latter examines a broad spectrum of digital rights, the analysis is framed conceptually rather than analytically. Similarly, Luminate's framed study on 'data and digital rights' focused more on the right to data privacy than digital rights generally.²⁴ The rest of the work merely focuses on specific digital rights. We will now review them in turn. Another

A. Right to Privacy

The right to privacy is one of the most frequently discussed digital rights in contemporary literature. According to Solove²⁵, privacy is more than controlling one's data; it also includes defense against unauthorised access

17 Freedom House Freedom on the Net 2024 <https://freedomhouse.org/country/nigeria/freedom-net/2024>

18 Freedom House Freedom on the Net 2023 <https://freedomhouse.org/country/nigeria/freedom-net/2023>

19 D Eke et al 'Nigeria's Digital Identification (ID) Management Program: Ethical, Legal and Socio-Cultural Concerns' (2022) 11 Journal of Responsible Technology 100039.

20 Itanyi, N. (2022). The emerging digital economy in Nigeria: sacrificing the protection of privacy and data of consumers on the altar of economic growth. *European Intellectual Property Review*, 44(3), 172-180.

21 Isin, E., & Ruppert, E. (2015). *Being digital citizens*. Rowman & Littlefield.

22 S Okedara, O Babalola & I Chukwukelu Digital Rights in Nigeria: Through the Cases (2022, Noetico Repetum Inc. & Global Macron Pace Limited, Lagos)

23 O Babalola 'Digital Rights Explained' in KA Adeyemo et al, Pursuit of Legal Education (A Book of Readings by the Faculty of Law, Lead City University, Ibadan)

24 Luminate Data & Digital Rights in Nigeria: Assessing the activities, issues and opportunities <https://luminategroup.com/storage/1361/Data-%26-Digital-Rights-in-Nigeria-Report-%5BFINAL%5D.pdf>

25 Solove DJ, *Understanding Privacy* (Harvard University Press, 2008).

and monitoring from governmental and non-governmental agencies. This is because the government and businesses can now gather, store, and analyse vast amounts of people's data, which makes privacy concerns soar in the digital sphere. People voluntarily exchange personal information for access to online services; a situation Westin calls the "privacy paradox".²⁶ This means that technology has significantly impacted privacy, as Abdulrauf pointed out.²⁷ Therefore, there seems to be a tension between the traditional and modern conceptions of privacy, the latter being significantly impacted by new technologies. Salau²⁸ discussed these tensions and their implications from the context of cybersecurity and state surveillance, where he argued that 'while cybersecurity measures are necessary to safeguard against threats to computer networks and public infrastructure and prevent identity theft, they must not become a subterfuge for unlawful surveillance and interference.' In this case, the author calls for a synergy between cybersecurity and online privacy to protect against the threats of state surveillance.

The implication of the above is that within the broader context of digital rights, privacy could be conceptually distinguished from data protection. Abdulrauf was one of the earliest scholars who started this debate in the Nigerian

academic space, where he contends that privacy should be conceptually distinguished from data privacy.²⁹ Much later, Babalola³⁰ and a host of other scholars joined the debate.³¹ This debate has also made its way to the judicial circle in landmark cases such as the *DRLI v. NIMC*³² and *DRLI v. NYSC*.³³ The prevailing position so far is that the right to data privacy is an integral part of the right to privacy under Section 37 of the Constitution.

B. Data Protection

Comparatively, data protection has attracted an overwhelming academic engagement among all the other digital rights. Before the NDPR and the NDPA, most of the discussion around the right focused on calling on the government to enact a law³⁴ and tracing the journey of several failed attempts toward enacting a data protection law in Nigeria.³⁵

After the adoption of the NDPR, scholarship focused on engaging different aspects of regulation and their implications. Most of the works were comparative analyses with the GDPR, which significantly inspired the NDPR.³⁶ Babalola³⁷ analysed the normative and institutional structure of the NDPR and considers it as a step in the right direction. Nevertheless, he called for the enactment of legislation on data protection. In another

26 Westin AF, *Privacy and Freedom* (New York: Atheneum, 1967)

27 LA Abdulrauf 'New technologies and the right to privacy in Nigeria: evaluating the tension between traditional and modern conceptions' (2016) 7 *Nnamdi Azikiwe University Journal of International Law and Jurisprudence* 113

28 AO Salau 'Cybersecurity, state surveillance and the right to online privacy in Nigeria: A call for synergy of law and policy' (2024) 1 *African Journal on Privacy and Data Protection* 152-175. Also available at <https://ajpdp.unilag.edu.ng/images/ajpdp/volume1/Data%20Journal%20Volume%201%20Salau.pdf>

29 LA Abdulrauf 'Do we need to bother about protecting our personal data? Reflections on neglecting data protection in Nigeria' (2014) 5 *Yonsei Law Journal* 163

30 Ibid 84 Olumide Babalola, 'Privacy Versus Data Protection Debate in Nigeria: The Two Schools of Thought' (Legalnaija, Feb. 1 2021) <https://legalnaija.com/privacy-versus-data-protection-debate/02900951941647681314/>

31 See, for example, GKA Adedipe & PA Okparavero 'Data Protection and the right to Privacy in the Digital Era: A Complex Twin' 6(1) *African Journal of Law and Human Rights* 14

32 For more discussions on this case, see F Emmanuel, 'Case review: Incorporated Trustee of Digital Rights Lawyers Initiatives & Ors v. National Identity Management Commission: A Milestone Towards a Human Rights-Based Approach to Data Protection in Nigeria' (2020-2021) 16 *The Nigerian Juridical Review* 306-314.

33 <https://www.dataguidance.com/news/nigeria-digital-rights-lawyers-initiative-files-3>.

34 LA Abdulrauf 'Do we need to bother about protecting our personal data? Reflections on neglecting data protection in Nigeria' (2014) 5 *Yonsei Law Journal* 163; and LA Abdulrauf 'Personal data protection in Nigeria: Reflections on opportunities, options and challenges to legal reforms' (2017) 38 *Liverpool Law Review* 105-134.

35 Paradigm Initiative Towards a Data Protection Legislative Framework in Nigeria: Assessing the Regulatory and Legislative Attempts to Enact a Data Protection Law (2021) https://paradigmhq.org/wp-content/uploads/2022/01/The-Legislative-Journey-towards-a-Comprehensive-Data-Protection-Framework-in-Nigeria_-FINAL-.pdf

36 O Babalola 'The EU GDPR and Nigeria's NDPR. A Comparative Analysis' (2021) 4(4) *Journal of Data Protection & Privacy* 372-387

37 O Babalola 'Nigeria's Data Protection Legal and Institutional Model: An Overview' (2022) 12(1) *International Data Privacy Law* 44

work, Babalola discussed the DPCOs under the NDPR in a comparative context with the GDPR monitoring bodies.³⁸ In a similar vein, Akintola³⁹ also considers the implications of the NDPR for data sharing in biobanking research. Other scholars were critical of the regime of NDPR in terms of its content and impact on the economy, Omotubora in an article titled *How (Not) to Regulate Data Processing: Assessing Nigeria's Data Protection Regulation 2019 (NDPR)*⁴⁰ highlights some of the significant flaws of the NDPR, including a fundamentally defective enforcement structure.

The recent enactment of the NDPA is also attracting considerable scholarly attention, with several scholars engaging different aspects of the law. Like most of the literature in this respect, scholars are more interested in understanding areas of convergence and divergence between Nigeria's data protection regime and the GDPR. Aloamaka comparative examines the NDPA with the GDPR to identify potential challenges in areas such as extraterritoriality, independence of regulatory authority, and enforcement mechanisms.

The enforcement structure of the NDPA is also another topical issue. Issues of independence of data protection authorities from a broader context were the subject of discussion by Abdulrauf,⁴¹ who laid a general foundation of how independence ought to be mainstreamed in data protection regimes across Africa. Nwodo and Amucheazi⁴² was more specific in suggesting how to attain independence for Nigeria's Data Protection Commission, with viable recommendations such as increased funding.

While a very lively debate is growing in the data protection landscape, it is important to stress that data protection is just one of the other digital rights. However, the higher scholarly attention, dedicated legal and institutional structure has seen that it has arguably ranked above all the other digital rights. This by no means means it is the most important of all of them, considering that rights such as freedom of expression are considered the cornerstone of democracy.

C. Right To Freedom of Expression Online

With the rise of digital platforms, this constitutional right has expanded into online spaces, where citizens use social media to participate in public discourse, mobilise for causes, and criticise government actions. The internet has therefore become central to the modern exercise of free expression in Nigeria.

New avenues for democratic participation have been made possible by digital platforms and social media networks such as Twitter, which served and still serves as a tool for advocacy, mobilization, and raising global awareness, particularly during the 2020 #EndSARS protests.⁴³ In a similar vein, Olatunji⁴⁴ observes that social media has changed the face of traditional media by enabling regular people to comment on and influence public policy issues. However, scholars such as Okocha et al have noted how the state has implemented regulatory measures that have occasionally curtailed online speech.⁴⁵ The most prominent example was the suspension of Twitter's operations in Nigeria from June 2021 to January 2022, which was perceived by some commentators as a violation

38 O Babalola, 'Data Protection Compliance Organizations (DPCO) Under the NDPR, and Monitoring Bodies Under the GDPR: Two Sides of the Same Compliance Coin?' (2022) 3(2) *Global Privacy Law Review* 98-106.

39 So Akintola 'Legal Implications of Data Sharing in Biobanking Research in Low-income Settings: The Nigerian Experience' (2018) 11(1) *South Africa Journal Bioethics and Law* 15.

40 A Omotubora 'How (Not) to Regulate Data Processing: Assessing Nigeria's Data Protection Regulation 2019 (NDPR)' (2021) 3(2) *Global Privacy Law Review* 186-199.

41 LA Abdulrauf 'Independence of Data Protection Authorities in Africa: Trends and Challenges' in LA Abdulrauf & H Dube (eds) *Data Privacy Law in Africa: Emerging Perspective* (2025, PULP) 355.

42 FA Nwodo & CO Amucheazi 'Analysis of regulatory strategies to ensure the independence of Nigeria's Data Protection Commission' 15(1) *International Data Privacy Law* 91-100

43 Iwuoha V, 'Digital Mobilisation and the #EndSARS Protests: A New Phase of Online Political Participation in Nigeria' (2021) *African Affairs* 120(480) 443.

44 Olatunji O, 'Social Media, Democracy and Civic Engagement in Nigeria' (2022) *Nigerian Journal of Media and Communications* 16(1) 98.

45 DO Okocha et al 'Social Media Regulation in Nigeria and the Implications on Digital Rights in a Democracy' in U Padhi (ed) *Media & Technology* (2021, Institute of Media Studies) 315.

of the right to freedom of expression⁴⁶ and the use of regulatory tools like the Code of Practice for Interactive Computer Service Platforms/ Internet Intermediaries⁴⁷ and the Cybercrimes (Prohibition, Prevention, etc.) Act⁴⁸ to stifle dissent, even though it addresses offenses like hate speech and cyberstalking.⁴⁹ Yet another perspective is the tension between freedom of expression and cybercrime, as rightly established by Ibe et al,⁵⁰ Adibe et al.⁵¹ While both works identify how section 24 of the Cybercrimes Act impacts the right to freedom of expression online, they do not envisage the current amendments to the Cybercrimes Act.

D. Right of access to the internet

Not too much scholarly attention has been devoted to the right to access the internet. Lawal et al⁵² however argued, using the human rights theory, that Nigeria has a legal and moral obligation to recognise and protect internet access as a human right. This work is indeed insightful in that it looks at internet access as a positive obligation and not the general conception of it as a negative obligation, which is usually advocated when making a case against government social media bans or internet shutdowns. This right was discussed in the context of the government providing an enabling environment for people to use the internet.

2.1.4. Institutional and judicial roles and mandate in the protection of digital rights

There is very scanty literature on the role of specific institutions in digital rights protection in Nigeria. While authors like Nwodo and Amucheazi⁵³ discuss the NDPC; these discussions are limited only to data protection. Obia⁵⁴ considered NITDA's initiative to regulate digital platforms with the Code of Practice for Interactive Computer Service Platforms (the Code). He argued that, unlike other similar regulatory paradigms in Nigeria, the Code regulates platforms and not users. However, what is noteworthy, according to Obia, is that the Code is 'one of Africa's first push towards digital and social media co-regulation.' Though this work was carried out from a digital rights perspective, it addresses issues of social media regulation and the potential capacity of institutions to serve as effective regulators for human rights protection. Importantly, Obia highlights how ineffective NITDA could be in enforcing its norms against big global digital platforms.

The judiciary is also one very important institution in the protection of digital rights. Okedara et al considered their role in digital rights protection by examining a few landmark cases. As earlier mentioned, the study focused more on the right to data privacy and freedom of expression online.

2.1.5. Strategies and pathways towards effective digital rights protection

Yet another theme with limited scholarly attention is providing strategies and pathways. Obia⁵⁵

- 46 Adebajo A, 'Nigeria's Twitter Ban: Implications for Freedom of Expression' (2022) *Nigerian Journal of Human Rights Law* 45.
- 47 National Information Technology Development Agency (NITDA), 'Code of Practice for Interactive Computer Service Platforms/ Internet Intermediaries' (2022) <https://nitda.gov.ng> accessed 18 August 2025.
- 48 Cybercrimes (Prohibition, Prevention, etc.) Act 2015.
- 49 Adetuyi A, 'The Cybercrimes Act and Free Speech in Nigeria' (2019) *University of Lagos Law Journal* 77.
- 50 IU Ibe et al 'The Dichotomy between Cybercrimes Act 2015 and Freedom of Expression under Nigeria's 1999 Constitution' (2024) 19(1) *COOU Law Journal*
- 51 R Adibe et al 'Press Freedom and Nigeria's Cybercrime Act 2015: An Assessment' (2017) 2 *Africa Spectrum* 117-127.
- 52 T Lawal et al 'Towards the recognition of internet access as a human right in Nigeria: A Theoretical and Legal Perspective' (2025) *International Review of Law, Computers & Tecchnology* <https://doi.org/10.1080/13600869.2025.2500798>
- 53 FA Nwodo & CO Amucheazi 'Analysis of regulatory strategies to ensure the independence of Nigeria's Data Protection Commission' 15(1) *International Data Privacy Law* 91-100
- 54 V Obia 'Digital Policy and Nigeria's Platform Code of Practice: Towards a Radical Co-Regulatory Turn' (2025) 7 *Data & Policy* e12
- 55 V Obia 'Digital Policy and Nigeria's Platform Code of Practice: Towards a Radical Co-Regulatory Turn' (2025) 7 *Data & Policy* e12

examines how platform co-regulation can help as an effective strategy within a relatively limited scope, focusing on digital platforms as digital rights violators. In another study, Abdulrauf⁵⁶ considers the application of the concept of digital constitutionalism toward infusing the rule of law and holding digital platforms to account. Both studies focus narrowly on digital platforms. What this means is that other holistic means of digital rights protection, such as enacting a digital rights legislation or a National Action Plan, have not really received significant scholarly attention.

2.2. Legal and Policy Review

There are several laws and policies that have a bearing on digital rights or their protection in Nigeria. This review will examine Nigeria's constitutional, legal, and regulatory instruments to highlight the evolving policy landscape of digital rights. By analyzing existing and pending legal frameworks, including the 1999 Constitution (as amended), the Nigeria Data Protection Act (NDPA), the Cybercrimes Act, and the Digital Rights and Freedom Bill, this review aims to evaluate these laws and identify possible gaps as they relate to digital rights.

2.2.1 Constitution of the Federal Republic of Nigeria 1999 (As amended)

The 1999 Constitution of Nigeria, as amended, is the primary legal document safeguarding the human rights of its citizens, including their digital rights. Its supremacy has been affirmed by the provision of section 1, which provides that the Constitution shall be the supreme law, and any law that goes contrary to the provisions of the Constitution shall be made null and void to the

extent of its inconsistency. Apart from these provisions, other provisions are foundational to digital rights in Nigeria. Section 37 is the bedrock for the data protection regime in Nigeria.⁵⁷ The courts have also held that data protection is part of the constitutional right to privacy.⁵⁸ Likewise, section 39 protects receiving, holding opinions, and imparting information both online and offline. Sections 38, 40, and 41 are also relevant for the online context, especially regarding organizing online protests via social media. These rights are, however, subject to the derogation test in section 45 of the Constitution. Finally, section 12 outlines the context for the bindingness of international instruments including that relating to digital rights

However, scholars have noted the limitations of the Constitution in digital rights protection because they were not drafted with digital rights in mind. Nevertheless, the Constitutional provisions will always serve a useful purpose in giving life to any subsequent initiative on digital rights.

2.2.2. Primary Legislation

Nigeria's digital rights framework is outlined in several important primary laws that expand on the freedom of expression and privacy guaranteed by the constitution. The most important of these is the Nigeria Data Protection Act (NDPA) of 2023, which supersedes the Nigeria Data Protection Regulation (NDPR) of 2019 as the nation's most extensive data privacy law.

A. Nigeria Data Protection Act (NDPA), 2023

The Nigeria Data Protection Act of 2023⁵⁹ provides the general framework for the protection of personal data. The Act seeks to

56 L Abdulrauf 'The Complex Path to Digital Constitutionalism in Africa' in G de Gregorio The Oxford Handbook of Digital Constitutionalism (2025, Oxford University Press).

57 O Babalola 'Nigeria's Data Protection Legal and Institutional Model: An Overview' (2022) 12(1) International Data Privacy Law 44

58 Incorporated Trustees of Digital Rights Lawyers Initiative v NIMC (CA/IB/291/2020; 24 Sept 2021)

59 https://cert.gov.ng/ngcert/resources/Nigeria_Data_Protection_Act_2023.pdf

protect data subjects' fundamental freedoms, rights, and interests as stipulated in the Constitution. In addition, it aims to control how personal data is processed fairly, legally, and responsibly, encouraging data processing methods that protect privacy and personal data security. Furthermore, the Act aims to safeguard the rights of data subjects by guaranteeing that data controllers and processors carry out their responsibilities and offering recourse and remedies for violations.⁶⁰

It also creates the Nigeria Data Protection Commission to oversee the processing of personal data. This Commission also has the power to make binding soft law and issue a directive. It recently made the Nigeria Data Protection Act (NDP Act) 2023 General Application and Implementation Directive to assist with the effective administration of the Act.⁶¹ Before now, the Nigeria Data Protection Regulation 2019 was the primary legal instrument on data protection. While there are controversies regarding its continued application, it has been preserved by section 64 of the Act. Other significant and context-specific regulations that are also important include the Guidelines for the Management of Personal Data by Public Institutions in Nigeria, 2020.⁶²

B. Cybercrimes (Prohibition, Prevention, etc.) Act 2015

The Cybercrimes (Prohibition, Prevention, etc.) Act 2015 (as amended 2024) is both a protector and a threat to digital rights. As much as it is meant to protect users online, it has provisions that are offensive to digital rights. For example, it has broad data retention requirements that require service providers to retain traffic data and subscriber information

for two years and disclose to authorities upon request.⁶³ There are also real-time collection and interception provisions whereby law enforcement authorities may collect traffic data and intercept content data under specified conditions.⁶⁴ On the other hand, the Act tries to protect privacy by outlining the duties of service providers.⁶⁵ The most controversial provision is section 24, which makes it an offence for any person to transmit a message via computer systems or networks that is grossly offensive, pornographic, indecent, obscene, or menacing, or knowingly send false information for causing annoyance, inconvenience, danger, or obstruction, etc. This provision has been criticized for its potential role in undermining the constitutionally guaranteed free speech. This is because of the vague and broad manner in which the provision is couched. The Court of Appeal dismissed a claim, questioning the provision's constitutionality, contending that the provision was not vague.⁶⁶ However, in 2024, the ECOWAS Court of Justice ruled that the section was contrary to Article 9 of the African Charter on Human and Peoples' Rights and ICCPR, ordering the Nigerian government to repeal the section.⁶⁷ Fortunately, the 2024 Amendment Act refined the language of section 24 of the 2015 Act by limiting its scope to pornographic or false information aimed at causing a breakdown of law and order or posing a threat to life.⁶⁸

C. Freedom of Information Act, 2011

The Freedom of Information Act of 2011 promotes the "access" aspect of digital rights by guaranteeing the right of information for public institutions (and some private bodies). This right is often exercised online. The Act also guarantees individuals' privacy by requiring public

60 Omowonuola A., Exploring Data Protection Laws and Practices in Nigeria: A Comprehensive Analysis

61 Section 62, NDPA. See https://ndpc.gov.ng/wp-content/uploads/2025/07/NDP-ACT-GAID-2025-MARCH-20TH.pdf?utm_source=chatgpt.com

62 <https://nitda.gov.ng/wp-content/uploads/2020/11/GuidelinesForImplementationOfNDPInPublicInstitutionsFinal11.pdf>

63 Section 38

64 Section 39, Cybercrimes Act

65 Section 38(5)

66 Solomon Okedara v Attorney General of the Federation (CA/L/174/18)

67 <https://www.premiumtimesng.com/news/top-news/520361-rights-violations-ecowas-court-orders-nigerian-government-to-amend-cybercrimelaw.html?tztc=1>

68 Section 5 of the Amended Act.

entities to refuse requests that would expose personal information without authorization. Therefore, FOI promotes transparency while preserving individual privacy and balancing two digital rights. The Act has, however, been criticized for its implementation deficits and a tendency towards a weak impact in practice due to exemptions, official secrecy cultures, and judicial inconsistencies.⁶⁹ Nevertheless, the Act is an essential enabler of digital accountability values such as open data, but its protective effect is whittled down without administrative compliance and jurisprudential clarity.

D. National Identity Management Commission Act 2007

Nigeria's national identity system is based on the National Identity Management Commission Act 2007. It made the National Identity Management Commission (NIMC) the principal government agency in charge of building and overseeing a centralized database of national identities. According to the Act, the Commission's primary duties include issuing a unique National Identification Number (NIN), managing the National Identity Database, and registering Nigerian citizens and legal residents. The NIMC Act establishes a legal foundation for using biometrics for identification by outlining the kinds of data that must be gathered, including biographical and biometric information like fingerprints and facial images.

An individual has active control over their data thanks to the Nigerian Identity Management Commission Act (NIMC Act) of 2007. This organization is in charge of protecting Nigeria's national database and making sure that the data isn't being used fraudulently.

E. Nigerian Communications Commission Act

Digital and telecommunications are governed by the Nigerian Communications Act (NCA)

2003. The NCA gives the NCC the authority to grant carrier licenses and permit communication interception for security reasons. As mentioned, in an emergency, interception is permitted under sections 147–148. The Lawful Interception of Communications Regulations (2019) made pursuant to the NCC Act recognize authorizations for specific law enforcement agencies and create storage, logging, and reporting duties. There has been a lot of criticism on the wide scope of powers of the "authorized agencies", limited external oversight, and the risk that technical assistance obligations on licensees outpace safeguards.

2.2.3. Soft Laws, Guidelines, and Regulation

A. NITDA's Code of Practice for Interactive Computer Service Platforms/ Internet Intermediaries (2022)

The Code introduced a co-regulatory regime for platform governance, which imposes a duty of care, content-handling obligations, cooperation expectations, and points of contact. In this way, it aims to protect users/citizens against the potential excesses of digital platforms. Although the text reads like best practice guidance, it contains heavy compliance obligations that have been argued by scholars such as Obia that could transcend into a regime affecting privacy and freedom of expression.⁷⁰ Amnesty International has also called on NITDA to ensure the code complies with International Human Rights Law. For example, the Code has been criticized for an attempt to blur the line between misinformation and disinformation.⁷¹ This is because 'criminalizing misinformation that is merely false, regardless of intent, could be problematic.'⁷² There were also concerns regarding numerous provisions mandating 24-hour take-down of online content and their

69 U Nwoke 'Access to Access to Information under the Nigerian Freedom of Information Act, 2011: Challenges to Implementation and the Rhetoric of Radical Change' (2019) 63(3) *Journal of African Law* 435-461.

70 V Obia 'Digital Policy and Nigeria's Platform Code of Practice: Towards a Radical Co-Regulatory Turn' (2025) 7*Data & Policy* e12

71 See Part V of the Code

72 Amnesty International 'Nigeria: NITDA Code of Practice must comply with International Human Rights Law' https://www.amnesty.org/en/documents/afr44/5818/2022/en/?utm_source=chatgpt.com

effect on freedom of expression. According to Amnesty International, these provisions 'incentivize overboard censorship by punishing a failure to remove content but offer no contrary incentive to retain protected expression.'⁷³

B. The Nigerian Broadcasting Code (6th ed., 2019/2020 amendments)

The National Broadcasting Commission issued the amendments to the 6th Edition of the Nigeria Broadcasting Code, which seeks to remove practices identified by NBC as anti-competitive. According to these amendments, broadcasters and licensees of the NBC are restricted from entering into agreements that would give the broadcasters or licensee exclusivity over content. This kind of restriction could impact private investments in digital distribution, thereby impacting online speech.⁷⁴

2.2.4. Policy Frameworks

Policies are not strictly speaking laws. However, they guide decisions and implementation across the policy process. They steer regulators and ministries, but they are not binding laws until they are reduced to statutes or regulations. Therefore, while they have no binding force on their own, they are important documents to guide the process of governance on a particular issue. Although there is no specific policy or strategy on digital rights in Nigeria, there are a few with implications for digital rights protection. The National Artificial Intelligence Strategy 2024⁷⁵ discusses AI as an engine of inclusive growth, but repeatedly notes that 'ethical,' 'responsible,' and 'human-centric' AI are important values in the development and deployment of AI. This is a partly rights-based approach with obvious implications for digital rights in Nigeria. Another important policy is the National Blockchain

Policy (2023),⁷⁶ which is also not a human rights document, but it upholds privacy and data protection-by-design, and it also explicitly expresses an obvious alignment with Nigeria's data protection regime. Furthermore, the National Digital Economy Policy and Strategy 2020-2030⁷⁷ is an umbrella strategy which, among other things, mainstreams access and inclusion as part of the right to access. There are still a lot more, but these are the most significant.

While there are attempts to incidentally include aspects of digital rights in these policies, it must be stressed that the texts are programmatic rather than creating justiciable legal rights.

2.2.5. Proposed Legislation

There are several proposed legislation with implications for digital rights in Nigeria. While some are pro-digital rights, others are anti-digital rights. Regarding those that are anti-digital rights,

A. Frivolous Petitions (Prohibition) Bill, 2015 (First anti-social-media bill)

The Bill seeks to criminalize 'abusive' online statements on broad terms thereby restricting freedom of expression guaranteed by section 39 of the Constitution. It was withdrawn after backlash and a negative committee report.⁷⁸

B. Protection from Internet Falsehood and Manipulations Bill, 2019 (Anti-Social Media Bill)

The Bill would have granted authorities with powers to order corrections/takedowns, block access and criminalise 'false statements' online; it passed second reading but got stuck as a result of very serious criticism and advocacy by

73 Amnesty International 'Nigeria: NITDA Code of Practice must comply with International Human Rights Law' https://www.amnesty.org/en/documents/afr44/5818/2022/en/?utm_source=chatgpt.com

74 N Itanyi et al 'Exclusivity in the 6th edition of Nigeria Broadcast Commission (NBC) Code and a glimpse of the practice in South Africa and the United Kingdom' (2021) 43(6) European Intellectual Property Review 338-396.

75 https://ncair.nitda.gov.ng/wp-content/uploads/2024/08/National-AI-Strategy_01082024-copy.pdf?utm_source=chatgpt.com

76 https://nitda.gov.ng/wp-content/uploads/2023/05/National-Blockchain-Policy.pdf?utm_source=chatgpt.com

77 https://nitda.gov.ng/wp-content/uploads/2020/06/National-Digital-Economy-Policy-and-Strategy.pdf?utm_source=chatgpt.com

78 https://www.aljazeera.com/news/2015/12/4/proposed-social-media-bill-under-fire-in-nigeria?utm_source=chatgpt.com

civil society.⁷⁹

C. Hate Speech (Prohibition) Bill, 2019

Just like the others above, the proposed Bill criminalizes 'hate speech'- a term which is used in the legislation with a very broad scope, thereby enabling the restriction of freedom of expression online.

D. NDPA Amendment Bill (2024/25) – SB.648/SB.650

This bill requires social-media platforms, bloggers, controllers, and processors to maintain physical offices in Nigeria. Non-compliance can lead to a 30-day ban. Although the proposed law is framed as a tool of accountability for digital platforms, it could be an avenue to control digital platforms and chill smaller actors.

Regarding pro-digital rights, the most notable proposed legislation is the Digital Rights and Freedom Bill (DRFB), which is like a comprehensive online human rights charter containing online privacy, expression, anonymity, due process for data requests, net-neutrality-style non-discrimination, etc. Although both legislative houses successfully passed the law after intense lobbying, the then-President refused to assent to the Bill. The Online Harms Protection Bill is also another significant digital rights instrument that, among other things, seeks to ensure accountability for digital platforms.

2.2.6. International and Regional Law

Regional and international norms are also significant in the whole discourse on digital rights protection in Nigeria. The ECOWAS Supplementary Act A/SA.1/01/10 on Personal Data Protection, which is binding, sets principles for the protection of personal data and requests members to establish independent data-protection authorities. At the continental level, the African Commission's Revised Declaration

of Principles on Freedom of Expression and Access to Information in Africa (2019), though soft law, is stated to be the continent's most detailed normative guide for digital rights as it addressed issues such as surveillance, access, anonymity and online expression, and is increasingly invoked in national debates and litigation strategy.⁸⁰

Adjudication at the regional level has concretely pushed back against overbroad digital repression. In *SERAP & ors v. Federal Republic of Nigeria*⁸¹ the ECOWAS Court held that the 2021 Twitter ban violated freedom of expression under Article 9 of the African Charter, ordering Nigeria to align measures with human-rights standards. That precedent is now a persuasive yardstick for evaluating any future platform-blocking or systemic throttling. It must be stressed, however, that in the absence of legislative domestication, international law has limited domestic effect, and state compliance with regional court judgements has been uneven, as SERAP's case illustrates.

2.2.7. Institutional Frameworks

There are multiple institutions with mandates regarding digital rights protection of aspects thereof. Indeed, the institutional framework is dense and overlapping. The most significant institution today in Nigeria is the Nigeria Data Protection Commission (NDPC), established by the NDPA, which focuses on data subjects' information-related rights. The NDPC, required by law to be an independent, separate entity with perpetual succession, also has rulemaking and enforcement powers to ensure respect for the norms stated in the NDPA. In parallel with the NDPC are sector-specific regulators with powers to shape digital life: These regulators include Nigerian Communications Commission (NCC) for telecommunication and interception procedure, the National Information Technology

⁷⁹ https://placng.org/i/protection-from-internet-falsehood-and-manipulation-bill-scales-second-reading-in-the-senate/?utm_source=chatgpt.com

⁸⁰ T Ilori 'Protecting Digital Rights Through Soft Law: Ensuring the Implementation of the Revised Declaration Principles on Freedom of Expression and Access to Information in Africa' (2024) 24(1) African Human Rights Law Journal 1-30.

⁸¹ (ECW/CCJ/APP/23/21; 14 July 2022),

Development Agency (NITDA) for ICT policy and development of ICT generally and the National Broadcasting Commission (NBC) for broadcast (including an asserted reach into web/online broadcasting). The National Identity Management Commission (NIMC) also has a mandate regarding Identity management in the country. The courts, both nationally and regionally, also provide structural support to these agencies in carrying out their functions.

The Federal Competition and Consumer Protection Commission, established by the Federal Competition and Consumer Protection Act (FCCPA) 2018, is not a digital rights agency per se. However, it provides protection that intersects with key digital issues, especially consumer protection, data privacy, fair practice, and platform accountability. The FCCPA prohibits unfair, deceptive, and unconscionable practices in trade and commerce, including digital commerce.⁸² This encompasses misleading user interfaces, hidden subscription fees, or opaque data collection practices. It was on the basis of this that Meta was fined by the Commission in 2025 for non-compliance with Nigerian consumer and data protection laws.⁸³

In view of the above, there are potential areas of conflict in their jurisdictional mandate. Some of these areas could be summarised below:

- i. Content governance: the NBC mandates to register and police online broadcasters could potentially conflict with NITDA's platform Code, producing parallel levers over online speech. This is why some scholars have questioned the legal and competition rationale of the NBCs' approach and cautioned about its potential impact on free speech if the standards remain vague and duplicated.⁸⁴
- ii. Privacy vs. national security: The Cybercrimes Act mandates two years' retention of traffic/subscriber data and

enables real-time collection/interception. This potentially conflicts with the NDPA principles of necessity, minimisation, and rights to contest automated or data-driven decisions unless closely monitored. This potentially brings the Office of the National Security Adviser (ONSA) or the EFCC/DSS into potential conflict with the NDPC.⁸⁵

- iii. Identity vs. Anonymity: The NIMC's NIN-SIM linkage project, which streamlines identity management but restricts anonymous participation and expands surveillance, could potentially conflict with the NDPC's oversight mandate. The implication is that the project can impact privacy and expression online.
- iv. Consumer protection v. data protection: As shown in the Meta case, there is an overlap between the roles of the FCCPC and NDPC. It needs to be pointed out that section 41 (5) of the FCCPA allows regulators to share powers and data with other enforcement bodies. This means the FCCPA can operate jointly with the NDPC under the NDPA where consumer data misuse intersects with unfair practices. Nevertheless, section 63 of the NDPA provides priority of the Act, especially where the provisions of another law are inconsistent with any of the provisions of the NDPA.

The above shows a patchwork of institutional frameworks, with many of the agencies only dealing with issues of digital rights incidentally. Though there are platforms for interagency collaborations, as seen in the joint investigation of the FCCPC and the NDPC with regard to the Meta/WhatsApp case and supported by the FCCPA, such platforms are extremely limited. What this means is multiplicity of institutions without comprehensive protection for digital rights.

82 See Sections 55-66

83 <https://fccpc.gov.ng/violations-tribunal-upholds-fccpcs-220-million-fine-against-meta-whatsapp/>

84 IA Olubiyi & DO Oriakhogba 'Implications of the Nigerian Broadcasting Code on Broadcast Copyright and Competition' (2021) 70(7) GRUR International 644-655.

85 https://paradigmhq.org/wp-content/uploads/2021/05/Digital-Rights-and-Privacy-in-Nigeria_0.pdf

2.3. Preliminary Conclusion: Literature and Policy Gap

As can be easily discerned from the foregoing, the scholarly, legal, and political landscape on digital rights is quite robust. As much as academics are taking an interest in the discussions, civil society is also engaging in a scholarly manner with the issues under contestation. Nevertheless, a few preliminary conclusions can be reached from the review.

- a. Absence of empirical evidence. There is a discernible absence of empirical evidence on digital rights in Nigeria. The scholarship is predominantly doctrinal, library-based, and mostly advocacy-driven. Indeed, not everything can be documented in published works, especially in a fast-paced environment that moves with the rapid advances in technology, and rich insights can be gained from empirical field-based research in this field.
- b. Limited recommendations on the way forward: Most of the scholarly work does not provide concrete recommendations on how to deal with the implementation gaps in their proposals. Indeed, while recommendations are common, only a few operationalise ways forward using concrete tools such as an NAP on digital rights with specific timelines, allocation of responsibilities, measurable indicators, etc.

On the legal and policy side, there are also a few conclusions that can be made from the review.

- a. Progress but fragmentation: While there is significant progress with the enactment of landmark legislation such as the Nigeria Data Protection Act 2023, there are still substantial overlaps between various legal instruments and institutions regarding digital rights. One discernible example is the overlap between the Nigeria Data Protection Commission, NITDA, and the FCCPA regarding the protection of the right to data privacy.

- b. Policy-heavy but scanty laws: In terms of new technologies and digital rights, it is manifest that the landscape is policy and soft law heavy and limited on enforceable and binding law. This is not to say that such soft law mechanisms do not have their own influence in terms of digital rights. However, given Nigeria's unique socio-political and cultural context, such influence is less significant compared to binding and enforceable norms.
- c. Sparse but growing jurisprudence: While courts are being engaged more often on issues of privacy and data protection, the landscape is still thin on binding precedent on other digital rights. The opportunity to promote freedom of expression online has been significantly limited, and such issues have not come before the courts for extensive deliberations. Indeed, one of the reasons for the limited jurisprudence is probably due to the absence of a comprehensive law on digital rights. Judges are more restrained in pushing the frontiers of the constitutional provisions to make them apply to digital rights.

CHAPTER

03

Methodology

This section outlines the methodology of this study and its inherent merits. As earlier noted, the distinctiveness of this research lies primarily in its methodological approach.

3.1. Study Design and Approach

The study utilised mixed methods of both qualitative and quantitative strategies (survey and semi-structured interview). Before then, desk research was utilised to map the scholarly, legal, and policy landscape of digital rights in Nigeria. The primary aim is to enable the researcher to evaluate the scope, quality, and thematic focus of existing academic literature, policy documents, and legal instruments while simultaneously capturing stakeholders' perspectives on the state of digital rights governance and implementation in Nigeria. The study design guarantees both depth and breadth in understanding the digital rights landscape. This design supports triangulation (using different types of data or data from different sources to examine the same phenomenon) and allows the research to bridge the normative analysis with the perception of ordinary digital rights users and stakeholder users. There are several justifications for the selected research design, especially within the context of this study. Some of the justifications of the design include:

- It increases the credibility of the study in that the findings become more robust and better supported across different sources
- It improves depth by allowing a more nuanced picture, considering the already noted gaps, such as the dearth of empirical studies on the subject. Besides, most of the existing studies do not really test the pulse of the users

of digital rights, who are supposed to be at the centre of any serious initiative towards the protection of digital rights.

- It also supports policy relevance, as conclusions for a hybrid study are more persuasive for policymakers because they are backed by multiple forms of evidence

3.2. Data Collection Methods and Tools

3.2.1. Desktop Research

For the first level of research, the study conducted a desk review focusing on three key sources:

- a. Scholarly literature – peer-reviewed journal articles, books, chapters in books, and reports mainly published within the last decade.
- b. Legal framework-national and subnational laws, regulations, and court decisions relevant to digital rights
- c. Policy instruments including strategies, guidelines, and initiatives from government, civil society, and multi-stakeholder platforms

Sources

Scholarly literature

Scholarly literature was basically sourced from general and specific searches of the major databases, including HeinOnline,⁸⁶ Taylor and Francis,⁸⁷ Juta e-Publications, JSTOR, Sabinet, SAGE Journals, Science Direct, Scopus, Westlaw Classic, African Journal Online (AJOL), and Wiley. Specific keywords were used in the search to ensure more relevant results, using keywords such as 'digital rights in Nigeria', 'freedom of expression online in Nigeria', 'human rights online in Nigeria', 'data protection law in Nigeria', etc. To ensure nothing significant is left out, the research also uses general search engines and LLMs such as Google Scholar, Google, ChatGPT, and Co-Pilot. The references in the identified literature also led the research to further literature. Indeed, general searches were also useful in that they directed the researcher to important literature that was not strictly academic, such as reports of Op-eds. The searches indeed yielded vast results. In this case, the researcher was selective and gave much more priority to publications between 2020 and the present. As has been alluded to, this is a period of significant revolution in Information Technology across several African countries, and arguably also the rapid growth in the literature on this subject.

Legal Framework and Policy Instruments

These were largely sourced from official gazettes, government websites, legislative archives and reputable NGOs/CSOs repositories or websites. The researcher also conducted an extensive search across known databases such as Law Pavilion, and websites of the National Assembly and specific government websites such as NITDA, NDPC, NCC, etc. This is also in addition to general web searches on relevant laws and policies on digital rights in Nigeria, with the support of LLMs. These multiple methods ensured nothing significant was left out in

carrying out the legal and policy review.

3.2.2.Key Informant Interviews (KIs)

The second level of the study design involved key informant interviews. From 10 July to 11 August, a total of 10 semi-structured interviews were conducted with a purposive sample of key stakeholders across three categories: Policymakers (NDPC, NITDA, NCC, NHRC, Presidential advisers); Civil society actors (PIN, MRA, DRLI); Academics and legal experts (scholars, activists, legal practitioners). All the interviews were conducted virtually via Zoom and lasted between an average of 30 minutes to 1 hour and 30 minutes. These interviews interrogated the legal gaps, practical experiences, and visions for a NAP.

Tool: An interview guide (See Appendix II) was designed and used to guide the interview and explore deeper insights into identified gaps and to verify findings from the desk review of the literature. This interview guide was structured in five parts, probing specific themes. The interviews were conducted between July and August on the Zoom platform and were recorded with the consent of the Key Informants.

Table 1: Distribution of Key Informants for the Qualitative Interview

Key Informant Expertise	Number of Participants
Policymakers	3
Civil Society	3
Academics/ Legal Experts	4

3.2.3.Survey

An open online survey was conducted using

86 <https://home.heinonline.org/>
87



an online platform without a specific target population.⁸⁸ The only target was to ensure that the participants cut across all the geopolitical zones of the country. The survey instrument was designed to be mobile-friendly, accessible, and context-sensitive, and it covered: understanding of the concept of digital rights, Awareness of digital rights and laws, Experience of digital rights violations, Expectations from the government and regulators, and perceptions about how to effectively protect digital rights, including their understanding of a national action plan. Survey dissemination leveraged academic networks, online platforms such as LinkedIn, X, and other social media platforms, including WhatsApp groups, to ensure geographic diversity and gender inclusivity.

Tool: A carefully crafted and validated survey questionnaire (See Appendix III) was designed using Google Forms. The questionnaire mainly consisted of closed-ended questions, mostly involving the selection of an option or options.

3.3. Data Analysis

Qualitative data: The recorded semi-structured interviews were first transcribed verbatim with the aid of a subscribed version of Fireflies AI Notetaker.⁸⁹ These transcripts were further thoroughly cleaned and scrutinised by the researcher to ensure accuracy. The process involved listening to the interview again and cross-checking the manuscript for accuracy. The interviews were systematically analysed through both manual and automated coding, enabling the identification of recurring themes and the triangulation of findings. ChatGPT 5.0 plus and NVivo were simultaneously used to further enhance accuracy. The findings from the literature, legal, and policy review were further cross-checked against the stakeholder perspectives to assess the implementation realities

Quantitative data: The survey data were analysed using descriptive statistics, including frequencies and percentages, to summarise respondents' characteristics and to identify patterns in awareness, scope, and thematic coverage of digital rights issues. This approach allowed for the distillation of broad trends across different respondent groups and facilitated comparisons between categories such as geographical location, professional affiliation, and stakeholder type. The descriptive analysis was complemented by cross-tabulations to explore relationships between key variables where relevant. Findings were then interpreted in light of the legal and policy context, enabling the identification of both strengths and gaps in the current digital rights landscape.

3.4. Ethical Considerations

Although the study was not reviewed or approved by a formal institutional ethics committee, the researcher implemented critical safeguards to ensure that ethical considerations were prioritised throughout the research process. First, participation in both the survey and the interviews was explicitly stated to be voluntary, with participants reminded that they could withdraw at any stage without consequence. This included the option to request, in advance or after participation, that their responses be removed from the dataset and excluded from the final report. Second, informed consent was obtained from all key informants and survey participants prior to their involvement. Third, no personal identifiers were collected through the survey, and the final report took deliberate steps to anonymise responses from key informants to prevent attribution. In some cases, key informants requested that certain responses be taken off the record, and the research was meticulous enough to take care of such requests.

⁸⁸ Indeed, there are several justifications for an Open survey. Some of the justifications include the exploratory nature of the research, the lack of a comprehensive sample frame, maximizing reach across a dispersed population, low-cost and time-efficient data collection, and the suitability for digital rights/internet-based topics. Most of these justifications apply in the context of this study

⁸⁹ <https://fireflies.ai>

3.5. Limitations

There are a few limitations associated with the methodology used for this study.

First, while an attempt was made to get as many citizens as possible to participate in the survey, it is important to stress that what is presented here is only a random sample of 165 respondents, although specific efforts were made to ensure that each geopolitical zone is represented. However, despite equal efforts to reach survey participants across the country, some geopolitical zones were less represented in the final sample. Similarly, rural perspectives may be underrepresented due to connectivity constraints, which limited participation in the online survey. This underrepresentation does not in any way imply weaker awareness or perception of digital rights in those areas. Notably, it does not compromise the validity of the study, as the analysis focuses on identifying broad trends and thematic patterns that are not dependent on proportional representation from each region.

Second, some legal instruments are evolving or under review, which may affect the currency of the analysis. For example, the Online Harms Protection Bill proposed by NITDA is still in the process and yet to be finalised. Consequently, only a white paper that gives insights into the content of the Proposed Bill is available for public consumption.⁹⁰

Third, due to time constraints, focus group discussions could not be conducted. Nonetheless, the key informant interviews (KIIs) achieved broad representativeness, though with a modest overrepresentation of male respondents. This imbalance was inadvertent, as concerted efforts were made to ensure the participation of both male and female respondents.

⁹⁰ While Paper on the Framework for an Online Harms Protection Bill in Nigeria <https://nitda.gov.ng/wp-content/uploads/2024/12/Updated-OHP-WHITE-PAPER-copy-compressed.pdf>

CHAPTER

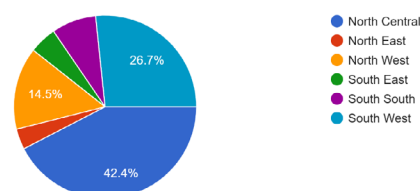
04

Presentation of Results

This section provides an overview of the empirical research findings. For clarity, the results are organised into two parts: the first part covers the Key Informants Interviews, and the second addresses the public perception survey. The qualitative and quantitative findings will be triangulated and jointly discussed in the subsequent section of the study.

4.1. Quantitative Data (Public Perception Insights)

5. Geopolitical zone:
165 responses



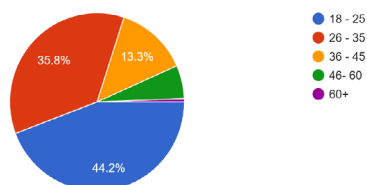
4.1.1. Background information (demographics)

Given the open and voluntary nature of the online survey distribution, there was no specific or predetermined target population or sample size. The survey link was widely disseminated via social media platforms, and a total of 165 responses from across the six geopolitical zones were received during the data collection period.

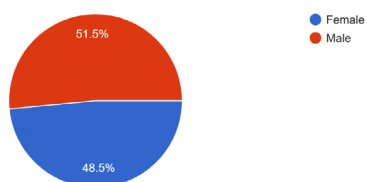
The study had an almost equal gender representation with 51.5% (85/165) females and 48.5% (80/165) males (Fig ???). These populations cut across age groups between 18 to 60+ years. The study had a predominance of respondents between the ages of 18-25 years. 44.2% (73/165) of the respondents fall within the age group, followed closely by 35.8% (59/165) of the respondents between 26-35 years. The ages of 46-60 and 60+ had very low representation with 6.1% (10/165) and 0.6% (1/165) respectively. Nevertheless, all age groups participated in the survey.

Regarding the geographical spread of the respondents, the North-central region had the participants, with 42.4% (70/165) of the respondents. The Southwest and the Northwest have 26.7% and 14.5% respectively. Low turnouts were recorded for the Southeast and Northeast, with 4.8% and 3.6% respectively. While the study aimed for broad geographical representation across Nigeria's six geopolitical zones, participants self-reported their location without distinction between state of origin and state of residence. As such, the geographical analysis reflects respondents' stated locations, which may capture either their place of origin or current residence, depending on individual interpretation. This approach aligns with the study's exploratory design and prioritises inclusivity over strict geographic stratification.

1. Age group
165 responses

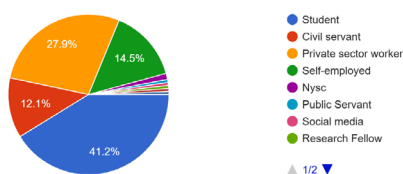


2. Gender
165 responses

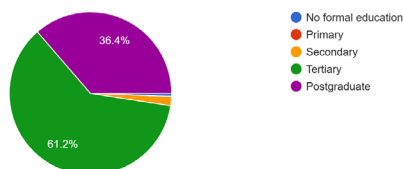


Most of the respondents for the study were well educated, with 61.2% (101/165) educated up to tertiary level, and a further 36.4% (60/165) with even postgraduate degrees. Just about 0.6% (1/165) have no formal education. The level of education also reflects in the occupation of the respondent, which varies broadly, with most of them being students, 41.2% (68/165), and followed by private sector workers, 27.9% (46/165). Other occupations, such as public servants and research fellows, were also represented with very negligible numbers.

3. Occupation
165 responses



4. Educational level
165 responses



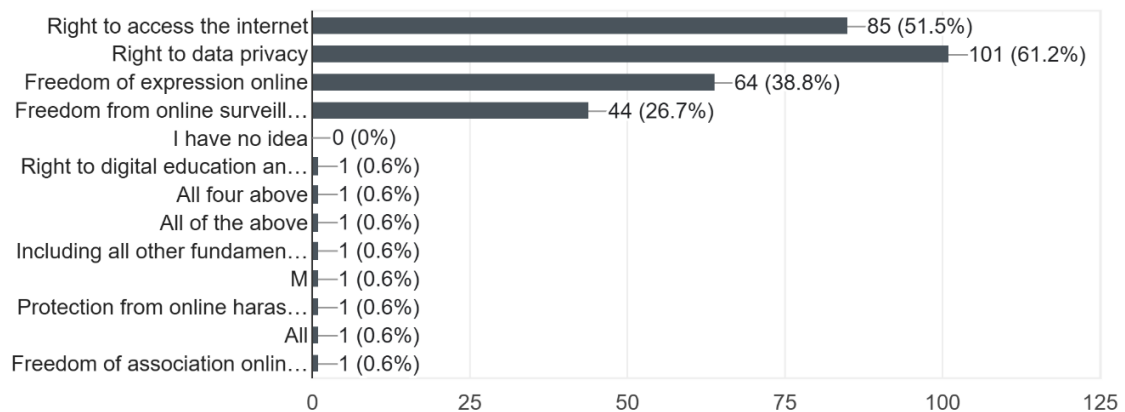
are all about, or at least, what they encompass. 61.2% opine that digital rights mean the right to data privacy, while 51.1% think it is the right to access the internet. Similarly, 38.8% agree that digital rights are all about freedom of expression online. None of the respondents (0%) had any idea what digital rights are all about. Regarding the significance of digital rights, most of them agree that digital rights are very important, 78.8% or Important, 12.1%. Just a few think that digital rights are not at all important, 1.8% or not important, 3.6%. As to which of the digital rights is most important, 82.4 % believe that the right to privacy and data protection is the most important. This is followed by the right to access the internet and the right to freedom of expression as the next most important digital rights, as noted by 47.3% of the respondents. It is noteworthy that none of the respondents (0%) had no idea of the most important digital rights.

4.1.2. Perception of digital rights

The respondents appear to be well aware of digital rights and their significance. Many of them understand broadly what digital rights

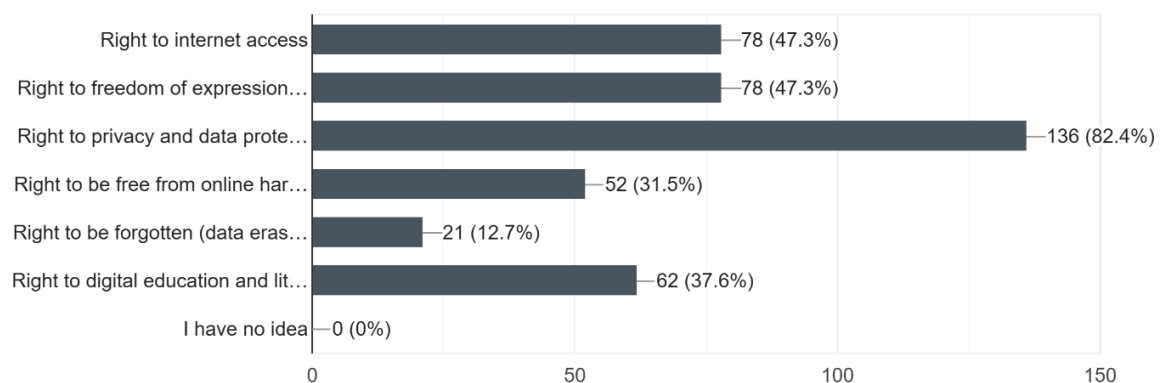
6. When you hear the term "digital rights", what comes to mind?

165 responses



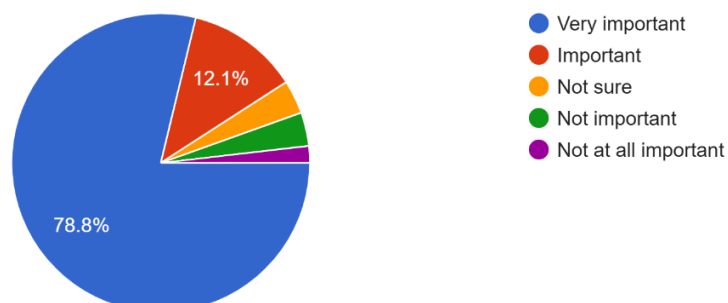
7. In your opinion, which of the following are the most important digital rights? (Select up to 3)

165 responses



8. How important do you think digital rights are in Nigeria today?

165 responses



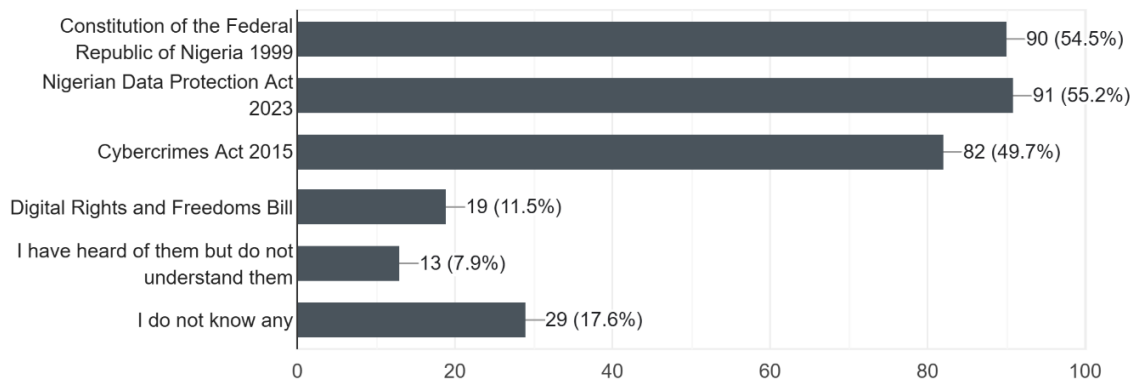
4.1.3. Awareness of legal and institutional frameworks

72.7% of the respondents are aware of laws or policies on digital rights in Nigeria, and 21.8% are not aware of these laws or policies. Regarding the particular law or policy regarding digital rights that they are aware of, the responses show that they are much more familiar with the Nigerian Data Protection Act 2023 (55.2%) and the Nigerian Constitution (54.5%). 17.4% of the respondents do not know any law or

policy on digital rights, while 7.9% have heard of such laws and policies but do not understand them. This data also broadly corresponds with awareness of government agencies responsible for enforcing digital rights, where 70.3% are aware and 23.6% are not aware. Regarding which government agencies the respondents are aware of, the responses are uneven. 32.1% and 17.6% are aware of the NDPC and NITDA, respectively, while 25.5% are not sure of which ones are responsible for protecting digital rights.

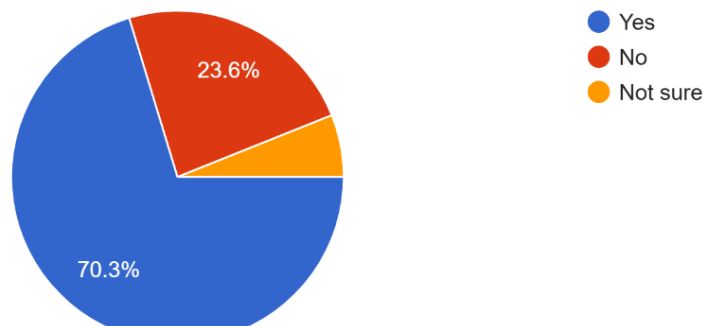
10. If yes, which of the following are you familiar with?

165 responses



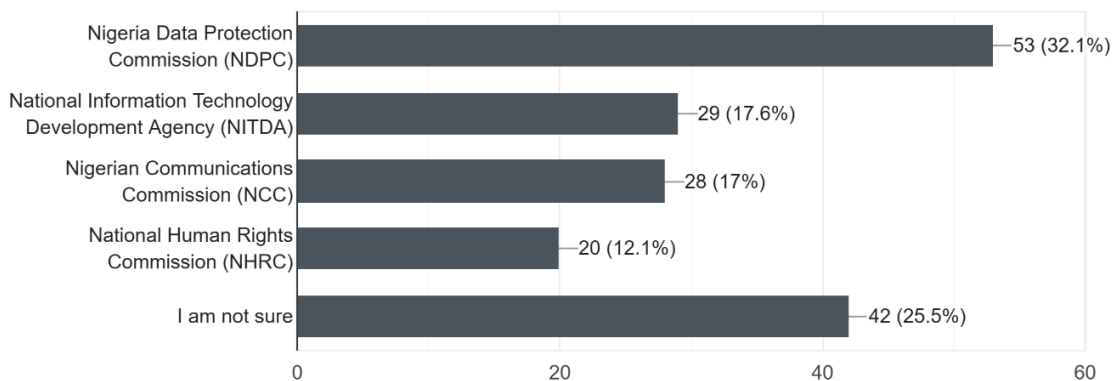
11. Are you aware of any government agency responsible for enforcing digital rights?

165 responses



12. If yes, which ones?

165 responses



4.1.4. Perception and experiences on rights enjoyment and violation

Respondents were asked whether they had experienced any of a list of specified digital rights violations. As shown in Table ??, the most common digital rights violations they had experienced is internet shutdown and social media ban (47.3%), online harassment

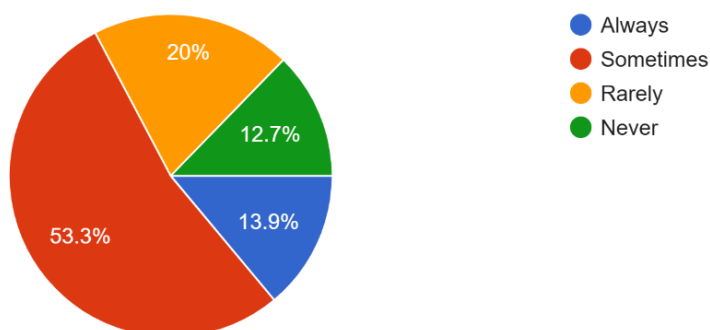
(33.9%). A smaller proportion, 27.9% reported that they had not experienced any form of digital rights violation. Relatedly, 53.3% sometimes feel safe expressing themselves online, as compared to 12.7% and 20% who never and rarely feel safe expressing themselves online, respectively. 13.9% however, always feel safe expressing themselves online.

Despite this, 41.8% never reported these digital rights violations because they think it would not help, and 30.3% of the respondents do not know where to report. Contrarily, 7.3% and 4.8% reported to a CSO and the government, respectively. This figure corresponds with the fact that 48.5% do not trust the government to protect their digital rights as against 30.9% who feel the government can effectively protect their digital rights.

Experience	Frequency (n)	Percentage (%)
Social media account taken down without reason	52	31.5
Government surveillance or monitoring	24	14.5
Internet shutdown or throttling	78	47.3
Online harassment (e.g., hate speech, doxing)	56	33.9
Exposure of personal data without consent	49	29.7
Arrest and/or detention as a result of comments online	32	19.4
I have not experienced any	46	27.9
Prefer not to say	3	1.8

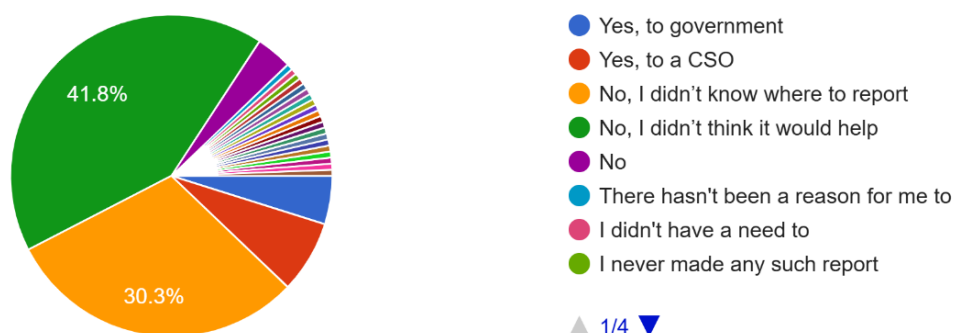
14. Do you feel safe expressing your opinions on digital platforms (e.g., social media, blogs)?

65 responses



15. Have you ever tried to report a digital rights violation?

165 responses



4.1.5. Expectations and policy preferences

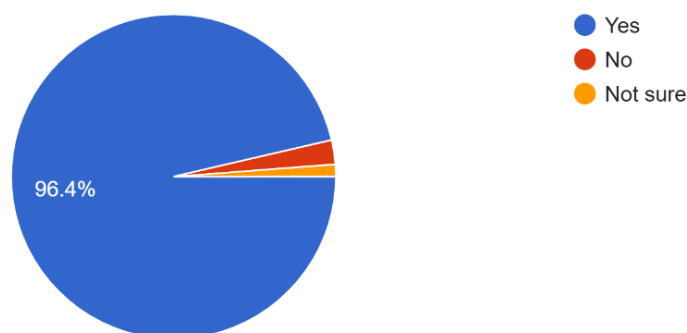
Respondents were asked for their expectations regarding how to move the protection and promotion of digital rights forward. An overwhelming majority of the respondents (96.4%) think Nigeria needs a NAP on digital rights, as against 2.4% who feel otherwise. Regarding what a NAP on digital rights should prioritize, respondents were given the option to select up to 3 options, and the majority think online privacy (85.5%) and affordable and accessible internet should be the priority (60%). Combatting online harassment and enhancing digital literacy also followed closely with 52.7% and 50.3% respectively. Surprisingly, just 20% think clear laws and policies on internet shutdown should be prioritized.

Regarding those who should be involved in the development of a NAP, 38.8% feel government agencies, while 32.1% think citizens/digital users. A moderate 19.4% think civil society organizations, while 11.5% and 9.1% opine that tech companies and academic institutions, respectively, should be involved.

Respondents were also given an opportunity to openly express themselves on any other suggestions they have to move digital rights protection forward. Several suggestions were made in response to the open-ended question, including an effective judiciary, raising awareness levels, prioritizing digital literacy, comparative lessons from other jurisdictions such as Europe, proper and effective implementation and enforcement of laws, clear reporting channels, bringing all stakeholders on board, effective governance of big tech platforms, etc.

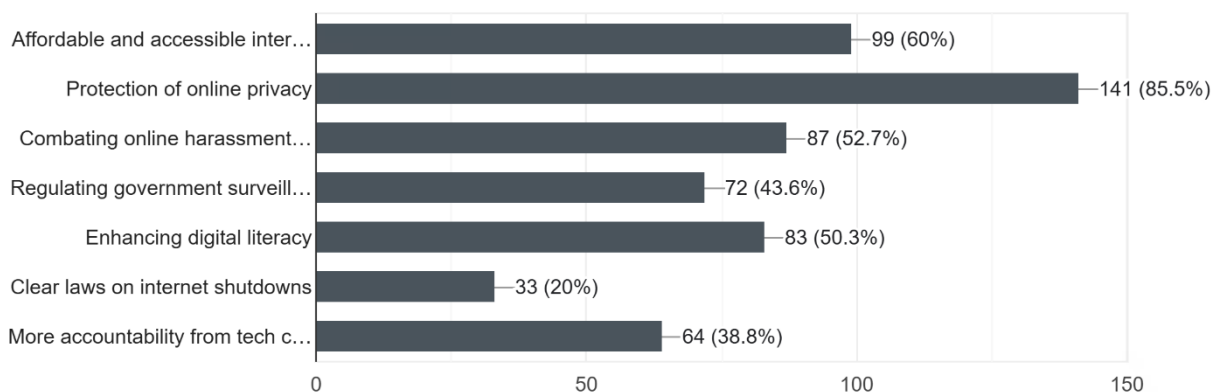
17. Do you think Nigeria needs a National Action Plan on digital rights?

165 responses



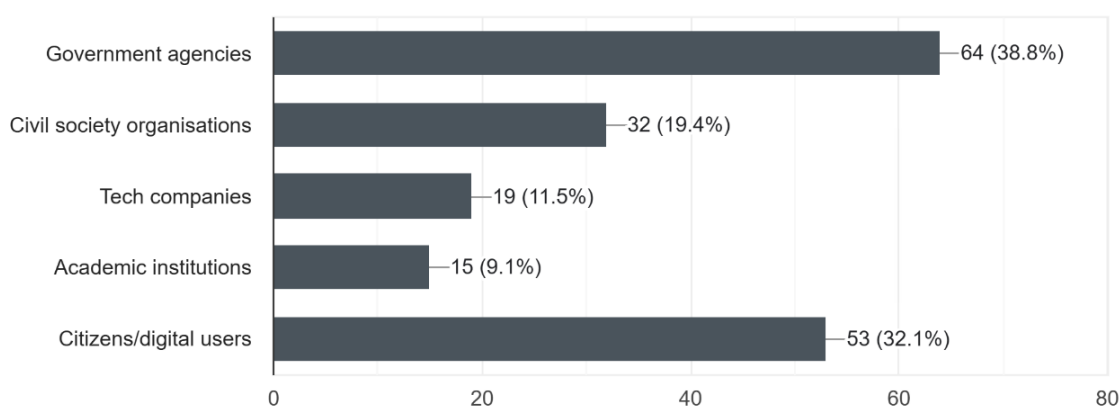
18. What should a National Action Plan on Digital Rights prioritize? (Select up to 3)

165 responses



19. Who do you think should be involved in the development of a National Action Plan? (Multiple choice)

165 responses



4.2 Qualitative Data (Key Informant Insights)

Through a thematic analysis of the Key Informants Interview transcripts, five themes emerged. These themes will be presented in turn.

4.2.1. Impression on the state of digital rights in Nigeria

Almost all the KIs acknowledged the significance of digital rights in today's democratic settings when they were posed questions in this regard. Across the interviews, most (7/10) of them see it as an integral part of human rights, which must be given its place, considering the advances and rapid uptake in new technologies and the internet in Nigeria currently. Nevertheless, the KIs (6/10) perceive the current state of digital rights in Nigeria today to be 'precarious', 'under threat' or 'under pressure', with key rights facing significant challenges. Regarding digital right that is (are) considered the most threatened in Nigeria today, the KIs converge on: (i) privacy and data protection; (ii) freedom of expression online (including arrests and platform restrictions); (iii) state surveillance and associated weak safeguards; (iv) network disruptions (shutdowns/throttling); (v) access/affordability & the digital divide; and (vi) protection of children online. According to KI2, explaining the nature of the challenge

to freedom of expression online and online surveillance,

...there's always been that... clampdown on social media, clampdown on government criticism happening online... We're seeing people being arrested; we're seeing provisions of existing laws being misinterpreted and misused... One grand example... the Twitter ban in 2021... Another critical issue is surveillance... we're seeing increasing investment from the government on... different surveillance tools... [and] safeguards... are significantly missing in Nigeria... no clear oversight mechanism or even public reporting... We have long retention periods... and... we're not prepared for emerging technologies... it's also a combination of... digital divide... more people are... getting disconnected... Governors are also using their powers... to declare [no-communication] spaces... under... fighting terrorism or banditry.

KI6, opined regarding issues of access/affordability; shutdowns/throttling; misuse of cybercrime provision that

...a key issue... was the whole question of access and affordability... Internet shutdown has become a big issue... we've had shutdowns in the Northeast... and... indications... during the August protest of last year... that somebody was trying to throttle the Internet... mass

surveillance... has become the most scary... And we've had such widespread abuse of the Cybercrimes Act... it appears to have been used mostly for journalists and other bloggers... rather than cyber criminals.

Likewise, KI8 noted regarding data protection, access, and children's rights that

...in a digital environment, your identity is all that you have. And if that identity is not protected... you... are not protected... we still have a lot of gaps in terms of awareness... Another fundamental one is the right to access... it costs money... and... the protection of children... nobody is teaching [children] the ethics of being in digital space...

KI9 noted that

...we receive complaints... [notably] cyberstalking... [and] hate speech... spreading certain messages online... that amounts to xenophobic attack... While we investigate, where crime is a component... we may refer to the police or the relevant authorities.

While the responses of the KIs above show that there is currently no unanimity on which of the digital rights is most threatened in Nigeria, there seems to be convergence around freedom of expression and privacy.

Different views were expressed on the most pressing issue regarding the protection of digital rights. There seems to be some strong support for issues of compliance and awareness. KI7 was unequivocal in pointing out that

I think the biggest for me is compliance. The second worst problem is awareness. And I say awareness is not first because compliance also beats awareness. Right. If somebody is punished for doing something wrong with someone else's data, as we have seen happen, the moment that Domino's Pizza was fined and UBA was fined, people were submitting requests immediately. I mean, will you tell me they didn't have awareness before - they did have awareness. But people don't believe. Just like in a democracy, where people

think, Oh, my vote doesn't count. It's the same thing with rights. When you have rights-respecting laws and people don't see them being respected, they see more people going to jail for posting things than more people being punished for sending people wrongly to jail. So clearly, compliance is a major problem.

KI3, however, feels awareness is improving, especially from the perspective of government officials/institutions. According to the Informant, 'The awareness at the top is improving, but the structures are uneven. You have different agencies that see digital rights mostly from their own narrow lenses.'

Yet another challenge identified for the protection of digital rights is associated with the judiciary and the lack of sufficient jurisprudence around digital rights. According to KI1, 'The most pressing... is... jurisprudence around digital rights in Nigeria... it's either non-existent or very weak... There is no [appellate] decision on the Internet shutdown... the ECOWAS Court [has ruled] but... in Nigeria... it's not been as effective as it should be.' To reiterate this position, KI1 further noted that 'We don't have many cases. In fact, we don't have enough cases to be able to even establish a jurisprudence around the cases, even those that we have brought.'

4.2.2. The Legal and Policy Landscape on Digital Rights

The KIs were asked for their perspectives on the state of Nigeria's legal and policy framework regarding digital rights. Though related to earlier questions on their perspective on the respect and protection of digital rights, this inquiry was approached from the standpoint of assessing the current state of digital rights protection. Some (5/10) of KIs maintained that Nigeria's legal and policy framework for digital rights is fragmented, inconsistent, and insufficient to address modern challenges. Specifically, the respondents noted the landscape is overwhelmed by a negative or offence-centric legal environment (lots of prohibitions, little affirmative rights protection), fragmented mandates across key agencies (NITDA, NDPC, NCC, FCCPC, NHRC, etc.), and

coordination gaps that obstruct enforcement. Some respondents also acknowledge the agenda-setting and standard-setting roles of CSOs, but these have had minimal impact largely because of resistance from government agencies or bureaucracy-related challenges. Yet, others do not believe that there is anything wrong with the legal landscape of digital rights. Based on this view, which seems to be in the minority, all that is needed is effective coordination (KI3).

Specifically, KI6 pointed out the issue of the affirmation gap and offence-centric laws. The respondent stated that ‘...you didn’t have a positive affirmation of rights... All you had was laws that made... activities in the online environment criminal offenses... you don’t really have any instrument... which affirms digital rights... [So] we lean to judicial interpretation... or regional and international instruments.’ This gap persists despite the influence of international law in this regard, as noted by K6, who further noted that ‘In 2012, the UN Human Rights Council... said the rights that exist offline must also be exercised and protected online... Nigeria was one of the six countries that co-sponsored [that] resolution.’

Issues of fragmentation and lack of coordination are another issue pointed out by many of the KIs. These issues persist in both the legal and institutional framework. While ‘issues to do with digital rights... can be found in other laws, both domestic and international, as rightly pointed out by KI9, the framework is fragmented and characterized by ‘different agencies who see digital rights mostly from their own lenses.’ (KI3). This situation, according to KI6, results in a system where there are ‘conflicting legislations and also conflicting interpretations by the courts.’

The respondents noted that overlap and lack of coordination in the laws have also impacted the effectiveness of the institutions. According to KI7, ‘We have policy whiplash... rigid procurement timelines that don’t fit tech cycles... multiple overlapping mandates that create a regulatory spaghetti... Agencies work in silos... accountability gets diffused.’ Similarly, KI1 contends that ‘...there will be overlaps... which must be clearly stated... so that one agency does not usurp the other... [as seen in] data protection and competition...

[and] fragmented data collection by FRSC, Immigration, NIMC, banks... harmonization was never followed through.’ Yet still, some of the KIs do not agree that there is overlap or lack of coordination in the multiple agencies.’ For example, KI3 pointed out that ‘The Nigeria Data Protection Commission, for example, is focused on data. The Office of the National Security Adviser is focused on national security.’ The Respondent argued that all relevant institutions in this regard have their broad mandates specified in their establishing statute and they stick to these mandates. KI3 further stated that there is effective interagency coordination and collaboration between the various agencies.

Be that as it may, KI8 gave suggestions on how to manage conflicting mandates to ensure better coordination. Accordingly,

Whichever regulator has powers offline... should also be given the same powers online... [A] need for synergy... it doesn’t matter where you report... it is the duty of that agency to... refer the problem to the right agency... [On loan apps] we approached FCCPC, NDPC, CBN... and the app stores... FCCPC issued consumer-protection rules; NDPC wrote to the apps... and... we used police to chase them... the problem has been handled.

Some of the participants also provided perspectives on the suitability of the Constitution and existing laws and their potential as effective digital rights instruments. Thus, while some KIs acknowledged that digital rights are covered by the Constitution and other existing laws, they stressed that the framework is not designed to address the unique complexities of the digital age.

Despite everything, KI5 and KI7 point out that the realization of the issues of fragmentation and lack of coordination is what brought about the Digital Rights and Freedom Bill, which was initiated as far back as 2014.

4.2.3. The Digital Rights and Freedom Bill

The respondents were asked to share their perspective on the Digital Rights and Freedom

Bill and its (or similar Law) potential added value to the digital rights protection landscape in Nigeria. 6 of the 10 KIs expressed their views on the Digital Rights and Freedom Bill since they have interacted with or had the opportunity to go through the Bill or participated directly in the processes culminating in the Bill. 4 of them opined that the Bill was a significant step forward because of its attempt to create a single, comprehensive legal framework for digital rights in Nigeria, as opposed to the current fragmented approach. Specifically, KI5 and KI7 were generally of the view that the intent of the Bill was indeed noble, considering that it sought to articulate and consolidate rights online.

Regarding the added value of the Bill if it had eventually been passed, KI2 stated that it was 'an attempt at being able to bring together and consolidate all of the different rights that were embedded in all of the different laws.' This consolidation would have provided a consolidated piece of legislation that digital rights users could reference. KI5 also noted that the Bill 'provided for a single piece of legislation that if I am an internet user and I feel that my rights have been violated, I should be able to go somewhere to seek redress, and I am not tossed to different agencies.' The KI also noted that it would have introduced 'oversight for surveillance, internet shutdown procedure.'

Despite the praises, some of the KIs identified certain technical issues with the Bill. For example, KI2 stated that:

Yes, noble intention... genuine problem... But... a number of its provisions are not doing enough to safeguard [issues]... words... not defined... enforcement might prove tricky... the mandate is meant to sit with the Human Rights Commission... what has success meant for [NHRC] in terms of preserving human rights... Are we going to repackaging the institution?

Most of the discussion centred around the Bill, why the President refused to assent to it despite its passage at the Senate and the House of Representatives. Although a formal letter, which

is publicly available, was sent to the National Assembly on the reason for rejection,⁹¹ KI5 explained that the stated reason was that,

The Bill reads like a constitution for the Internet... sweeping, duplicative, and at points internally inconsistent. It drifts into areas already covered by sector laws—competition, consumer protection, even criminal procedure—without grappling with how those mandates would interact. It promises rights expansively but is thin on remedies and realistic enforcement pathways.

Other KI, especially KI1, KI14, KI8 explained other reasons why the Bill would ordinarily not be assented to by the President. According to KI1,

If the bill is seeking to create a commission... that is where their problem will also start... I don't believe a law must necessarily create a commission... If you don't fund a rights commission... you are subjecting them to [government] control... There's no way they can be independent.

On his part, KI4 contends that '...there was... a healthy suspicion on what the bill wants to achieve... would it provide some protection to deviants... There was no government ownership of the idea... engagement fell short... Harmonization and coordination... should have been done before writing the law.'

KI8 was very clear that the Bill was always bound to fail because it attempted to 'transfer existing agencies' mandates to the Human Rights Commission without proper technical expertise.'

Be that as it may, a few KIs, especially KI5, KI6, KI7, and KI10, express very strong support of a similar legislative initiative as one of the best means of moving digital rights protection forward in Nigeria. According to KI6, for example,

I'm absolutely in support of having a specific legislation which removes any

ambiguity... A constitutional amendment would be helpful... We lack phrases like ICCPR's 'any other media' in our Constitution... which was why the Digital Rights and Freedom Bill would have been a huge benefit.

4.2.4. The Need for a National Action Plan on Digital Rights

There is a clear divide among the stakeholders regarding the need for a National Action Plan (NAP) on digital rights. While 6 of the KI are strongly in support, 4 opposed the idea of a NAP. KI4, KI6, KI7, KI8, KI9, and KI10 belong to the former category. According to KI9, for example, a NAP

It is needed because it is going to... give the country a focus... avoid duplicating mandates... set a roadmap... map... stakeholders... [including] the judiciary... National Assembly... NHRC... NITDA... sub-national actors... The [NAP] will bring together laws, policies, programs... and most importantly the metrics... timelines... key performance indicators.

Similarly, KI7 expressed strong support for it, where he stated that

Absolutely. So I. I don't believe in either or... I believe in. And I believe that even if you have a law, you should have an action plan to introduce, implement, monitor, and ensure that the law succeeds. So if you say, for example, that you want to have a national action plan on digital rights in Nigeria, I absolutely fundamentally believe in that. The ideal is that the national action plan is built on existing legislation, policies, or guidelines. But if they don't exist, then the guideline, I mean the national action plan itself, can then suggest.

Meanwhile, KI1, KI2, KI3, and KI5, who are not in support of it, provide several justifications too. For example, KI states that:

But again, we need to think about things in the context in which they exist. What has the history been with documents like this? We've had legacy documents like this in the past. How many of them has

really been transformational? And that's not me speaking as a pessimist, but you also realize that in two years we can or cannot have a change of government. This can become secondary. But even if there is no change of government, it also means it may not be a priority for the government. So again, the question then becomes, should we rather take a different approach to things rather than having another aspirational document? It's not the first time we're having documents with an implementation timeline.


Furthermore, KI5 sees a NAP as a 'potentially redundant administrative document' and cited Nigeria's 'implementation record with national plans [as] historically poor'. In a similar light, KI1 worries about creating 'another ineffective academic document without practical implementation.'

4.2.5. Design and content of a potential NAP on Digital Rights

The 6 KIs that are in support of the idea of an NAP also shared their perspective on the design, content, stakeholders, and monitoring of a NAP on Digital Rights. KI 6 contends that a proposed NAP should be a living document with a short-term cycle of '2-3 years, and then you review and renew'. KI 7 shared five crucial elements that must be contained in a proposed NAP. According to the KI, 'clear objectives, responsibility assignment, timeline specification, implementation methodology, and measurement criteria.' Although KI1 was not in support of the NAP initiative, s/he still suggested that if the idea should be pushed forward, then it should be 'rights-based' and 'connect digital rights to existing constitutional protections rather than creating entirely new rights.'

KI9 provided elaborate details of the structure of such an NAP. The KI contended that

The document should... give a background... [and] a contextual exposition... whether there are laws, programs, [and] what are Nigeria's [international/regional] obligations... The action plan... will... map...



stakeholders... you may be surprised [how many are relevant]... bring [laws, policies, programs] on board... and then most importantly the metrics... [with] timelines...

Furthermore, according to KI9, the NAP should '...avoid duplicating mandates... and possible clash... either with the constitution or causing any sort of confusion.'

CHAPTER 05

Analysis and Discussion

The study assessed the need for a National Action Plan on Digital Rights in Nigeria while also evaluating the legal, policy, and institutional framework and empirically examining the people's perception and experiences of digital rights protection. The discussion will also proceed thematically under the following headings: perception, priorities, and experiences on digital rights; adequacy of the legal and policy framework; institutional framework; a sui generis digital rights law; a NAP as a way forward; and what a NAP on digital rights should prioritize. Each of these themes will now be discussed extensively below.

5.1. Perception, Priorities, and Experiences on Digital Rights

The importance of digital rights is increasingly being acknowledged in the legal, policy, and academic landscape in Nigeria.⁹² This growing recognition is evident in the rising number of relevant laws and policies in recent years. The recent enactment of the Nigeria Data Protection Act, the NITDA's Code of Practice for Interactive Computer Service Platforms/Internet Intermediaries, and the current efforts toward the Online Harm Prevention Bill are all indications of the changing landscape and arguably an increasing appreciation of the significance of digital rights. However, there is a need to point out that it is not only about what is happening on paper. The question remains, what are the people's perception, priorities, and experience on digital rights? Do they align with the increasing legal and policy efforts to protect such rights? Indeed, public perception and lived experiences are critical to this discourse.

The first issue is, do people understand what the concept of "digital rights" is and why it is important to define and describe it as a distinct

concept? From the interviews and surveys, the concept of digital rights is broadly understood as the online projection of constitutionally protected rights, including the rights to privacy, freedom of expression, access to information, and access to the internet. Several KI understood digital rights as the online dimension of existing human rights, which require special recognition and operational safeguards in today's rapidly changing online world. KI4, for example, in describing digital rights, noted the absence of a single framework which "spells out the gamut" of digital rights and how they are protected, while noting that current practices rely much more on constitutional inference and sectoral laws rather than an explicit regime. KI7 went further to state that using the concept of "digital rights" in a law is itself a strategic choice because Nigerian courts, regulators, and law enforcement tend to respond to "named" norms. The survey responses show that people have a good understanding of what digital rights are, and by that, one could argue that they also appreciate why they should be described with a distinct term. In the survey, 0% of the respondents had no idea of what digital rights are, as against 51.5%, 61.2% and 38.8% think

92 White Paper on the Framework for an Online Harms Protection Bill in Nigeria <https://nitda.gov.ng/wp-content/uploads/2024/12/Updated-OHP-WHITE-PAPER-copy-compressed.pdf>

digital rights are all about the right of access to the internet, right to data privacy, and right to freedom of expression online. Furthermore, when asked how important they think digital rights are, an overwhelming majority (78.8%) agree it is very important, as against 3% who think it is not important at all. This confirms the initial assumption that Nigerians understand the concept of digital rights and their importance today.

Regarding priorities on digital rights, privacy and data protection come top among the other digital rights. Many of the KIs placed this right above the others, indicating Nigeria's need (KI2 and KI8). Some of the KIs also acknowledge the NDPA 2023 as a major step, but not without challenges in terms of awareness and redress. The survey respondents also confirmed this fact, where they ranked privacy and data protection as the most important digital right and even a top priority for a NAP. Accordingly, an overwhelming 82.4% consider privacy and data protection to be the most important digital rights. With 47.3% each confirming the right to internet access and the right to freedom of expression online as the next most important rights. Yet again, none of them had no idea about the most important digital rights, which confirms a high level of awareness. Other salient rights, by no means less important, are the right to protection from online harassment/tech-facilitated gender-based violence (TFGBV) and digital literacy. These were pointed out by KI10. The above is also partly a reflection of continental priorities, as the African Declaration on Internet Rights and Freedoms stresses these rights in addition to non-discrimination as key principles and core values that should be translated into national law and policy.⁹³

The next issue is the lived experience of Nigerians. The survey does not really paint a good picture regarding the experiences of

people with digital rights violations. 47% have witnessed platform restrictions/shutdown, while about 34% report experiencing online harassment like hate speech and doxing. 30% reported misuse/exposure of personal data, while 19% have experienced arrest or detention as a result of comments made online. This is probably why about 53.3% only sometimes feel safe when expressing themselves online, and 20% and 12.7% respectively rarely or never feel safe expressing their opinions online. The KIs help explain these numbers. For example, KI6 and KI1 mentioned the Twitter suspension and End SARS protests as a watershed in public consciousness on arbitrary restrictions and shutdown threats. That is what the ECOWAS Court, in its 2022 judgement, rebuked the government of Nigeria, declared the suspension unlawful, and ordered the government to align its framework with freedom of expression standards.⁹⁴ All these are part of the reasons why Nigeria is still considered partly free in the Freedom on the Net 2024 report, with a score of 59 out of 100 countries assessed.⁹⁵ This is unlike countries like South Africa that are considered free.⁹⁶

Interestingly, despite the prevalence of digital rights violations, the concept of digital rights is not strange to Nigerians. It is therefore surprising that despite the high number of digital rights violations, 41.8% of the survey respondents never made any report. A likely reason may be that a great number (30.3%) do not know where to report violations. Be that as it may, this situation may also explain the low level of jurisprudence on digital rights in Nigeria, as noted by KI1. For the courts to engage with such matters, reports must be made, and individuals must be willing to pursue legal action – something that can be both daunting and expensive. So far, CSOs like the Digital Rights Lawyers Initiative (DRLI) have played a significant role by pursuing such cases as public

93 African Declaration on Internet Rights and Freedoms https://africaninternetrights.org/sites/default/files/African-Declaration-English-FINAL.pdf?utm_source=chatgpt.com; See also Declaration of Principles on Freedom of Expression and Access to Information in Africa <https://achpr.au.int/en/node/902>

94 SERAP v. Federal Republic of Nigeria https://globalfreedomofexpression.columbia.edu/cases/serap-v-federal-republic-of-nigeria/?utm_source=chatgpt.com. See also Judgment: ECOWAS Court finds Nigeria violated freedom of expression with twitter blocking https://www.mediadefence.org/news/ecowas-nigeria-twitter-blocking/?utm_source=chatgpt.com

95 <https://freedomhouse.org/country/nigeria/freedom-net/2024#B>

96 <https://freedomhouse.org/country/south-africa/freedom-net/2024>

interest cases. However, KI1 confirmed that this has not been easy, and the lack of funding to pursue many of these cases has been a serious obstacle.⁹⁷

5.2. Adequacy of the Legal and Policy Framework

While there are multiple laws and policies related to digital rights in Nigeria, their adequacy is, however, questionable. As rightly pointed out by some of the KIs, some of the significant laws merely seek to give the government powers over the people rather than protect rights. For example, in reaction to the perceived ineptitude of Twitter, the NITDA Code of Practice for Interactive Computer Service Platforms/Internet Intermediaries⁹⁸ was made to ensure greater control over the digital platform, which may be used to restrict free speech. Besides, some of these norms only exist in soft law form and are not binding. These are some of the reasons why the jurisprudence on digital rights (apart from data privacy) is arguably thin, as noted by KI1. It is important to stress, however, that the issue of limited jurisprudence on digital rights is not a Nigerian issue. For example, Bart Custers noted regarding the European Union that 'There has been very little litigation to date on many of these [digital rights] issues. Technology often seems to develop faster than the body of case law. As a result of this legal uncertainty, the extent to which citizens are protected is not clear.'⁹⁹

Although awareness of the laws and policies on digital rights is high, 41.8% of the survey

respondents have never reported a violation despite many of them witnessing one. This pattern suggests (though it does not prove) shortcomings in the legal and policy framework. This view is consistent with the 48.5% of the survey participants who do not trust the government to protect their digital rights. This is not surprising considering the proliferation of social media repressive laws and policies lately, including the Protection from Internet Falsehood and Manipulations Bill (Anti-Social Media Bill) 2019.¹⁰⁰ This explains why just 53.3% of the survey respondents only sometimes feel safe expressing their opinions online, while 20% rarely feel safe.

One of the main reasons why the KIs who are of the view that the legal and policy framework is inadequate is that, apart from aspects of freedom of expression online (presumably protected by the NITDA Code) and the right to data privacy, all other rights are virtually unprotected. Some of the critical rights in that are left unprotected include the right to freedom of peaceful assembly online, anonymity, freedom of information online, the right to create public knowledge,¹⁰¹ and, more recently, rights in the algorithmic era, such as the right to explainability and transparency.¹⁰² Regional frameworks, such as the Declaration of Principles on Freedom of Expression and Access to Information in Africa (Revised 2019), have also proved unhelpful given the constitutional encumbrance associated with ratification and domestication.¹⁰³ Besides, the Declaration is also a soft-law mechanism with its own limitations.

Assessing the adequacy of the legal and policy landscape on digital rights will also involve

97 Many of the laudable initiatives of the DRLI in litigation have been reported in S Okedara, O Babalola & I Chukwukelu Digital Rights in Nigeria: Through the Cases (2022, Noetico Repetum Inc. & Global Macron Pace Limited, Lagos)

98 NITDA Code of Practice for Interactive Computer Service Platforms/Internet Intermediaries <https://nitda.gov.ng/wp-content/uploads/2022/06/Code-of-Practice.pdf>

99 B Custers 'New Digital Rights: Imagining Additional Fundamental Rights for the Digital Era' (2022) 44 Computer Law & Security Review 105636

100 The NDPA Amendment Bill SB. 648/SB. 650, which mandates physical offices in Nigeria for social media platforms, data controllers, processors, and even bloggers, is also considered to be one such social media repressive law. It stipulates that any entity that fails to comply will be barred from operating.

101 These rights can be found in the Digital Rights and Freedom Bill, Sections 3 to 12

102 See generally L Lane 'Clarifying Human Rights Standards through Artificial Intelligence Initiatives' (2022) 71(4) International & Comparative Law Quarterly 915-944. See also D Khazanchi & M Saxena 'Navigating Digital Human Rights in the Age of AI: Challenges, Theoretical Perspectives, and Research Implication' (2025) Journal of Information Technology Case and Application Research <https://doi.org/10.1080/15228053.2025.2452028> © 2025 The Author(s). Published with license by Taylor & Francis Group, LLC.

103 Section 12, Constitution of the Federal Republic of Nigeria (As Amended)

questions regarding the extent to which recent initiatives incorporate digital rights. Indeed, KI3, in vehemently rejecting the idea of both a special digital rights law and a National Action Plan, argued that digital rights are mainstreamed into current policies and frameworks. A quick overview of a few of these recent strategies shows that just limited reference is made to digital rights. For example, the National Action Plan on the Promotion and Protection of Human Rights (2024-2028) only considers the right to affordable internet access for all citizens as part of the right to freedom of expression.¹⁰⁴ Similarly, they only mention the need to assign responsibilities and roles to specific government institutions for data and privacy protection without more.¹⁰⁵

To conclude, while there are multiple laws and policies on aspects of digital rights, the framework remains fragmented, weak in rights protection, and tilted heavily towards state control. All these have implications for trust and confidence in the legal and policy framework, as confirmed by the survey data.

5.3. Institutional Framework

Just like the legal and policy framework, multiple institutions have mandates regarding digital rights, as noted by many of the KIs. NITA, NDPC, NCC, NBC, CBN, and NIMC all play a role that touches on digital rights, but without a clear delineation of responsibilities. Coordination, therefore, is a challenge. Although KI8 argues that issues that wrongly come before one of the government agencies are quickly redirected to the right agency, the degree of effectiveness of this process is still in doubt. There is also an overall lack of confidence in institutional mechanisms by citizens, as 41.8% of the survey participants chose not to report because they didn't think it would help. This is so despite 70.3% of the participants being

aware of government agencies responsible for enforcing digital rights. There is also disharmony or distrust between these institutions and CSOs, so the institutions, as revealed by KI5, are a reason for the failure of the Digital Rights and Freedom Bill.

5.4. A sui generis digital rights law

The question of whether there is a need for a special law to protect digital rights is a very controversial one. As the interview results suggest, the Key Informants are divided on this issue. KI4, KI6, and KI9 are clear that while the Constitution of the Federal Republic of Nigeria guarantees fundamental rights like privacy and freedom of expression, these provisions were not drafted with the digital age in mind, thereby creating a significant protection gap. Accordingly, to KI 6, the ambiguity has led to a legal environment that is described as “negative” and tilting more heavily in favour of criminalizing online activities rather than upholding rights. KI7 specifically noted that in the Nigerian context, ‘judges only respect cybercrime because there’s a law on cybercrime.’ Without a named ‘digital rights’ law, the issues would not get the desired attention. KI5 further opined that even after the amendment of section 24 of the Cybercrimes Act, authorities continue to use it to arrest people for online speech, demonstrating that without clear, rights-affirmative law, state actions will continue to exploit these gaps. In contrast, other KIs warn against a law that will create a “super-regulator” or duplicate existing mandates. KI3, also, contends that multiple new laws create compliance confusion and bureaucratic blots.

The implication of the foregoing is that there is convergence by the KIs on the problems (i.e., fragmentation and weak remedies) and divergence on the tool to be used to overcome the problems (i.e., making a new law or

¹⁰⁴ National Action Plan on the Promotion and Protection of Human Rights (2024-2028) 48. See [https://www.nigeriarights.gov.ng/files/nap/NAP%20FINAL%2014%20January%202024%20\(1\)%20New.pdf](https://www.nigeriarights.gov.ng/files/nap/NAP%20FINAL%2014%20January%202024%20(1)%20New.pdf). It naturally provides for the right to privacy, although it makes reference to the Nigeria Data Protection Regulation Act 2019.

¹⁰⁵ National Digital Economy Policy and Strategy (2020-2023) <https://nitda.gov.ng/wp-content/uploads/2020/06/National-Digital-Economy-Policy-and-Strategy.pdf>

reforming an existing one). Meanwhile, some of the responses to the open-ended question regarding how to move the protection of digital rights forward explicitly call for enacting the Digital Rights Law and strengthening/enforcing data protection rules.

It is important to stress that the debate over whether a sui generis law is necessary for digital rights protection goes beyond the Nigerian context, and it is tied to a broader issue of whether or not digital rights should be considered a new generation of independent rights or an integral part of existing human rights. Indeed, the United Nations' position that the same human rights that people have offline should be enjoyed online is part of the reasons for a common conception that digital rights are part of existing rights and should not be established with a new regime.¹⁰⁶ This has been described as the normative-equivalence paradigm.¹⁰⁷

The point remains that the rapid adoption and use of the internet should also be acknowledged in terms of influence to be able to generate its own normative force. Over time, the internet has become an essential and integral part of the contemporary lives of people around the world, including in developing nations like Nigeria, and it is directly or indirectly affecting every aspect of society and human.¹⁰⁸ This development will consequently be associated with a number of threats and risks, including unique human rights challenges. The acknowledgement of such risks and threats is the reason why the internet moved beyond the idea of a space beyond government regulation.¹⁰⁹ In view of these,

there is a need for recognition of independent human rights associated with the online world, which has been argued to be conceptually and practically different from the offline world.¹¹⁰ As rightly noted by Dror-Shpoliansky and Shany

In the digital environment, new needs and interests present themselves, and pre-existing threats and challenges assume radically different implications. Such features render tenuous the 'fit' between offline human rights and the specific protections required in cyberspace. It is for this reason that the normative equivalency paradigm was sharply criticized by the United Nations (UN) special rapporteur on the right to privacy, who argued that it cannot afford adequate protection for the right to privacy in the digital age."¹¹¹

All the above are just theoretical debates that may not make much sense to the ordinary man on the streets, who just want to enjoy basic digital rights protection. The 78.8% survey participants who feel digital rights are very important do not care as much about how it is protected, provided the protection system is efficient. For the Key Respondents, KI5 and KI7 were very clear about the added-value of special digital rights laws. According to them, given the unique nature of the Nigerian society, there is a need to have these things written down in a binding document so that the people can have something to hold onto. A sui generis law will also assist civil society in its advocacy drive. Such a law will also simplify the task of the judiciary in terms of having the necessary tools to work with. Beyond all these, it is important to

106 See United Nations General Assembly Resolutions GA Res. 68/167, 18 December 2013, para. 3; GA Res 69/166, 18 December 2014, para. 3; GA Res.71/199, 19 December 2016, para. 3; GA Res. 73/179, 17 December 2018, para. 3. See also Human Rights Council Resolutions 20/8, UN Doc. A/HRC/RES/20/8, 5 July 2012, at 2, para. 1; HRC Res. 26/13, UN Doc. A/HRC/RES/26/13, 26 June 2014, at 2, para. 1; HRC Res. 32/13, UN Doc. A/HRC/RES/32/13, 1 July 2016, at 3, para. 1; HRC Res. 38/7, UN Doc/HRC/RES/38/7, 5 July 2018, at 3,

para. 1.

107 D Dror-Shpoliansky & Y Shany 'It's the End of the (Offline) World as We Know It: From Human Rights to Digital Human Rights- A Proposed Typology' (2021) 32(4) The European Journal of International Law 1251

108 D Dror-Shpoliansky & Y Shany 'It's the End of the (Offline) World as We Know It: From Human Rights to Digital Human Rights- A Proposed Typology' (2021) 32(4) The European Journal of International Law 1251

109 D Dror-Shpoliansky & Y Shany 'It's the End of the (Offline) World as We Know It: From Human Rights to Digital Human Rights- A Proposed Typology' (2021) 32(4) The European Journal of International Law 1251

110 Y Zhang & S Jiang 'The Concept of Digital Human Rights and Its Reshaping of Basic Rights' (2023) 22(5) Journal of Human Rights 973-993.

111 D Dror-Shpoliansky & Y Shany 'It's the End of the (Offline) World as We Know It: From Human Rights to Digital Human Rights- A Proposed Typology' (2021) 32(4) The European Journal of International Law 1252

stress that the uniqueness of digital rights calls for specific elucidation in a special instrument. As much as we can make an argument for data protection law being an elucidation of the constitutional right to privacy, we must also consider a digital rights law to be an elucidation of the fundamental rights in the Constitution.

There are several crucial lessons to learn from the processes leading to the Digital Rights and Freedom Bill and the subsequent refusal of the President to assent to the Bill. One of the critical lessons K5 notes is the reluctance of government agencies to support any policy initiative coming from civil society. The stated reasons for the President's refusal to assent to the Bill were that

it seeks to cover too many technical subjects in one text and in the process fails to address any of them exhaustively. These areas include surveillance and data protection, lawful interception of communications, data protection and retention, etc, which are currently the subject of various bills pending at the National Assembly.¹¹²

K15 observes that the actual reasons for declining the Bill were that various government agencies felt threatened by a civil society-owned initiative. Therefore, the felt Civil Society and the National Human Rights Commission were attempting to usurp their powers. K4, on the other hand, was of the view that it was a result of insufficient public consultation, especially with relevant government agencies. This fact was rejected by K14, contending that the Bill underwent extensive public consultation and relevant government agencies took part in the process. The thinking and reluctance of government agencies to support such an initiative was expressed by K13, who noted that an initiative such as the above creates another layer of bureaucracy for government agencies. From the foregoing, it is clear that the failure of the bill was not due to a single issue but a combination of institutional resistance, perceived exclusion, and bureaucratic inertia.

Although there is now a move towards enacting an Online Harm Prevention Bill as an executive Bill by NITDA,¹¹³ this does not arguably substitute for a Digital Rights Law. While the former manages harmful content and platform duties, the latter guarantees rights, limits state power, and ensures judicial remedies. Invariably, the Online Harm Prevention Bill is not a human rights instrument.


5.5. A National Action Plan as a way forward

While an overwhelming majority (94.6%) of the public survey is in support of a National Action Plan as a way forward to the current digital rights protection conundrum, opinions among the Key Informants vary. In summary, those who are not in support believe that a NAP on digital rights will just be another idle document (K12) without any potential influence (K11), cannot help resolve the critical issues in the digital rights landscape (K15), or will add further financial burden to the government (K13). Those who support a NAP contend that a NAP can be a viable tool for building consensus and ownership (K14), a pathway to a law (K17), and an opportunity to create a "clear framework on digital rights protection" that is fundamentally "human centric" (K110).

Both sides advance strong arguments, but not taking any action is not an option. Nigeria cannot remain in a holding pattern while digital rights are at risk. The current patchwork - partial frameworks, inter-agency turf conflicts, and gaps in coverage - falls short, and the future of a comprehensive law is bleak. We therefore need a practical way forward, not inaction. Indeed, the evidence from both the public and experts suggests that while a standalone NAP is not a panacea, it represents the most viable path forward in Nigeria's current digital rights climate. It is not simply about creating another document but about initiating a much-needed

¹¹² Channels 'Buhari Declines Assent to Digital Rights and Freedom Bill, Four Others' <https://www.channelstv.com/2019/03/20/buhari-declines-assent-to-digital-rights-and-freedom-bill-four-others/>

¹¹³ White Paper on the Framework for an Online Harms Protection Bill in Nigeria <https://nitda.gov.ng/wp-content/uploads/2024/12/Updated-OHP-WHITE-PAPER-copy-compressed.pdf>



process of national dialogue, coordination, and consensus-building.

Other options provided seem impractical for a situation demanding immediate or rapid action. For example, KI3 forcefully argues against a new standalone plan, suggesting that proponents of the idea of a NAP should 'find a way to include these things in existing action plans'. He points out that this would streamline monitoring, evaluation, and resource allocation, reducing bureaucratic fatigue and making implementation more feasible. While it is unclear to see how easy such a streamlining process would be, the process would appear more complicated than coming up with a new action plan altogether. Besides, there are different stakeholders involved in different action plans. Therefore, those who participated in the action plan on a particular subject may not be able to provide useful insight for an action plan on another subject. It needs to be reiterated that digital rights are a complex subject requiring the involvement of not only legal professionals but also IT specialists and other specialists.

5.6. What a National Action Plan Should Prioritize

There have been incisive suggestions from both the survey and interview respondents on what a National Action Plan on Digital Rights should include. This is not surprising considering the recent proliferation of National Action Plans in related areas, as previously mentioned. However, this is not to say that all National Action Plans have a similar structure or content. That is why the study focused on identifying key priorities, rather than prescribing specific content for the National Action Plan.

The most important priority for a proposed NAP on digital rights, as noted by KI1, KI6, and KI7, is that it must adopt a rights-based approach. This is very crucial, considering that the protection of digital rights is at the core of such initiatives. Although KI3 believes that the economic-based approach should be a priority and human rights can be integrated within the broader effort of wealth creation for the people and prosperity for the nation. According to KI3, digital rights should be framed in the context of 'supporting

security, innovation and investor confidence', contending that proposals are more likely to succeed if they align with the government's focus on economic growth. The ideas of KI3 are no doubt challenging for several reasons, and the most important is that prioritizing economic outcomes without a strong human rights foundation risks marginalizing vulnerable groups and overlooking the core values that digital rights seek to protect.

Furthermore, most of the KIs that support a NAP suggest that it should prioritize a pragmatic, multi-stakeholder approach, which focuses on building consensus, clarifying institutional roles, and establishing a robust mechanism for accountability.

Specifically, a proposed NAP, according to a cross-section of some of the KI is that must incorporate the following:

- a. **Overarching Strategy and Approach:** Since there were a few KIs who do not support yet another policy document that may remain unimplemented, it is important that the proposed NAP's core strategy should not exist as a standalone document but serve as a dynamic framework toward coordination, advocacy, and eventual legislative reform. Several suggestions were provided by the KIs in this respect, but all were strongly in support of the fact that the strategy should be a pathway towards a law. Thus, the argument is that the NAP should be framed as a strategic roadmap, not an end goal. KI4 suggests that a NAP can be 'the strategy to get the bill done' by identifying stakeholders, highlighting issues and building buy-in. KI7 contends that the strategy should be a necessary precursor to effective legislation and implementation, noting that 'the law is the what to do, the plan is the how to do it.'
- b. **Identify and outline the core digital rights clearly:** These rights should not just be named, but they should be tied to constitutional guarantees and Nigeria's international law commitments, and must also be expressed in terms of the digital context. The survey respondents


have prioritized these rights. Accordingly, 85.5%, 60% and 52.7% think that the protection of online privacy, the right to affordable and accessible internet, and combating online harassment must be given priority. Other comparatively less important rights include regulating government surveillance, enhancing digital literacy, and ensuring more accountability for tech platforms. Identifying the rights, according to KI7, meets the requirement of 'name it to enforce it' concern that judges and agencies respond to explicitly framed norms.

- c. Institutional coordination and oversight: Key Informants, especially those from government and civil society, agree on resolving institutional and interagency overlaps, especially those between NDPC/NITDA/NCC/NHRC/ONSA. This may be achieved by (i) assigning lead-agency roles by functions, (ii) mandating MoUs and joint protocols for investigations and enforcements, and (iii) establishing independent review and reporting for issues such as surveillance, content moderation, and shutdown decisions. (KI3, KI8 and KI9). Some form of coordination is already taking place, especially by some of the government agencies. For example, KI6 noted how they transfer cases to the relevant agencies and even follow up if a matter comes to their agency wrongly. These things should be institutionalized and clarified in a proposed NAP for better coordination.
- d. Close compliance and remedy gaps: As mentioned earlier, most survey participants reveal low reporting of digital rights violations and low trust in existing protection measures. This implies that a NAP must incorporate measures to overcome this significant challenge. A proposed NAP should contain a

simple, public-facing reporting channel, (ii) provide timelines for remedies, (iii) require government and platform transparency and due process, and (iv) invest in judicial capacity-building on digital rights adjudication. The work of Paradigm Initiative, together with the leadership of some of the courts in Nigeria, is quite noble and noteworthy, and could also be referenced.¹¹⁴

- e. Inclusive stakeholder participation and ownership: Some of the KIs strongly believe that one of the reasons for the failure of the Digital Rights and Freedom Bill was the absence of genuine government ownership (KI4, KI5, KI8). This fact has implications for a proposed NAP- it must prioritize broad, inclusive, and early engagement to avoid this pitfall. In this regard, the NAP must secure government co-ownership from the start according to KI4. This fact is confirmed by the survey, where 38.8% and 32.1% think government agencies and citizens/digital users should be involved in developing a NAP. In addition, KI4 also recommended that security agencies, the media, researchers, and international observers be included. To ensure the diversity of stakeholders, KI10 stresses the need for civil society actors representing journalists, women, children, and persons with disabilities. KI2 also emphasized kids' roles in public schools because of the stark difference in perspectives on online harm.
- f. Implementation, monitoring, and accountability: To overcome the challenge of becoming just another 'bulky document', KI9 recommended that the NAP must have a clear, actionable, and enforceable implementation framework. This fact is confirmed by KI7, who contends that it must provide clear, measurable, and time-bound actions. KI7 unequivocally notes that

¹¹⁴ See the Ikot Ekpen Declaration Resolutions and Commitments on Upholding and Strengthening Judicial Capacity on Digital Rights and Cyber-Governance, May 12-15, 2025. <https://paradigmhq.org/wp-content/uploads/2025/07/Ikot-Ekpen-Declaration.pdf>



'Accountability without accountability, we are joking.' KI4 calls for an 'active stakeholder-led monitoring, evaluation plan with elements of accountability and transparency.' Drawing from the success recorded with the Open Government Partnership model, KI6 recommends that the NAP be 'very short periods,' such as two to four years. He stressed that this will allow for periodic review, adaptation to new technologies, and prevent the plan from being obsolete.

CHAPTER

06

Recommendations

To advance digital rights protection in Nigeria, the study offers the following recommendations focusing on the most pressing challenges.

- Increased Advocacy and Public Enlightenment Campaign by the Civil Society Organizations, including the National Human Rights Commission: This is very significant. For any progress on digital rights in Nigeria, the government must be made to understand what they entail and how important they are for democracy and national development. Digital rights agitations are not anti-government agitation but a call for better protection of human rights in a different context. The government and policymakers should understand that it is not just about trying to ensure connectivity, but also respecting rights when individuals have access. This is indeed an essential task for CSOs, including the NHRC. As shown in this study, since the people's awareness of these issues is relatively high, there is a need to shift focus to the government.

- Establish a Mechanism for Inter-agency Collaboration

Issues of a lack of interagency cooperation also top the list the challenges of digital rights protection in Nigeria. One important step forward is to properly delimit the roles of each of these agencies. Another step is to draw lessons from the United Kingdom and the European Union. In this regard, three options are available. The first is to establish a Nigeria Digital Rights Cooperation Forum, which mirrors

the UK Digital Regulation Cooperation Forum – a body primarily responsible for coordinating cross-cutting digital issues in the UK. This forum can bring together NDPC, NITDA, NCC, NHRC, MoJ, ONSA, and CBN for coordination and joint action. A second option, which is least favoured, is the EU approach of appointing a Digital Services Coordinator as the single point of contact. A third option is the use of a Lead authority/ one-stop shop for cross-cutting cases, just like what the European Data Protection Board does in coordinating cross-border enforcement. Therefore, for multiagency cases, one regulator is designated the lead and forms a joint case team with the support of others.

- The National Action Plan on Digital Rights in Nigeria

Immediately commence the process towards a NAP with a view to harmonizing the varying issues and paving the way for legislation on digital rights.



CHAPTER 07

Conclusion

The study evaluated the necessity or otherwise of a National Action Plan on digital rights in Nigeria, alongside an evaluation of the legal, policy, and institutional landscape on digital rights protection in Nigeria. It starts by trying to understand users' experience on the state of digital rights and their perception of digital rights protection. Unlike other studies in this respect, the current research deployed a mosaic of methodologies beyond mere doctrinal analysis. This is in a bid to be human-centred, factual, evidence-based, and to support policymaking. Contrary to a general assumption, the study finds that many people are aware of what digital rights are all about and desire adequate protection. But they do not trust the structures available enough to enforce their rights. While there are legal and policy frameworks on digital rights, they do not provide comprehensive protection for several reasons. First, apart from data protection, there are no enforceable norms that citizens can rely on in court, especially for the other digital rights. Indeed, the concept of digital rights is like a basket containing several rights of people online, and data protection is only one of them. Arguably, the Constitution provides protection, but it lacks a detailed enunciation of these rights in a way that could assist the courts in interpreting and applying them for comprehensive protection. This is indeed a challenge in a society characterized by a conservative judiciary. Second, most other related laws and policies are at best soft law mechanisms without any binding force. Therefore, in line with global best practice, the idea of legislation that gives life to these rights in Nigeria is imperative. However, given the circumstances surrounding the unsuccessful attempt at the Digital Rights and Freedom

Bill 2019, it is unlikely that such a law is immediately feasible. Besides, other similar initiatives, such as the Online Harm Prevention Bill, may compete with and obstruct the passage of a Digital Rights Law. Additionally, the issue of institutional overlap in the various agencies dealing with issues related to digital rights is another imminent challenge. In light of these findings, the study concludes that a coordinated, intermediate initiative is required to integrate existing efforts and chart a path toward comprehensive and sustainable digital rights protection.

The idea of a National Action Plan is not novel, considering similar initiatives lately, especially with the recent National Action Plan on the Protection and Promotion of Human Rights 2022-2026. While such an initiative is bound to come with certain reservations, considering the fate of similar initiatives, most stakeholders are of the view that this makes a difference if all hands are on deck and civil society is able to ensure a buy-in. This study, however, concludes that a NAP will be meaningful only if it charts a path towards sustainable, enforceable, and comprehensive digital rights protection. Specifically, a NAP would be useful if it could lead to more concrete norms on digital rights. Therefore, the study concludes that a NAP is urgently required as an initial step to bring clarity and coordination into Nigeria's uncoordinated legal landscape on digital rights protection.



References

Academic Literature

Legal Instruments

Policy Documents

APPENDIX I – KEY INFORMANTS INFORMATION

KI No	Name	Designation	Category
I	Olumide Babalola	Managing Partner, Olumide Babalola LP, Ph.D. candidate	Legal Expert/Academic
II	Ridwan Oloyede	Co-founder, Tech Hive; Director, Center for Law and Innovation	Legal Expert
III	Fernandez Marcus-Obiene	Special Assistant to the President on Justice Sector Reforms And ICT/Digital and Innovative Technology	Policy maker
IV	Kasim A. Sodangi	Co-founder & Director. Advocacy for Policy and Innovation (API). Formerly, National Coordinator, Office for Nigerian Content Development in ICT (ONC), NITDA	Legal Expert/ Policy Maker
V	Adegboye Adegoke	Principal, Africa Luminate	Civil society
VI	Edeaten Ojo	Executive Director of Media Rights Agenda	Civil society/Legal Expert
VII	'Gbenga Sesan	Executive Director, Paradigm Initiative	Civil society
VIII	Emmanuel Edet	Ag. Director, Regulation & Compliance Department and Head of the Legal Services, NITDA	Policy Maker
IX	Kabiru Aliyu Elayo	National Human Rights Commission (NHRC)	Policy Maker
X	Amina Salaudeen	Women's Rights and Safety Officer, TechHer	Civil Society

APPENDIX II- INTERVIEW GUIDE

LEGAL EXPERTS, ACADEMICS, POLICY MAKERS, AND CIVIL SOCIETY

SECTION 1: Opening and Background

1. Can you briefly describe your work about digital rights in Nigeria?
2. What do you consider to be the most pressing digital rights challenges in Nigeria today?

SECTION 2: Assessment of Existing Legal and Policy Frameworks

3. How effective are the existing laws, policies, and institutional mechanisms in protecting digital rights in Nigeria?
4. Are there areas of overlap, contradiction, or institutional ambiguity in the current digital rights governance structure?
5. In your opinion, what explains the persistent implementation gaps despite existing instruments and institutions?
6. What is your assessment or comment on the Digital Rights and Freedom Bill (DRFB)?

SECTION 3: Evaluating the Need for a National Action Plan (NAP)

7. Do you believe Nigeria needs a National Action Plan on Digital Rights? Why or why not?
8. What would be the added value or unique contribution of a National Action Plan, as opposed to simply amending existing laws or strengthening institutions?
9. What risks or limitations do you foresee with developing and implementing a NAP in the Nigerian context?

SECTION 4: Design and Content of a Potential NAP

10. If Nigeria were to adopt a National Action Plan, what core components or thematic areas should it include?
11. What principles or values should guide the design of such a Plan to ensure it is rights-respecting, inclusive, and enforceable?
12. Can you identify any global or regional models of National Action Plans or digital rights frameworks that Nigeria can draw lessons from?
13. How should such a Plan be monitored and evaluated? What institutional arrangements would ensure sustainability and accountability?

SECTION 5: Final Reflections

14. What key stakeholder groups must be involved in both the design and implementation of the NAP to make it legitimate and effective?
15. Do you have any final recommendations on how Nigeria can more effectively protect and promote digital rights, whether through a NAP or other mechanisms?

APPENDIX III- SURVEY QUESTIONS

Section 1: Background Information (Demographics)

Purpose: to help in understanding representation across zones and categories.

- | | |
|---|---|
| 1. Age group: | <input type="radio"/> Unemployed |
| <input type="radio"/> 18–25 | <input type="radio"/> Other: _____ |
| <input type="radio"/> 26–35 | |
| <input type="radio"/> 36–45 | 4. Educational level: |
| <input type="radio"/> 46–60 | <input type="radio"/> No formal education |
| <input type="radio"/> 60+ | <input type="radio"/> Primary |
| | <input type="radio"/> Secondary |
| 2. Gender: | <input type="radio"/> Tertiary |
| <input type="radio"/> Male | <input type="radio"/> Postgraduate |
| <input type="radio"/> Female | |
| <input type="radio"/> Other / Prefer not to say | 5. Geopolitical zone: |
| | <input type="radio"/> North Central |
| 3. Occupation: | <input type="radio"/> North East |
| <input type="radio"/> Student | <input type="radio"/> North West |
| <input type="radio"/> Civil servant | <input type="radio"/> South East |
| <input type="radio"/> Private sector worker | <input type="radio"/> South South |
| <input type="radio"/> Self-employed | <input type="radio"/> South West |

Section 2: Perception of Digital Rights

Purpose: to understand how people define or conceptualize digital rights.

- | | |
|--|--|
| 6. What comes to mind When you hear the term “digital rights”? | <input type="radio"/> Right to privacy and data protection |
| <input type="radio"/> Right to access the internet | <input type="radio"/> Right to be free from online harassment |
| <input type="radio"/> Right to data privacy | <input type="radio"/> Right to be forgotten (data erasure) |
| <input type="radio"/> Freedom of expression online | <input type="radio"/> Right to digital education and literacy |
| <input type="radio"/> Freedom from online surveillance | <input type="radio"/> I don't know |
| <input type="radio"/> I don't know | 8. How important do you think digital rights are in Nigeria today? |
| <input type="radio"/> Other (please specify): _____ | <input type="radio"/> Very important |
| | <input type="radio"/> Important |
| 7. In your opinion, which of the following are the most important digital rights? (Select up to 3) | <input type="radio"/> Not sure |
| <input type="radio"/> Right to internet access | <input type="radio"/> Not important |
| <input type="radio"/> Right to freedom of expression online | <input type="radio"/> Not at all important |

Section 3: Awareness of Legal and Institutional Frameworks

Purpose: to gauge familiarity with key instruments like the NDPA or DRFB.

- | | |
|---|---|
| <p>9. Are you aware of any laws or policies in Nigeria that protect digital rights?</p> <ul style="list-style-type: none">○ Yes○ No○ Not sure <p>10. If yes, which of the following are you familiar with?</p> <ul style="list-style-type: none">○ Nigeria Data Protection Act 2023 (NDPA)○ Digital Rights and Freedoms Bill○ Nigerian Constitution (as it relates to online freedom)○ Cybercrimes Act 2015○ I have heard of them but don't understand them | <p>○ I don't know any</p> <p>11. Are you aware of any government agency responsible for enforcing digital rights?</p> <ul style="list-style-type: none">○ Yes○ No○ Not sure <p>12. If yes, which ones?</p> <ul style="list-style-type: none">○ Nigeria Data Protection Commission (NDPC)○ National Information Technology Development Agency (NITDA)○ NCC○ NHRC○ I'm not sure |
|---|---|

Section 4: Experience and Access (Implementation)

Purpose: to document practical experiences of rights enjoyment or violation.

- | | |
|--|---|
| <p>13. Have you ever experienced any of the following online in Nigeria? (Select all that apply)</p> <ul style="list-style-type: none">○ Social media account being taken down without reason○ Government surveillance or monitoring○ Internet shutdown or throttling○ Online harassment (e.g., hate speech, doxing)○ Exposure of personal data without consent○ I have not experienced any○ Prefer not to say <p>14. Do you feel safe expressing your opinions on digital platforms (e.g., social media, blogs)?</p> <ul style="list-style-type: none">○ Always | <p>○ Sometimes</p> <p>○ Rarely</p> <p>○ Never</p> <p>15. Have you ever tried to report a digital rights violation?</p> <ul style="list-style-type: none">○ Yes, to government○ Yes, to a CSO○ No, I didn't know where to report○ No, I didn't think it would help○ No, other reason: _____ <p>16. Do you trust the government to protect your digital rights?</p> <ul style="list-style-type: none">○ Yes○ No○ Not sure |
|--|---|

Section 5: Expectations and Policy Preferences

Purpose: to explore what people want from a national action plan.

- | | |
|---|--|
| <p>17. Do you think Nigeria needs a National Action Plan on digital rights?</p> <ul style="list-style-type: none">○ Yes○ No○ Not sure <p>18. What should a National Action Plan on Digital Rights prioritize? (Select up to 3)</p> <ul style="list-style-type: none">○ Affordable and accessible internet for all○ Protection of online privacy○ Combating online harassment and hate speech○ Regulating government surveillance○ Enhancing digital literacy○ Clear laws on internet shutdowns | <ul style="list-style-type: none">○ More accountability from tech companies <p>19. Who do you think should be involved in the development of a National Action Plan? (Multiple choice)</p> <ul style="list-style-type: none">○ Government agencies○ Civil society organisations○ Tech companies○ Academic institutions○ Citizens/digital users <p>20. Do you have any suggestions on how digital rights can be better protected in Nigeria?</p> <ul style="list-style-type: none">○ (Open-ended comment box) |
|---|--|

