AN ASSESSMENT OF THE SCOPE AND ENFORCEMENT OF DATA SUBJECT RIGHTS UNDER NIGERIAN DATA PROTECTION REGIMES.

By Dolapo Dorcas Oyawole[1]

NBA, IKEJA || dolawuyi.od@gmail.com

[1] Dolapo Dorcas Oyawole; NBA Ikeja; dolawuyi.od@gmail.com

Abstract

This research provides a comprehensive assessment of the scope and enforcement of data subject rights under Nigeria's data protection regimes, analysing the pivotal legal transition from the Nigeria Data Protection Regulation (NDPR) of 2019 to the more robust Nigeria Data Protection Act (NDPA) of 2023. It acknowledges the global trend toward stronger data protection, driven by the recognition of digital rights as fundamental human rights, and positions Nigeria's recent legislative efforts within this movement. The study investigates the legal provisions of the NDPA, which granted key rights such as the right to be informed, the right to access, and the right to erasure, and examines the establishment of the Nigeria Data Protection Commission (NDPC) as the primary enforcement body. It identifies a critical gap between the law's comprehensive framework and its practical implementation. The research will discuss significant challenges to effective enforcement, including the NDPC's institutional capacity, a widespread lack of public awareness, the high cost and complexity of judicial redress, and the practical difficulties of enforcing the law extraterritorially against foreign companies. It concludes that while Nigeria has a strong legal foundation for data privacy, the true measure of its success lies in overcoming these systemic challenges. The study offers targeted recommendations for policymakers and the NDPC to enhance institutional capacity, improve public education, and streamline enforcement mechanisms, thereby ensuring that the rights of data subjects are not just codified but are effectively protected and enforced in practice.

Keywords: Data Privacy, Data Subject, Data Subject Rights, Enforcement, NDPR, NDPA.

1.0 INTRODUCTION

The increasing digitalization of societies has brought the issue of data privacy and protection to the forefront of global legal and policy discourse. Nigeria, Africa's largest economy and a major hub for technological innovation, has not been an exception to this trend. With the rapid growth of the digital economy and the proliferation of data-driven services, the need for a robust legal framework to protect the fundamental rights of individuals concerning their personal data has become paramount.

Before 2019, the initial legal framework on data protection principles in Nigeria was fragmented, with the right to privacy primarily enshrined in Section 37 of the Constitution of the Federal Republic of Nigeria 1999 (as amended) (the Constitution), coupled with other Nigerian laws that have data protection provisions such as the Consumer Code of Practice Regulations 2007, Freedom of Information (FOI) Act 2011, Cybercrime (Prohibition, Prevention, etc.) Act 2015, and the National Identity Management Commission (NIMC) Act 2007.

However, a more comprehensive data protection regime began with the issuance of the Nigeria Data Protection Regulation (NDPR) of 2019. The NDPR was a significant step, as it introduced key principles for data processing, such as consent, data minimization, and accountability, and established the rights of data subjects. This was the first comprehensive legal framework in Nigeria designed to protect personal data. [2] It was issued by the National Information Technology Development Agency (NITDA) in January 2019 to safeguard the rights of individuals and foster a secure digital environment.[3] Although it has been superseded by a new law, it laid the foundation for Nigeria's modern data protection regime.[4]The NDPR, while a foundational document, was a subsidiary regulation, which created questions about its enforcement and overall legal force. Recognizing the need for a more robust and comprehensive legal framework, the Nigerian government enacted the Nigeria Data Protection Act (NDPA) in June 2023 and established the Nigeria Data Protection Commission (NDPC) to serve as an independent regulatory body for the Act. This new legislation marks a pivotal shift, moving data protection from a regulatory guideline to a substantive legal right with significant penalties for non-compliance. It also clarifies key concepts and aligns Nigeria's data protection regime more closely with international standards, such as the European Union's General Data Protection Regulation (GDPR).[5]

Despite these legislative advancements, a critical question remains: To what extent are the data subject rights outlined in these regimes being effectively scoped and enforced? This research aims to provide an in-depth assessment of the scope and enforcement of data subject rights under Nigerian data protection regimes. It will examine the legal provisions of both the NDPR and the NDPA, analyse their practical implementation, and investigate the challenges and opportunities in ensuring that individuals can effectively exercise their rights in a fast-evolving digital landscape.

2.0 CONCEPTUAL ANALYSIS

2.1 Data Privacy

Data privacy is the concept that individuals have a fundamental right to control how their personal information is collected, used, shared, and stored.[6] It is a critical component of a digital society, encompassing both the legal frameworks that protect personal data and the ethical responsibilities of those who handle it.

Recent legal and academic discourse has focused on how new technologies, such as artificial intelligence and big data analytics, challenge traditional notions of privacy.[7] This has led to the development of stronger, more comprehensive data protection laws globally.

2.2 Data Subjects

A data subject is a natural person or individual whose personal data is being processed, collected, or stored by an organization. Essentially, if an organization holds your personal information, be it your name, email address, location data, or any other identifier, you are the data subject. This term places the individual at the centre of data protection law, emphasising that they are the rightful owners and have control over their own data.

2.3 Data Subject Rights

Data subject rights are the legal entitlements granted to individuals by data protection laws, such as the NDPA and the GDPR. These rights empower individuals to have control over their personal data and hold data processors accountable. While the specific rights can vary slightly between jurisdictions, they generally include the right to be informed, right of access, right to rectification, right to erasure, right to restrict processing, right to data portability, right to object, and rights related to automated decision-making.

3.0 IMPORTANCE OF DATA PRIVACY

Data privacy is significant in the modern digital age due to technological advancements. Its importance is multifaceted, impacting individuals, businesses, and governments alike. It has helped in building trust and maintaining customer loyalty. Businesses prioritizing data privacy is no longer a mere legal obligation but a business imperative. Studies show that a majority of consumers are

[6] Babalola Olumide, 'The Constitutional Origins of the Right to Privacy in Nigeria' (2025) 2 African Journal on Privacy & Data Protection 83-97.
[7] Indah S, Muh FN, 'Legal Perspectives on Data Privacy and Cybersecurity in the Digital Age' (2025) ResearchGate February 2025 3(2) 471-481.

concerned about their online privacy and would stop doing business with a company if it mishandled their sensitive data.[8]

Data privacy also ensures legal and regulatory compliance. Recently, there has been a surge in comprehensive data protection laws globally. The GDPR has served as a blueprint for new legislation worldwide, including NDPA and various U.S. state laws. Compliance with these regulations is essential to avoid severe financial penalties, lawsuits, and reputational damage from data breaches.[9]

Data privacy safeguards individual rights and freedoms; it gives individuals control over their personal information, protecting them from exploitation, discrimination, and unwarranted surveillance by both commercial entities and governments. It also fosters innovation and economic growth; while seemingly a constraint, data privacy can actually drive innovation. By forcing companies to adopt privacy-by-design principles and develop privacy-enhancing technologies (PETs), regulations encourage a more secure and trustworthy digital environment. This, in turn, boosts consumer confidence and facilitates the free flow of data with trust, which is critical for a well-functioning digital economy and global business operations.[10] Lastly, it mitigates financial and reputational risks; data breaches carry a high financial cost in addition to significant operational and legal expenses.

4.0 THE GLOBAL TREND TOWARD STRONGER DATA PROTECTION LAWS AND NIGERIA'S PLACE IN THIS MOVEMENT.

Prior to the issuance of the NDPR, the legal protection for data privacy was primarily derived from sources like the Constitution, particularly Section 37, which guarantees the privacy of citizens,[11] their homes, correspondence, telephone conversations, and telegraphic communications.[12] While it provided a constitutional right, it was often seen as too narrow and did not explicitly address the collection, storage, and processing of digital data by private entities. Some sectors also had their own rules, such as the FOI Act, while not a data protection law, offered some protection for personal information by exempting certain types of private data from being disclosed to the public by government institutions.[13] This patchwork of laws meant that there was no single legal recourse for individuals whose data privacy rights were violated by a private company. The absence of a

[8] Secureframe. 2025. "110+ Data Privacy Statistics: The Facts You Need to Know In 2025." (Secureframe) <https://secureframe.com/blog/data-privacy-statistics> accessed 30 September 2025
[9] Freshfields, '2025 Data Law Trends' (Freshfields) <https://www.freshfields.com/en/our-thinking/campaigns/data-trends-2025> accessed 17 October 2025.
[10] OECD, 'Privacy and Data Protection' (OECD) <https://www.oecd.org/en/topics/privacy-and-data-protection.html> accessed 17 October 2025.
[11] *Incorporated Trustees of Digital Rights Lawyers Initiative & Ors v National Identity Management Commission* (NIMC), (CA, 2021).
[12] The Constitution of Federal Republic of Nigeria 1999 (amended), Section 37.
[13] Freedom of Information Act (2011)

dedicated data protection authority and a clear framework for enforcement left citizens vulnerable to data misuse.

This inadequacy led to the issuance of NDPR, a groundbreaking and game-changing piece of legislation that represented Nigeria's first comprehensive and modern data protection framework. The NDPR introduced concepts such as: governing principles of data processing,[14] data subject's consent,[15] penalty for default,[16] rights of the data subjects,[17] among others. NDPR signalled Nigeria's commitment to aligning with global data protection standards, most notably the GDPR. It shifted the legal framework from a reactive, constitution-based approach to a proactive, principle-based one.

Recent legislative efforts are increasingly concerned with how new technologies, particularly Artificial Intelligence (AI) and automated decision-making, handle and use personal data. This has led to discussions and new regulations aimed at ensuring accountability and preventing bias in algorithmic systems.[18] This movement is a direct response to the explosive growth of the digital economy, the increasing number of data breaches, and a rising public demand for greater control over personal information.[19] Countries around the world are enacting and amending laws to align with international standards, with the GDPR widely serving as the gold standard for regulatory frameworks.[20]

This global push is characterized by several key features, such as emphasis on data subject rights, strengthened enforcement and penalties protection, extraterritorial reach, and focus on emerging technologies.

Nigeria's journey toward a robust data protection regime reflects its place within this global trend. The NDPR was a pioneering move for an African nation, and it was openly acknowledged to be heavily inspired by the GDPR. However, as a subsidiary legislation, its legal force and enforcement capabilities were limited. Then came the NDPA, which marked Nigeria's definitive entry into the global data privacy movement as a major player. The NDPA significantly strengthens the country's legal framework, establishing an independent regulatory body, the NDPC. It adopts and solidifies core GDPR principles, including data minimization, purpose limitation, and accountability. This alignment is strategic, making it easier for Nigerian businesses to operate internationally and for

[14] NDPR, Part 2 (2.1).
[15] NDPR, Part 2 (2.3). See *Folashade Molehin v United Bank for Africa (UBA),* Suit no FHC/L/CS/2625/2023.
[16] NDPR, Part 2 (2.10).
[17] NDPR, Part 3.
[18] Future of Privacy Forum, 'What to Expect in Global Privacy in 2025' (Future of Privacy Forum 2025) <https://fpf.org/blog/what-to-expect-in-global-privacy-in-2025/> accessed 27 September 2025.
[19] Freshfields, '2025 Data Law Trends' (Freshfields) <https://www.freshfields.com/en/our-thinking/campaigns/data-trends-2025> accessed 17 October 2025.
[20] PwC, Regulatory Alert: An Overview of the Nigeria Data Protection Act 2023 (PwC Nigeria, August 2023) <https://www.pwc.com/ng/en/assets/pdf/regulatory-alert-august-2023.pdf> accessed 17 October 2025; UCC Law Journal. 2025. *A Critical Analysis of the Nigeria Data Protection Act 2023: Elevating Standards to Global Norms*. UCC Law Journal 4 (2): 242-263.

foreign investors to enter the Nigerian market with confidence.[21] Also, NDPA, like the GDPR, has an extraterritorial scope, applying to data controllers and processors outside Nigeria who process the personal data of Nigerian citizens or residents. This brings Nigeria's law into direct alignment with the global standards for data protection.

By adopting a comprehensive, principles-based approach and establishing a dedicated regulatory body, Nigeria is positioning itself as a trustworthy player in the global digital economy, recognizing that robust data protection is a key component of national security, economic growth, and the protection of fundamental human rights.

5.0 DIGITAL RIGHT AS A HUMAN RIGHT

The concept of digital rights as human rights asserts that the fundamental rights and freedoms guaranteed to individuals in the physical world also apply in the digital sphere. This is not about creating entirely new rights but rather applying existing human rights, such as freedom of expression, privacy, and assembly, to the context of the internet and digital technologies.

The global recognition of this principle has gained significant momentum recently, driven by several factors, including the increasing role of technology in everyday life and growing concerns over government surveillance, corporate data exploitation, and the use of technology to suppress dissent. International bodies, national governments, and civil society organizations have all been instrumental in this movement

5.1 International and National Recognition

Recently, there has been a surge in formal recognition of digital rights as human rights through various international and national instruments:

United Nations: The UN Human Rights Council has consistently affirmed the principle that the same rights that people have offline must be protected online. Its reports have focused on critical issues like internet shutdowns, the right to privacy in the digital age, and the human rights implications of new technologies like artificial intelligence (AI).[22] The UN's commitment to a Global Digital Compact further solidified this stance, aiming to create a framework for a more open, free, and secure digital future rooted in human rights.[23]

European Union: The EU has been a leader in this area with its Declaration of Digital Rights and Principles, which outlines a set of commitments to ensure that the digital transition is human-

[21] PlanetWeb, 'Comparison of NDPA 2023 and GDPR: What Nigerian Businesses Should Know' (PlanetWeb, 2025) <https://planetweb.ng/comparison-of-ndpa-2023-and-gdpr/> accessed 7 September 2025.

[22] Office of the High Commissioner for Human Rights (OHCHR), 'Privacy in the Digital Age' OHCHR <https://www.ohchr.org/en/privacy-in-the-digital-age> accessed 17 October 2025.

[23] United Nations, 'Global Digital Compact' (Online: United Nations) <https://www.un.org/global-digital-compact/en> accessed 17 October 2025.; Demos 2025 Digital rights in 2025 (PDF) <https://demos.co.uk/wp-content/uploads/2025/02/Digital-Rights-in-2025.ac_.pdf> accessed 17 October 2025.

centric and respects fundamental rights.[24] This declaration builds upon its foundational data protection law, the GDPR, which has set a global standard for privacy and data subject rights.[25]

National Laws and Policies: Many countries have taken steps to enshrine digital rights in their national laws. For instance, South Korea adopted a Digital Bill of Rights, and countries like Nigeria enacted the NDPA, which provides a statutory basis for data privacy and other digital rights. Legal scholars and human rights advocates have highlighted how these laws are a crucial step in formalizing and enforcing digital human rights.[26]

5.2 Specific Rights and Concerns

The global discourse around digital rights has focused on several key areas:

Right to Access: The right to access the internet is increasingly seen as a fundamental human right. As an article on Nigeria's legal framework argues, the internet is not just a tool but an essential platform for exercising other rights, such as access to information and freedom of expression. The ECOWAS Court of Justice's 2022 ruling against Nigeria's Twitter ban further reinforced this position.[27]

Privacy and Data Protection: The importance of data privacy has grown significantly due to the rise of AI, biometric surveillance, and big data. Reports from organizations like IBM and the Office of the UN High Commissioner for Human Rights (OHCHR) have highlighted the need for a human-centric approach to data governance to prevent mass surveillance and discrimination.[28]

Freedom of Expression and Information: This remains a central pillar of digital rights. Recent years have seen increased concerns over online censorship, content moderation by tech companies, and the spread of disinformation.[29] A crucial aspect is ensuring that individuals can express themselves freely and access information without fear of reprisal or surveillance.

6.0 LEGAL FRAMEWORK FOR THE ENFORCEMENT OF DATA SUBJECT RIGHTS IN NIGERIA

The legal framework for enforcing data subject rights in Nigeria transitioned from a sub-legal regulatory framework to a robust, statutory one. Two major instruments govern data subject rights and their enforcement in Nigeria.

---

[24] European Commission, 'European Declaration on Digital Rights and Principles' (Online: European Commission) <https://digital-strategy.ec.europa.eu/en/library/european-declaration-digital-rights-and-principles> accessed 17 October 2025.
[25] GDPR-info.eu, 'General Data Protection Regulation (GDPR)' (Online: GDPR-info.eu) <https://gdpr-info.eu/> accessed 17 October 2025.

[27] Media Defence, 'Freedom of Expression Online: Sub-Saharan Africa' (Media Defence Resource Hub) <https://www.mediadefence.org/resource-hub/freedom-of-expression-online-sub-saharan-africa/> accessed 17 October 2025.
[28] United Nations, Human Rights Council, A/HRC/56/45 (online) <https://docs.un.org/en/A/HRC/56/45> accessed 17 October 2025.
[29] Freedom of Information Act, 2011.

Nigeria Data Protection Regulation (NDPR) 2019 and its Implementation Framework 2020: Both were issued and enforced by NITDA, which received complaints, conducted investigations, and issued compliance orders and fines.[30] However, with the issuance of the Nigeria Data Protection Act – General Application and Implementation Directive 2025 (GAID), the NDPR 2019 and its Implementation Framework have been repealed.[31]

Nigeria Data Protection Act (NDPA) 2023 and the General Application and Implementation Directive (GAID) 2025: The NDPA and its recently issued GAID of 2025 established the NDPC, which has explicit powers to investigate complaints, impose administrative fines, issue compliance and enforcement orders, and even initiate prosecution for serious violations.[32]

7.0 ENFORCEMENT MECHANISMS

The legal framework provides two primary avenues for enforcement:

Administrative Enforcement by the NDPC: This is the most common and streamlined route. A data subject can lodge a complaint with the NDPC, which will then investigate the alleged violation. The Commission can then issue a range of directives, from ordering the data controller to cease processing to imposing fines.

Judicial Enforcement: Data subjects retain the right to sue a data controller or processor directly in court. The NDPA provides a clear legal basis for such lawsuits, ensuring that individuals can pursue a remedy through the judicial system.

8.0 CHALLENGES WITH THE ENFORCEMENT OF THE RIGHTS OF A DATA SUBJECT

Even with NDPA, the enforcement of data subject rights still faces significant challenges. These issues stem from a combination of legal, institutional, and socio-economic factors that complicate the practical application of the law. While the creation of the NDPC is a major step forward, its effectiveness is a key concern. The Commission faces resource constraints, including inadequate funding and a shortage of personnel with the technical and legal expertise required to investigate and regulate complex data processing activities, particularly those involving advanced technologies like AI and blockchain.[33] Also, many Nigerians, including both data subjects and small to medium-sized enterprises (SMEs), are largely unaware of their data rights and obligations under the NDPA. This ignorance makes it difficult for individuals to recognize when their rights have been violated

[30] DLA Piper, Data Protection Laws in Nigeria, (DLA Piper, 18 January 2025), <https://www.dlapiperdataprotection.com/index.html?t=law&c=NG> accessed 17 October 2025.
[31] NDPA-GAID, Article 3(3).
[32] Nigeria Data Protection Act (NDPA) Sec 4-5 (2023); National Development Planning Commission, 'NDPC' (NDPC) <https://ndpc.gov.ng> accessed 17 October 2025.
[33] Omaplex Law Firm, 'Critical Assessment Of The Nigerian Data Protection Act—General Application And Implementation Directive 2025' (Omaplex Law Firm, 2025) <https://omaplex.com.ng/critical-assessment-of-the-nigerian-data-protection-act-general-application-and-implementation-directive-2025/> accessed 7 September 2025.

and to seek recourse, while also contributing to widespread non-compliance by businesses.[34] The NDPA provides a right for data subjects to seek redress in court, but this process can be slow and expensive. The Nigerian judicial system's limited experience with complex data privacy cases and the high cost of litigation may be a barrier for individuals seeking justice.

Another challenge is the enforcement of the NDPA's extraterritorial provisions in Section 2(2)(c). While the law applies to foreign companies processing the data of Nigerians, the practical ability of the NDPC to investigate and impose sanctions on companies not physically located within Nigeria's jurisdiction remains a complex legal and logistical issue.[35] Despite the NDPA's clarity, some of its provisions, like the exact definition of legitimate interest as a lawful basis for data processing, still require further clarification from the NDPC due to ambiguity in interpretation.[36] There has also been a continuous resistance to adopting new digital data protection practices, as many businesses still rely on traditional paper-based data collection and storage, which the NDPA does not comprehensively address, creating a vulnerability in compliance and enforcement.[37]

9.0 CONCLUSION AND RECOMMENDATIONS

9.1 Conclusion

Nigeria has made significant strides in aligning with global data protection standards by transitioning from the fragmented legal framework to the principles-based regime of the NDPA.[38] The establishment of the NDPC and the enactment of its GAID of 2025 are proven pivotal advancements, which have provided a clearer, more robust legal and institutional structure for safeguarding data subject rights, moving beyond the limitations of the previous legislation.[39]

Despite this progress, the enforcement of these rights remains a work in progress.[40] The effectiveness of the new legal framework is challenged by institutional capacity issues at the NDPC, widespread lack of public awareness about data rights, and the practical difficulties of enforcing the law against foreign entities.[41] Furthermore, the complexities of navigating Nigeria's judicial system and a general lack of a data privacy culture among businesses and citizens create significant barriers to the effective realization of data subject rights.[42]

---

[34] The Law Brigade Publishers, 'Effective Data Protection in Nigeria: Challenges' (The Law Brigade Publishers, 2022) <https://thelawbrigade.com/wp-content/uploads/2022/11/Patrick-Chukwunonso-Aloamaka-CLRJ.pdf> accessed 7 September 2025.
[31] Ibid. (KPMG, 2023).
[36] NG Chimeziri, 'An Analysis of the Adequacy of the Nigerian Data Protection' (2025) Arcadia Global Studies Journal <https://scholarworks.arcadia.edu/cgi/viewcontent.cgi> accessed 17 October 2025.
[37] Ibid.(PwC Nigeria,2023)
[38] Ibid (KPMG, 2023).
[39] Ibid (PwC Nigeria,2023)
[40] Ibid (Lawhaven Solicitors)
[41] Isaac Juma and Bukola Faturoti, Enforcing Data Privacy in Kenya and Nigeria: Towards an African Approach to Regulatory Practice, (2025) International Review of Law, Computers & Technology 1.
[42] Ibid.

In essence, while the legal framework is now largely in place, the true test lies in its practical enforcement and the widespread adoption of a data protection mindset across the Nigerian digital ecosystem.[43]

9.2 Recommendations

To ensure the effective enforcement of data subject rights and to fully realize the objectives of the NDPA, the following recommendations are crucial:

a. The government must provide the NDPC with adequate funding, advanced technical resources, and a sufficient number of skilled personnel. This will enhance the Commission's ability to conduct thorough investigations, enforce penalties, and handle the high volume of complaints effectively.
b. The NDPC, in collaboration with civil society organizations and media outlets, should launch a nationwide campaign to educate citizens about their data privacy rights under the NDPA. This campaign should use simple language and accessible formats to inform people on how to identify a violation and lodge a complaint.
c. The Nigerian judiciary needs specialized training on data protection laws and digital forensics. This will expedite the legal process and provide a more effective avenue for redress. Also, the cost of litigation related to data privacy should be reduced for greater accessibility by the average citizen.
d. The NDPC should work with industry associations and professional bodies to promote a culture of proactive compliance among businesses. This includes encouraging the adoption of privacy-by-design principles, conducting regular compliance audits, and implementing robust data security measures to prevent breaches before they occur.[44]
e. The NDPC should develop clear guidelines and engage in international cooperation agreements to enforce the NDPA's extraterritorial provisions. This will hold multinational companies operating in Nigeria accountable and ensure that data is protected regardless of where it is processed.

By implementing the above, Nigeria can overcome all enforcement challenges and solidify its position as a leader in data protection in Africa, thereby fostering a more secure, trustworthy, and rights-respecting digital economy.

---

[43] Ibid (OECD).
[44] WTS Blackwood Stone, 'Navigating GAID 2025' (OWTS Blackwood Stone, 2025) <https://wtsblackwoodstone.com/navigating-gaid2025/> accessed 17 October 2025.