*JOURNAL OF JURISPRUSDENCE, INTERNATIONAL LAW AND CONTEMPORARY LEGAL ISSUES*
*Rivers State University, Faculty of Law* *ISSN: 1115 5167 Vol.21 Issue.1, 2026*

# A CONCISE LEGAL REVIEW OF DIGITAL RIGHTS UNDER THE NIGERIAN LEGAL SYSTEM: THE EVOLVING FRONTIER

---

**Desmond O.N. Agwor, Ph.D* & Chioma Stanley Amaehule****

***Abstract***
*The rapid proliferation of digital technologies has profoundly reshaped human interaction, commerce, and governance, giving rise to digital rights, which are traditional human rights adapted to the online environment. These rights encompass access to the internet, freedom of expression, privacy, data protection, and participation in the digital sphere. In Nigeria, their recognition and enforcement are increasingly significant, with Chapter IV of the 1999 Constitution (as amended) providing the doctrinal foundation for extending fundamental rights into cyberspace. Complementary statutes, including the Copyright Act, the Cybercrimes (Prohibition, Prevention, etc.) Act, the Freedom of Information Act, and the Nigeria Data Protection Act 2023, further delineate protections for intellectual property, cyber security, and personal data. Despite these frameworks, Nigeria's digital rights regime faces persistent challenges. Weak enforcement mechanisms, inadequate judicial capacity, the digital divide, and recurring tensions between freedom of expression and state security imperatives hinder effective realization. Cyber security threats and widespread digital illiteracy compound these vulnerabilities, leaving citizens exposed to surveillance, cybercrime, and rights violations. This article argues for a coherent and rights-based governance approach, combining legislative reform, judicial strengthening, and public awareness. Such measures are essential to ensure that Nigeria's digital transformation enhances democratic values, secures fundamental freedoms, and aligns with international human rights standards.*

***Keywords:*** *Digital Rights, Freedom of Expression, Privacy and the Nigerian Legal System*

## 1. Introduction

The 21st century is undeniably the digital age, characterised by an unprecedented integration of technology into every facet of human life, making the advancement of Digital Technologies advanced rapidly than any innovation in the history of humanity.[1] From communication and commerce to education and governance, to the health care sector and legal landscape, digital platforms and services have become indispensable. This far-reaching digital transformation has, however, brought to the fore a new set of rights and challenges, collectively termed "digital rights." These are not entirely new rights but rather the application of existing human rights principles to

* Ph.D, LL.M, LL.B (RSU, Port Harcourt), BL (Abuja), DIP (RIVCAS, Port Harcourt), MCIArb; Lecturer at Law, Department of Jurisprudence and International Law, Faculty of Law, Rivers State University, Nkpolu-Oroworukwo, P.M.B. 5080, Port Harcourt, Nigeria. Tel: +2348035425341, E-mail: desmond.agwor3@ust.edu.ng; desmondnoa@gmail.com
** LL.B, LL.M (RSU, Port Harcourt), Ph.D Candidate, Rivers State University, Port Harcourt, Nigeria. Tel: +2347039305415. Email: chiommy4real2002@yahoo.com
[1] United Nations: 'The Impact of Digital Technology'<www.un.org> accessed 25 March, 2026

the online environment, also known as "Internet rights," e- human rights, and cyber rights[2] They seek to ensure that individuals can access, use, create, and publish digital media, as well as access and use computers, other electronic devices, or communication networks, without undue interference or discrimination. The recognition and protection of digital rights are crucial for fostering an inclusive, democratic, and equitable digital society. In Nigeria, a country with a rapidly expanding internet user base, the discourse around digital rights is gaining increasing prominence. This article aims to provide a comprehensive overview of digital rights, exploring their conceptual foundations, the existing legal framework for their protection in Nigeria, and the contemporary challenges to their full realisation. By examining constitutional provisions, judicial interpretations, and relevant statutes, it seeks to illuminate the current state of digital rights in Nigeria and underscore the imperative for a proactive approach to their safeguarding.

## 2. The Conceptual Framework of Digital Rights

Digital rights in Nigeria encompass the protection of privacy, data, and freedom of expression online, governed by a combination of constitutional provisions,[3] sector-specific laws, and emerging regulations like the Nigeria Data Protection Act 2023,[4] Cybercrimes (Prohibition, Prevention, etc.) Act 2015 (as amended),[5] The Copyrights Act.[6] The National Information and Technology Development Agency (NITDA) Act 2007,[7] and The Freedom of Information Act 2011.[8] Digital rights are an extension of fundamental human rights into the digital realm. They are rooted in the understanding that the principles of human dignity, liberty, and equality must apply equally online as they do offline.[9] From the international perspective, the protection and promotion of human rights online is also an issue of growing concern for international organizations operating in the field of human rights.[10] In a series of resolutions issued in recent years, both the United Nations General Assembly (GA)[11]and the Human Rights Council (HRC)[12] have addressed this topic, embracing the position that the same human rights that people have offline must be protected online

[2] K.I. Bieliakov, O.O. Tykhomyrov & Anor, 'Digital Rights in the Human Rights System' Inter EU Law East: Journal for the International and European Law, Economics and Market Integrations, (2023)10(1), 141-142.
[3]The 1999 Constitution of the Federal Republic of Nigeria (as amended) Cap C23 LFN 2004
[4]Nigeria Data protection Act 2023
[5] Cybercrimes Act 2015 (as amended)
[6]The Copy Rights Act Cap. C28, LFN 2004
[7] National Information and Technology Development Agency Act 2007, Act No.20
[8] Freedom of Information Act 2011
[9]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" European Journal of International Law, (2021) 32 (4) 1271
[10] M. Land, 'Toward an International Law of the Internet', Harvard International Law Journal (2013) 393, 437–442.
[11]Report of the Office of the United Nations High Commissioner for Human Rights' (2014) A/HRC/27/37, United Nations Human Rights Council <https://www.ohchr.org/en/documents/thematic-reports/ahrc2737-right-privacy-digital-age-focus-surveillance-report-office>accessed 27 March, 2026
[12]Human Rights Council, 'The right to privacy in the digital age' (2011) UN Doc A/HRC/16/L.13<https://www.ohchr.org>accessed 27 March, 2026

as well. While there is no single universally agreed-upon definition, digital rights generally encompass:

i) Right to Access the Internet: This includes the right to access information and communication technologies (ICTs) and the internet without discrimination, recognising it as a facilitator for other rights.

ii) Freedom of Expression Online: The right to express oneself, share information, and engage in public discourse through digital platforms, free from censorship or arbitrary restrictions.

iii) Right to Privacy and Data Protection: The right to control one's personal data online, to be free from unlawful surveillance, and to have one's digital communications protected.

iv) Right to Assembly and Association Online: The ability to form groups, organise, and participate in collective action through digital means.

v) Right to Education and Information: Access to online educational resources and diverse sources of information.

vi) Right to Non-Discrimination Online: Protection against discrimination based on race, gender, religion, political opinion, or any other status in the digital space

vii) Right to Due Process in the Digital Sphere: Ensuring fair procedures and remedies in cases of online content removal, account suspension, or other digital infringements. These rights are interdependent and indivisible, meaning that the violation of one digital right often impacts the enjoyment of others. For instance, a breach of data privacy can undermine freedom of expression, while lack of internet access can impede the right to education.

Therefore, digital rights (or rights in the digital era) are those fundamental rights that are directly or indirectly affected by the growing integration of digital technologies into private and public life. In other words, digital rights are not wholly new entitlements; rather, they represent an adaptation or expansion of existing constitutional guarantees to address emerging challenges posed by modern data-driven and online realities.[13] Digital rights allow individuals to access, use, create and publish digital media or to access and use computers, other electronic devices and telecommunication. The right to access internet and use social media platforms is the digital rights in internet era. This right includes right to data protection, right to online privacy and freedom of online expression.[14]

## 3. The Legal Framework for Digital Rights in Nigeria

### a. The 1999 Constitution of Nigeria (as amended)

The protection of digital rights in Nigeria is primarily anchored in the country's constitutional provisions, which serves as the supreme law of the land and the bedrock upon which all digital

[13]J. Müller, Rights in the Digital Age (International IDEA, Stockholm, 2025)<https://www.idea.int/publications/catalogue/rights-digital-age> accessed 27 March 2026.

[14]O.K. Fatimah & Others, 'Unravelling the Concept of Digital Rights Law in Nigeria' Digital Rights Lawyers Initiative <https://digitalrightslawyers.org/publications/> accessed 27 March 2026.

rights protections must be constructed and contains a robust chapter on fundamental rights (Chapter IV) that forms the bedrock for the protection of digital rights.[15]Although the Constitution was drafted before the widespread adoption of the internet, many of its provisions are broad enough to be interpreted and applied to the digital environment. Key rights relevant to the digital sphere include:

i) Right to Life (Section 33): While seemingly indirect, this right can be invoked in cases where digital technologies or their misuse could lead to threats to life, such as cyber bullying resulting in suicide or the use of digital tools to coordinate violence.

ii) Right to Dignity of Human Person (Section 34): This protects individuals from degrading treatment, which can extend to online harassment, cyber stalking, and the non-consensual sharing of intimate images.

iii) Right to Personal Liberty (Section 35): This can be implicated by arbitrary arrests or detentions based on online activities without due process.

iv) Right to Fair Hearing (Section 36): This is essential for ensuring that individuals accused of online offences receive a fair trial and that their digital rights are respected in legal proceedings.

v) Right to Private and Family Life (Section 37): This is perhaps the most direct constitutional basis for digital privacy and data protection. It protects individuals from unlawful interference with their private lives, correspondence, and communications, which extends to digital communications, personal data, and online activities. Thus the privacy of citizens, their homes, correspondence, telephone conversations and telegraphic communications is hereby guaranteed and protected.[16] This provision, while drafted well before the advent of the modern internet, has been interpreted by legal scholars and regulatory authorities as broad enough to encompass digital communications and online privacy. The Nigeria Data Protection Commission (NDPC) has explicitly anchored its mandate in this constitutional guarantee, recognising Section 37(CFRN) as the primary constitutional authority for the protection of the privacy of natural persons in the digital age.[17] In addition, Article 12 of the Universal Declaration of Human Rights provides that: “No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honour and reputation. Everyone has the right to the protection of the law against such interference or attacks.”[18]

vi) Right to Freedom of Thought, Conscience and Religion (Section 38): This protects individuals' beliefs and opinions, including those expressed online.

[15]The Constitution of the Federal Republic of Nigeria (CFRN), 1999 (as amended)
[16] CFRN 1999 (as amended) s37
[17] Nigeria Data Protection Commission <https://ndpc.gov.ng> accessed 27 March, 2026
[18]Article 17 of the International Covenant on Civil and Political Rights

vii) Right to Freedom of Expression and the Press (Section 39): This is fundamental to digital rights, guaranteeing the right to hold opinions and to receive and impart ideas and information without interference. This right is crucial for online speech, blogging, social media use, and access to information. However, it is not absolute and can be subject to limitations prescribed by law for reasons such as public order, national security, or defamation. In other words, the Constitution also guarantees every person the right to freedom of expression, including freedom to hold opinions and to receive and impart ideas and information without interference.[19]However, Section 45(1) permits derogations "as are reasonably justifiable in a democratic society" in the interest of public safety, defence, public order, morality, or for the purpose of protecting the rights of other persons.[20]

viii) Right to Peaceful Assembly and Association (Section 40): This right extends to online gatherings and the formation of digital communities and groups.

ix) Right to Freedom from Discrimination (Section 42): This ensures that individuals are not discriminated against in their access to or use of digital services based on their background or characteristics.

It is important to state that the enforcement of these fundamental rights under the Fundamental Rights (Enforcement Procedure) Rules, 2009[21] is strictly limited to breaches of rights guaranteed in Chapter IV of the Constitution of the Federal Republic of Nigeria, 1999. As affirmed in *Incorporated Trustees of Digital Rights Lawyers Initiative & Ors v National Identity Management Commission* **(**NIMC),**[22]** where the Incorporated Trustees of Digital Rights Lawyers Initiative (DRLI), along with other applicants, challenged the actions of the National Identity Management Commission (NIMC).Their grievance centered on alleged violations of citizens' digital privacy rights in the process of collecting and managing biometric and personal data for the National Identity Number (NIN) scheme. The applicants argued that NIMC's practices infringed on the fundamental rights to privacy and data protection, guaranteed under Section 37 of the 1999 Constitution (as amended) and reinforced by international human rights standards. They sought enforcement of these rights under the Fundamental Rights (Enforcement Procedure) Rules, 2009, asking the Court of Appeal to recognize privacy as a constitutional right in the digital context. The Court of Appeal however, reiterated that "the trite law is that only a suit which relates to infringement of any of the fundamental rights provided under Chapter IV of CFRN, 1999 can be brought under the Fundamental Rights (Enforcement Procedure) Rules, 2009. This underscores the importance of linking digital rights claims directly to these constitutionally enshrined provisions. Furthermore, this case also touched on the procedural aspect of fundamental rights enforcement, noting conflicting decisions of the Court of Appeal regarding joint applicants. While

[19] CFRN 1999(as amended) s39(1)
[20] Ibid s45
[21]Fundamental Rights (Enforcement Procedure) Rules, 2009, Cap C23, Laws of the Federation of Nigeria (LFN) 2004.
[22][ 2021] 17 NWLR (Pt. 1806) 456

acknowledging the conflicting views, the Court referenced a recent decision in *Government of Enugu State v Onya & Ors*[23] which held that joint applicants can bring an application to enforce fundamental rights. The Respondents were allocated stalls at ENSEPA Mini Shops by the Enugu State Environmental Protection Agency (ENSEPA). They were later evicted without due process, prompting them to file for enforcement of their fundamental rights under the Fundamental Rights (Enforcement Procedure) Rules2009.The Appellants (Government of Enugu State) argued that the Respondents had no title to the land, and therefore could not claim rights violations. The Court of Appeal held that title is not a prerequisite for enforcing fundamental rights when the right to peaceful occupation and dignity is violated. The above cases are very important because both emphasize how fundamental rights are interpreted by the Courts in modern contexts, while one is in relation to property and dignity, the other is in relation to digital privacy and data protection. This procedural clarity is very crucial for civil society organisations and groups advocating for digital rights. These constitutional provisions are supplemented by specific statutes and judicial pronouncements. These specific statues are known as digital rights laws, which are legislation and legal frameworks that govern the protection of people's rights in the digital age.[24] These laws are Constitutional Guarantees: Chapter IV of the 1999 Constitution the Constitution of the Federal Republic of Nigeria, 1999 (as amended) which serves as the supreme law of the land

**b. The Copyright Act**

Beyond the 1999 Constitution, the Copyrights Act is a specific statute that address intellectual rights in the digital space. The Copyrights Act is relevant for protecting intellectual property in the digital environment.[25] Section 1 of the Act outlines the eligibility for copyright, including "literary works,""musical works,""artistic works,""cinematograph films,""sound recordings," and "broadcasts." It specifies that such works must have "sufficient effort expended in making the work to give it an original character" and must be "fixed in any definite medium of expression now known or later to be developed." This provision is crucial for creators of digital content, software, online publications, and multimedia, ensuring their original digital creations are protected. The Act addresses copyright infringement, stating that "All infringing copies of any work in which copyright subsists, and all plates, master tapes, machines, equipment or contrivances used, or intended to be used for the production of such infringing copies, shall be deemed to be the property of the owner of the copyright."[26] This provides a legal basis for copyright holders to take action against digital piracy and unauthorised reproduction or distribution of their works online. Section 40 of the Act introduces a levy on "any material used or capable of being used to infringe copyright in a work." This provision aims to generate funds to combat copyright infringement, which is a significant challenge in the digital realm. While the Copyrights Act primarily deals with intellectual

[23][2021]17 NWLR (Pt. 1806)456
[24]O.K. Fatimah & Others (n13)
[25] The Copy Rights Act Cap. C28, Laws of the Federation of Nigeria (LFN) 2004
[26] Ibid s18

property, its application in the digital context is a critical component of digital rights, protecting creators' economic and moral rights in their online works.

**c. Cybercrimes (Prohibition, Prevention, etc.) Act 2015 (as amended)**

The Cybercrimes (Prohibition, Prevention, etc) Act 2015, as amended in 2024, establishes the primary legislative framework for combating cyber offences in Nigeria. It criminalises hacking, identity theft, cyber fraud, unauthorised access to computer systems, and related offences. This law was the first legislation in Nigeria to deal specifically with cyber security, and criminalized various illicit online activities such as hacking, identity theft, cyber-stalking and cyber-fraud, also sets out punishments for the afore-mentioned crimes.[27]The Act also mandates the protection of critical national information infrastructure and promotes the operational resilience of information systems, electronic communications, data, and related intellectual property and privacy rights. The Act has been at the centre of the most significant controversies surrounding digital freedom of expression in Nigeria. While the Act serves the legitimate purpose of combating computer-related crimes, section 24 of the Act criminalised the sending of messages deemed 'offensive, insulting, or annoying' via computer systems which was broadly applied by law enforcement agencies to suppress legitimate political speech, journalistic activities, and social commentary online.[28] While the 2015 Act was a monumental step, the ever-evolving nature of cybercrime necessitated continuous review. Recent amendments, such as those introduced in the Cybercrimes (Amendment) Act 2024, aim to strengthen the legal framework further. Key changes include heavier penalties for cybercrimes like hacking and online fraud, stricter punishments for unauthorized crypto currency transactions, and increased liability for social media platforms failing to remove “offensive” content promptly. These amendments underscore Nigeria’s commitment to adapting its laws to the fluid cyber threat landscape. However, the effectiveness of the Act continues to be debated, with challenges such as weak enforcement, jurisdictional complexities, and limited technical expertise often cited as hindrances to its full impact.[29]

The ECOWAS Court of Justice, in Serap v Federal Republic of Nigeria,[30] found that Section 24 of the Cybercrimes Act in its original form violated Articles 9(2) of the African Charter on Human and Peoples' Rights (ACHPR), and Article 19 of the International Covenant on Civil and Political Rights (ICCPR), due to its vague and overbroad nature. The Court ruled that Nigeria violated citizens’ rights to freedom of expression and access to information, ordering the government to refrain from future arbitrary internet shutdowns.. A subsequent ECOWAS Court ruling in the case

[27] Cybercrimes (Prohibition, Prevention, etc.) Act 2015, Cap C38, Laws of the Federation of Nigeria (LFN) 2004 (as amended).
[28]H. Gyang, “Nigeria’s Cybercrime Reform,” <https://naltf.gov.ng/nigerias-cybercrime-reform/.>accessed 28 March, 2026
[29]A.M. Tahir, “Cybercrime Legislation in Nigeria: Effectiveness and Gaps,” <https://www.researchgate.net/.> accessed 28th March, 2026
[30]ECW/CCJ/JUD/40/22

brought by SERAP Nigeria in March 2022 reaffirmed that the provision's "vague and arbitrary nature" was incompatible with international human rights standards and ordered Nigeria to amend the law.

In February 2024, the National Assembly amended the Cybercrimes Act, narrowing the definition of 'cyber stalking' under Section 24 to apply only to messages that are pornographic or knowingly false 'for the purpose of causing a breakdown of law and order, posing a threat to life.' Civil society organisations welcomed this reform. However, critics noted that the heavy penalties under the original law were retained, and concerns remain about the potential for continued misuse of the amended provision.[31] Furthermore, there are other provision of the Act that provides for the establishment of the Nigerian Computer Emergency Response Team (CERT) to deal with cyber security issues and also provisions required for financial institutions to protect customer's data.

**d. The National Information and Technology Development Agency (NITDA) Act 2007**

The National Information Technology Development Agency (NITDA) Act, enacted in 2007, provides the statutory foundation for Nigeria's institutional framework in information and communications technology (ICT) governance.[32] Originally established by policy in 2001 and later given legislative force under President Obasanjo's administration, NITDA is vested with the mandate to regulate, supervise, and promote the development of ICT across the country. The Act empowers NITDA to issue regulations and guidelines for the assessment, control, and advancement of information technology practices. Its responsibilities extend to fostering innovation, ensuring compliance with standards, and coordinating national ICT programs. In the context of digital rights, NITDA plays a pivotal role by shaping Nigeria's digital ecosystem, setting benchmarks for cyber security, data protection, and digital literacy, and providing the regulatory backbone for subsequent instruments such as the Nigeria Data Protection Regulation (NDPR) of 2019 and the Nigeria Data Protection Act (NDPA) of 2023.

By institutionalizing ICT governance, the NITDA Act laid the groundwork for Nigeria's broader digital rights architecture. It underscores the state's commitment to harnessing technology for national development while safeguarding citizens' rights in the digital sphere. The act is also vested with the authority to provide regulations and guidelines for the development, supervision, assessment, and control of information technology practices and all issues pertaining to and for them.[33]

[31]Cybercrimes (Prohibition, Prevention, etc.) Act 2015 (as amended) (n26)
[32]National Information Technology Development Agency Act, 2007, Cap N78, Laws of the Federation of Nigeria(LFN) 2004, s.6(c).
[33]Ibid

**e. The Nigeria Data Protection (NDPA) Act 2023**

The Nigerian Data Protection Act (NDPA), signed into law on 14 June 2023, establishes Nigeria's most comprehensive framework for safeguarding personal information and advancing digital rights. It addresses the shortcomings of the earlier Nigeria Data Protection Regulation (NDPR) of 2019 and creates a statutory, independent regulatory authority; the Nigeria Data Protection Commission (NDPC) with powers of investigation, enforcement, and sanction. The Act broadens the legal bases for processing personal data beyond consent, incorporating legitimate interest, contractual necessity, legal obligation, public task, and vital interest. It expands the definition of sensitive personal data to include genetic and biometric information, thereby strengthening protections in the digital age. Importantly, it shields individuals from decisions based solely on automated processing, including profiling, that produce legal or similarly significant effects as a critical safeguarding the age of data-driven governance and automated decision-making. Furthermore, the NDPA requires data controllers and processors of "major importance" to register with the NDPC,[34] defined as entities processing data from more than 200 individuals within six months. This provision ensures accountability and transparency in large-scale data processing.[35]

By embedding these principles into law, the NDPA represents a significant advancement in Nigeria's digital rights landscape. It situates privacy and data protection firmly within constitutional guarantees, aligning national standards with international human rights norms and reinforcing citizens' trust in digital governance. The Act also provides that data controllers or data processors owe a duty of care in respect of personal data processing. They must demonstrate accountability relating to the principles and lawful basis for processing personal data. They must ensure that personal data is processed in a fair, lawful, and transparent manner.[36] This emphasizes the importance of digital rights, because technology and the Internet have reshaped how people communicate, participate, and behave. Protecting digital rights ensures that people have control of their data and can use their voices in designing policies that govern the digital space.

**4. Challenges and Emerging Issues in Digital Rights Protection**

The Nigerian digital rights landscape is one of the most rapidly evolving in Africa and, indeed, in the developing world. Despite the existing legal framework, Nigeria is still faced with numerous challenges in fully realising and protecting digital rights. While the Society has moved digital, many of our laws remain analogue. Although society has largely moved into the digital age, many of Nigeria's laws remain rooted in analogue frameworks, leaving gaps in protection. Data privacy and surveillance are pressing concerns, as the absence of a comprehensive data protection regime

[34]Nigeria Data Protection Act 2023, s. 5(2), https://ndpc.gov.ngaccessed 28 March, 2026
[35]O. Babalola, Data Protection in Nigeria: Law and Practice<https://www.olumidebabalola.com>accessed 28March, 2026.
[36]G. Eze, 'Understanding the Nigeria Data Protection Act 2023: Obligations of Digital Platforms and Businesses< https://www.mondaq.com/nigeria/privacy-protection/1430338/understanding-the-nigeria-data-protection-act-2023-obligations-of-digital-platforms-and-businesses#:>accessed 28 March, 2026

until very recently meant that both government and private actors could collect and use personal data with little transparency or accountability. Even with the Nigeria Data Protection Act of 2023, enforcement remains uncertain. Also, freedom of expression online is constitutionally guaranteed, but attempts to regulate social media and online content are often justified by concerns over misinformation, hate speech, or national security, which have sparked fears of censorship and suppression of dissent. This tension highlights the difficulty of balancing individual rights with state interests. At the same time, the digital divide continues to limit access to rights, with rural communities and lower-income groups facing barriers to internet connectivity and digital literacy. This inequality prevents many Nigerians from participating fully in the digital space. Cyber security threats compound these challenges, as rising incidents of hacking, phishing, and online fraud undermine trust in digital platforms. Enforcement mechanisms are weak, with slow judicial processes, limited legal aid, and low public awareness making it difficult for victims to seek redress. Governments often invoke national security or public order to justify restrictions, but without strong judicial oversight, such measures risk eroding fundamental freedoms. Finally, widespread digital illiteracy and lack of awareness about digital rights leave many Nigerians vulnerable to violations such as cyber bullying, phishing, and identity theft. As Donald Miller aptly noted, "in the age of information, ignorance is a choice," yet for many Nigerians, ignorance is imposed by structural barriers to education and awareness; but in the case of Nigerians, how do we demand rights we are not aware of? This lack of knowledge fosters a culture of impunity, where violations go unreported and unaddressed.

Altogether, Nigeria's digital rights environment reflects both the promise of technological progress and the urgent need for reforms that align legal protections with digital realities, strengthen enforcement, and the empowering citizens through awareness and literacy.

## 5. Conclusion

Digital rights have become an indispensable extension of human rights, forming the bedrock of an open, inclusive, and democratic society in the digital age. They are, in essence, the translation of traditional rights into the online environment, ensuring that freedoms such as privacy, expression, and access to information remain protected in cyberspace. Nigeria's constitutional framework, particularly Chapter IV of the 1999 Constitution (as amended), provides the foundation for the protection of these rights. Judicial pronouncements, most notably in *Incorporated Trustees of Digital Rights Lawyers Initiative & Ors v. National Identity Management Commission*, have begun to clarify the scope of digital rights and the mechanisms available for their enforcement. Complementary statutes, such as the Copyright Act, further safeguard intellectual property in the digital realm, underscoring the breadth of digital rights beyond privacy alone. Recent jurisprudence and policy debates have reinforced the urgent need for robust data protection measures, setting clear expectations for individuals, organizations, and government institutions. For Nigeria's digital economy to flourish, and for citizens to exercise their rights without fear of surveillance or misuse

of personal data, comprehensive reforms are essential. Such reforms must embed accountability, transparency, and enforceable rights into the legal framework, thereby building public trust in digital systems and strengthening democratic governance. Although, the journey toward comprehensive digital rights protection remains unfinished, persistent challenges including weak enforcement mechanisms, inadequate judicial capacity, the digital divide, and threats to online freedom of expression, demand a multi-layered response. This requires strengthening legislative frameworks, equipping the judiciary to interpret and enforce digital rights effectively, promoting digital literacy across all levels of society, and fostering a culture of respect for human rights in online spaces. As Nigeria advances in its digital transformation, a proactive, human rights-based approach to digital governance will be paramount. Only by embedding these principles into law and practice can Nigeria ensure that the benefits of technology are widely shared, while fundamental freedoms remain protected. In this way, the country can secure a future where innovation and rights coexist harmoniously, and where the digital age enhances, rather than diminishes, the constitutional guarantees of its citizens.

## 6. Recommendation

In order to achieve the goal of strengthening Nigeria's digital rights framework to meet the challenges of the present and the opportunities of the future, the following recommendations are suggested:

i) The government should prioritize the enactment of a comprehensive data protection law that moves beyond fragmented regulations and establishes a unified framework for safeguarding digital rights. This legislation must set clear standards for how personal data is collected, processed, shared, and stored by both government agencies and private organizations. It should also create mechanisms for accountability, including oversight structures and penalties for violations, while empowering citizens with rights to access, correct, and request deletion of their personal information.

ii) Nationwide awareness campaigns should be launched to educate citizens about their digital rights and the importance of protecting them. Digital literacy programs should be integrated into schools, universities, and other educational institutions to equip Nigerians with the skills necessary to navigate the digital environment responsibly and securely.

iii) Nigeria should also establish a comprehensive national cyber security strategy that provides a framework for securing its digital infrastructure. This strategy should include training for law enforcement agencies and the judiciary to effectively investigate and prosecute cybercrimes, as well as the creation of a national incident response system to coordinate responses to cyber attacks.

iv) Legislators must be equipped with knowledge on digital rights and emerging technologies, drawing from international best practices such as the European Union's regulations on data protection and artificial intelligence. Inclusive engagement with stakeholders - including

civil society, academia, the private sector, and security agencies - will ensure that legislation balances the protection of citizens' rights with national security imperatives.

v) Organizations across Nigeria should implement advanced cyber security tools, including AI-driven threat detection, encryption, and multi-factor authentication. These technologies will enhance resilience against cyber threats and strengthen trust in digital systems.

vii) Finally, a unified national approach to cyber security should be pursued through collaboration between government agencies, the private sector, and international partners. This will improve Nigeria's capacity to anticipate, prevent, and respond to cyber threats while aligning with global standards.