African Journal of Law, Ethics and Education [AJLEE] Vol. 9, No. 1 (2026)
https://ajleejournal.com [ISSN: 2756-6870]

DIGITAL RIGHTS AS HUMAN RIGHTS: ENSURING RESPECT FOR HUMANDIGNITY IN THE INFORMATION AGE

Erhurhu Ogheneovo Omosefe*
Bright F. Ajibade**

Abstract

The rise of the digital age has transformed how people exercise their fundamental rights, introducing new legal and ethical challenges for protecting human dignity online. This paper explores how traditional human rights relate to and shape the concept of digital rights in today's global information society. It argues that digital rights are not entirely new, but rather modern extensions of existing rights such as privacy, freedom of expression and access to information that are now at risk due to issues like mass surveillance, misuse of personal data, among others. Using the doctrinal methodology, this study appraises major legal documents, including the Universal Declaration of Human Rights, the International Covenant on Civil and Political Rights, and other statutes as well as academic writings and relevant case laws. The paper finds that there remain serious gaps in implementation and international cooperation especially in developing countries. The study concludes that safeguarding human dignity in the digital world requires stronger data protection systems, AI policies based on human rights and more active judicial engagement. The study calls for the constitutional recognition of digital rights, creation of independent digital rights commissions and global alignment of data and algorithm governance standards.

* Erhurhu Ogheneovo Omosefe, Lecturer, Faculty of Law, Michael and Cecilia Ibru University, Agbarha -Otor,
Delta State, Nigeria, Email: erhurhuomosefe@gmail.com.

** Bright F. Ajibade, Lecturer, Department of General Studies, Petroleum Training Institute (PTI), Warri, Delta State,
Nigeria, Email: equalright_bright@yahoo.com, ajibade_bf@pti.edu.ng,

Its main contribution to knowledge is the emphasis that protecting digital rights is central to preserving human dignity and promoting democratic values in the 21st century.

Keywords: Human dignity, Privacy, Artificial Intelligence, Data Protection

1.0 INTRODUCTION

Digital technology is reshaping every aspect of human endeavour, with artificial intelligence at its core. The influence of digital technology cuts across virtually every aspect of human existence. The recent surge in human dependence on digital systems has had a profound impact on how people interact with one another. This dependence notwithstanding, it has also raised difficult questions about how to protect basic human rights within the digital space. In this new era, digital rights have become essential for preserving human dignity, as have traditional human rights.[1]

Societal increased exposure to threats like state surveillance, misuse of personal data, and cyber stalking birthed the idea of digital rights in emerging technologies.[2] In truth, digital rights are not new or distinct from human rights but modern forms of existing rights, reinterpreted and adapted to fit the realities of the digital era.[3]

---

[1] Shaleeza Yaqoob Siddiqui et al. 'Human Rights for the Digital Age' [2024] < https://arxiv.org/abs/2408.17302> Accessed 1 November, 2025

[2] Lee TL, Sekalala S, Villarreal P, '*AI and Data Surveillance: Embedding a Human Rights-based Approach*' [2025] *J Law Med Ethics*; [5] [S1]70-74.

[3] Umbrello, Steven & O'Hara, Paul, 'Human Dignity in the Digital Age' [2025], *Journal of Ethics & Emerging Technologies*] 35 (1); 1-21, Vardanyan, Lusine et al., 'Digital Integrity: A Foundation for Digital Rights and the New Manifestation of Human Dignity' [2022], *TalTech Journal of European Studies*, [12] [1], 159-185, Ilori and Tomiwa, 'Framing a Human Rights Approach to Communication Surveillance Laws through the African Human Rights System in Nigeria, South Africa and Uganda' *African*

For example, the Universal Declaration of Human Rights [1948] and the International Covenant on Civil and Political Rights [1966] though written long before the digital age, their core principles remain foundational to the shaping of digital rights.[4] Under the UDHR, *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.*[5]

Similarly, Article 19 affirms that *Everyone has the right to freedom of opinion and expression; this right includes freedom to hold opinions without interference and to seek, receive and impart information and ideas through any media and regardless of frontiers.* This is the precursor to the right to online expression and digital communication freedom. Article 17[6] provides that *no one shall be subjected to arbitrary or unlawful interference with his privacy, family, home or correspondence, or to unlawful attacks on his honour and reputation. Everyone has the right to the protection of the law against such interference or attacks.* This is the bedrock for the right to digital privacy and data protection, which today applies to digital communications, social media, and personal data.

Furthermore, Article 19 guarantees the right to hold opinions without interference and to express them through any other media of his choice, thus extending protection to digital and virtual platforms.

Human Rights Yearbook, [2021], vol.[5] [1] < https://doi.org/10.29053/2523-1367/2021/v5a7>

[4] Art. 12, Universal Declaration of Human Rights (UDHR, 1948); Art. 17, International Covenant on Civil and Political Rights (ICCPR, 1966)

[5] *Ibid.*Art 12

[6] ICCPR

Globally, courts and policymakers have recognised this connection. In *Google Spain v. Agencia Española de Protección de Datos*,[7] the European Court of Justice established the "right to be forgotten, "confirming that personal data protection is part of the broader right to privacy. Similarly, in *Carpenter v. United States*,[8] the United States Supreme Court ruled that law enforcement must obtain a warrant before accessing digital location data, reinforcing privacy protections in the digital era.

In Africa, the *Malabo Convention on Cyber Security and Personal Data Protection* [9] recognises that safeguarding personal data and online freedom is central to protecting human dignity.[10] This is the first regional treaty in Africa to expressly recognise digital rights.[11] Article 8[12] provides that *"Every individual shall have the right to the protection of personal data concerning him or her."* Furthermore, Article 25[13] provides that *"Member States shall ensure that every person's privacy rights are respected and protected in the digital and electronic communications environment."* These provisions align with Articles 12 UDHR and 17 ICCPR situating data privacy within the Human rights systems.

Nigeria's growing reliance on digital technology for governance, education, and commerce has intensified the need for protection of digital rights. The Nigerian Data Protection Act [14] is a positive step

[7] (Case C-131/12) [2014] E.C.R. I-317.
[8] [2018] 138 S. Ct. 2206 (U.S. Supreme Court).
[9] 2014
[10] African Union, *Convention on Cyber Security and Personal Data Protection (Malabo Convention)*(2014)<https://au.int/en/treaties/african-union-convention-cyber-security-and-personal-data-protection> Accessed on 1st November, 2025.
[11] *Ibid*
[12] *Ibid*
[13] *Ibid*
[14] 2023

towards regulating the collection and use of personal data.[15] Nigerian courts have also began recognizing the dimensions of digital rights. In the case of *Digital Rights Lawyers Initiative v. National Identity Management Commission (NIMC)*,[16] the court acknowledged that citizens' rights to privacy and data protection extend to online activities. Yet, weak enforcement, limited public awareness, and institutional inefficiencies continue to undermine the effective protection of digital rights.[17] The paper contributes to the global discussion on digital governance and responsible technology use. It highlights Africa's role in shaping global digital policy and argues for the development of human-rights-based approaches to artificial intelligence and data protection.[18] The paper ultimately calls for constitutional recognition of digital rights, stronger enforcement institutions, and international cooperation in digital governance. By doing so, it aligns with global efforts led by the United Nations and the African Union to ensure that technology advances human dignity and strengthens democracy rather than eroding them.[19]

2.0 CONCEPTUAL ANALYSIS OF HUMAN AND DIGITAL RIGHTS

2.1 Understanding Human Rights

[15] s. 2[1].

[16] Suit No. FHC/ABJ/CS/1447/2020.

[17]Paradigm Initiative, *Nigeria's Digital Rights and Freedom Bill: Legislative Analysis Report* [2022]< https://paradigmhq.org/wp-content/uploads/2023/06/Nigeria-Londa-2022.pdf>

[18] United Nations Human Rights Council, *The Right to Privacy in the Digital Age*, [2021] A/HRC/RES/48/4< https://docs.un.org/en/A/HRC/RES/48/4> Accessed 1st November, 2025.

[19] African Union Commission, Digital Transformation Strategy for Africa (2020–2030),< https://au.int/sites/default/files/documents/38507-doc-dts-english.pdf> Accessed 1st November, 2025.

Human rights are the basic freedoms and protections that belong to every person simply because they are human. They apply universally irrespective of nationality, race, gender, religion, or social class. They are based on the belief that every individual has value and dignity that must be respected and protected by law.[20]

The Universal Declaration of Human Rights[21] clearly states that *"all human beings are born free and equal in dignity and rights."* Later, the International Covenant on Civil and Political Rights[22] reinforced these ideas by guaranteeing rights such as privacy, liberty, and freedom of expression.[23]

The African Charter on Human and Peoples Rights supports these same values by recognising the right to dignity and the right to receive and share information.[24] Together, these instruments form the foundation for what we now call digital rights, reflecting the need for laws to adapt to protect people's dignity and freedoms in technological spaces [25]

2.2 Understanding Digital Rights

Digital rights are human rights applied in digital environment. They protect how people use, share, and control information online.[27] These include the right to privacy, freedom of expression online, access to information, protection of personal data, and participation in the digital economy.[26]

---

[20] <https://www.diplomacy.edu/topics/human-rights> Accessed 1st November, 2025

[21] UDHR 1948

[22] ICCPR 1966

[23] Articles 17 and 19

[24] ACHPR,(1981) Arts 5 and 9

[25] Ageng N. Ahmad F.S, Adriyanto, A. Imam Al Mutaqin [2025] *East Asian Journal of Multidisciplinary Research (EAJMR)* Vol. 4, No. 1, 183-194

[26] United Nations Human Rights Council [2021] *The Right to Privacy in the Digital Age*, A/HRC/RES/48/4.< https://docs.un.org/en/A/HRC/RES/48/4#:> Accessed 2nd November, 2025

Johan Rochel[27] describe digital rights as part of digital integrity; the idea that everyone should be able to protect their online identity and personal information. Similarly, Vardanyan explain that digital integrity is a new way of expressing human dignity; ensuring people are treated as full individuals and not just as data or statistics.[28]

Johan Rochel and Lusine Vardanyan contributions focus on the moral and philosophical reasons why people's online identities and personal information should be protected. However, their perspectives are mostly based on Western experiences and legal systems. Placing the discussion within the African context**,** with particular focus on Nigeria. In countries like Nigeria where digital literacy is low, data protection is weak, and government surveillance is common, protecting digital integrity cannot rely solely on moral or ethical principles. Real progress requires strong constitutional laws and effective institutions that make the protection of digital identity a legally enforceable right.

Digital integrity entails not only privacy, but also personal autonomy, digital inclusion, and equality. Safeguarding human dignity in today's information-driven world means ensuring that everyone; regardless of gender, social class, or digital access; has control over their own data, is fairly represented in digital and algorithmic systems, and is protected from online discrimination.

Tomiwa Ilori[29] warns that government surveillance and poor data protection laws threaten these rights. He suggests that African countries should use human rights principles when making digital laws. The

[27] Johan R., Connecting the Dots: Digital Integrity as a Human Right [2021] vol. 21(2) Human Rights Law Review, 358.
[28] Vardanyan L., Stehlík V., and Kocharyan, Digital Integrity: A Foundation for Digital Rights and the New Manifestation of Human Dignity [2022] vol. 12(1) TalTech J. Eur. Studies, 159.
[29] Ilori T., 'Framing a Human Rights Approach to Communication Surveillance Laws in Nigeria, South Africa and Uganda' [2021] African Human Rights Yearbook

Malabo Convention, 2014 supports this view, stating that every person has the right to protection of their personal data.[30]

It should be noted that human rights principles alone are not enough as suggested by T. Ilori. In practice, many African countries still struggle with poor enforcement, low public awareness, and limited institutional capacity. Consequently, the need arises for a robust legal and institutional framework that ensures real accountability, strong enforcement mechanisms**,** independent oversight bodies**,** and public awareness campaigns.

2.3 Understanding Human Dignity

The moral foundation of all human rights is the idea that every person has intrinsic worth and human dignity.[31] Dignity is has also being explained to mean "the basic idea behind all other human rights."[32] In Africa, dignity is given special importance in the ACHPR[33], where respect for human dignity is guaranteed and forbids any form of humiliation or exploitation.

In modern globalisation, dignity also reflects digital self-determination; the right to control your digital identity, data, and online activities. Thus, treating people's personal data as a economic objects (something to be bought or sold) weakens their human dignity.[34] Likewise, Umbrello and O'Hara stress that protecting dignity today means

[30] Art. 8, 25

[31] <https://www.theihs.org/blog/human-dignity-the-cornerstone-of-classical-liberalism/#> Accessed 2nd November, 2025.

[32] Christopher McCrudden 'Human Dignity and Judicial Interpretation of Human Rights' [2008] [19] *Eur. J. Int'l L* 655.

[33] Article 5

[34] Vardanyan, (supra note 28).

building ethics and human-rights values into digital systems such as artificial intelligence and automation.[35]

In Nigeria; where awareness about data protection and digital ethics is limited, the challenge stretches beyond the *commercial use* of personal data but also the *lack of transparency and accountability* in how governments and private companies handle information. Thus, safeguarding human dignity in the digital era must go beyond ethical theory. It requires practical legal reforms that define clear boundaries for data collection, sharing, and monetisation.

2.4 The Link between Human Rights, Digital Rights, and Human Dignity

Human rights, digital rights, and human dignity are interrelated. Human dignity entails the moral basis for rights; Human rights describe the protections that flow from them, while digital rights extend these protections to the digital space.[36]

Globally, the UDHR[37] and ICCPR[38] protect privacy and free expression, which now apply to online communication and data privacy. Therefore, digital rights are a continuation of human rights in cyberspace ensuring the persistence of these rights with technological evolution. Oghomwen Rita Ohiro[39] has argued that as the country's digital and AI systems expand, the law must strike a balance between innovation, privacy, and ethical governance.

---

[35] Umbrello and O'Hara, 'Human Dignity in the Digital Age' [2025] *J. Ethics & Emerging Technologies*, vol. [35][1], 165.
[36] Zhang Y and Jiang S, 'The Concept of Digital Human Rights and Its Reshaping of Basic Rights' [2024], *The Journal of Human Rights,* [23] [4].
[37] Art.17
[38] Art.19
[39] Ohiro, O. R. O., 'Striking a balance: AI, national security, and privacy rights in Nigeria*'* [2025] *UCC Law Journal*, [4][2], 157–208.

3.0 LEGAL FRAMEWORK ON DIGITAL RIGHTS

Digital rights build upon established human rights principles in international and domestic law. Protections for privacy, data, and online expression originate from rights predating the digital era but are now interpreted to address technological developments.

3.1 International Legal Framework

Article 12 of the Universal Declaration of Human Rights[40] states that *"no one shall be subjected to arbitrary interference with his privacy, family, home or correspondence*," while Article 19 guarantees the freedom "*to seek, receive and impart information and ideas through any media and regardless of frontiers.*" These provisions form the basis for protecting privacy, data, and online freedom of expression.

3.1.1 International Covenant on Civil and Political Rights [41] reinforces the rights provided for in Art. 12 and 19. Article 17 of the ICCPR prohibits unlawful interference with a person's privacy, while Article 19 upholds the right to freedom of expression. Courts and human-rights bodies have extended these protections to online activities, digital surveillance, and the collection of personal data. In *Toonen v. Australia*;[42] Nicholas Toonen, a gay rights activist challenged Tasmanian laws criminalizing consensual private sexual activity between adult men. The UNHRC found this as a violation of Article 17 of the ICCPR, interpreting "privacy" to include sexual orientation. The case led to the federal Human Rights (Sexual Conduct) Act 1994, effectively decriminalizing homosexuality in Australia. Also, in *Digital Rights Ireland Ltd vs. Ireland,* [43] Digital Rights Ireland challenged EU data-retention legislation requiring telecoms to store all users' data for 6–24 months.

[40] UDHR 1948
[41] ICCPR, 1966
[42] Communication No. 488/1992, U.N. Doc CCPR/C/50/D/488/1992 (1994).
[43] [2014] Europe (ECJ)

3.1.2 International Covenant on Economic, Social and Cultural Rights, 1966

The International Covenant on Economic, Social and Cultural Rights[44] supports digital rights. Articles 6, 9, 13, and 15 guarantee the rights to work, education, social security, and access to the benefits of scientific progress. These provisions are now interpreted to include access to technology, digital education, and online participation, reinforcing human dignity in the information age. These instruments collectively indicate that digital rights are extensions of pre-existing human rights adapted to new technological realities.

3.2 African Regional Legal Framework

Africa has incorporated digital considerations into its human-rights system. The ACHPR[45] recognises the right to dignity,[46] the right to receive and impart information,[47] and the right to privacy and security of the person[48]

3.2.1 African Union Convention on Cyber Security and Personal Data Protection[49] represents Africa's first continent-wide treaty addressing digital governance. Article 8 guarantees protection of personal data while Article 25 requires states to ensure respect for privacy in electronic communication. The Convention also establishes principles such as *lawfulness, consent, transparency, and purpose limitation* to guide data processing and use.

Furthermore, The African Commission on Human and Peoples' Rights, through its 2019 Declaration of Principles on Freedom of Expression

[44] ICESCR, 1966
[45] ACHPR1981
[46] Art. 5
[47] Art. 9
[48] Art. 4
[49] Malabo Convention, 2014

and Access to Information in Africa,[50] explicitly recognises online privacy and data protection as human-rights obligations.

3.3 Nigerian Legal Framework

3.3.1 The Constitution of the Federal Republic of Nigeria (1999, as amended)

Sections 37 and 39 of the constitution provide the foundation for protecting privacy and expression. However, despite these guarantees, there have been several instances where government agencies or actors have violated citizens' digital rights in practice.

3.3.2 Nigeria Data Protection Act,[51]

The Act provides lawful protection for personal data, yet, frequent data leaks from public institutions like the National Identity Management Commission (NIMC) and Joint Admissions and Matriculation Board (JAMB) raises concerns about poor enforcement. Investigative reports in 2023 revealed that Nigerians' National Identification Numbers (NINs) and personal details were being sold online, directly contravening section 2(1) of the Act[52] This undermines the credibility of Nigeria's digital governance efforts and reveal the failure to implement adequate cyber security safeguards.

3.3.3 Cybercrimes (Prohibition, Prevention, etc.) Act, 2025

The Cybercrimes Act[53] was designed to prevent unlawful access, data breaches, and online abuse. Yet, evidence shows that some government actions have directly violated both the spirit and letter of this Act, particularly concerning citizens' rights to privacy and free expression. Key examples include: the June, 2021, Twitter Ban Case. The

[50] [2019]
[51] 2023
[52] <https://www.google.com/search?q=investigative+reports+in+2023> 2025
[53] 2025

Government's suspension of Twitter's operations in Nigeria resulted in denial of millions of citizens access to platform for communication and expression. This was criticised as a violation of the Constitutional right to freedom of expression and Section 24 of the Cybercrimes Act**,** which criminalises unlawful interference with electronic communications.[54] It also contradicted Article 9 of the African Charter on Human and Peoples' Rights, which protects the right to receive and impart information.

Another example was the 2020 EndSARS Digital Surveillance. During the #EndSARS protests, credible reports showed that Nigerian authorities used digital surveillance tools to track activists, freeze bank accounts, and monitor social media conversations.[55] These contravened Section 8 of the Cybercrimes Act, 2025, which prohibits the interception of electronic communications without judicial authorisation, and also violated Section 37 of the Constitution, which guarantees the privacy of citizens.[56]

3.3.4 NCC Data Collection Directive:

The Nigerian Communications Commission[57] directed telecom companies to link all SIM cards to NINs, threatening to block non-compliant users. While aimed at national security, the lack of privacy safeguards violated Sections 6 and 8 of the Cybercrimes Act, which prohibit unauthorised access and interception of personal data.

---

[54] SERAP v. Federal Republic of Nigeria, ECW/CCJ/APP/23;24;26&29/21 Judgment No: ECW/CCJ/JUD/40/22

[55] Amnesty International, *Nigeria: Authorities Target Activists through Digital Surveillance during #EndSARS* (2020)< https://www.amnesty.org/en/latest/campaigns/2021/02/nigeria-end-impunity-for-police-violence-by-sarsendsars/> Accessed 2nd November, 2025

[56] *Incorporated Trustees of Media Rights Agenda* v *National Broadcasting Commission*, Unreported Suit No. FHC/IB/CS/101/2020, judgment delivered on 23/06/2021 by J.O. Abdulmalik J at Federal High Court of Nigeria, Ibadan Judicial Division

[57] NCC, 2021

3.3.5 Suspension of Online Media Outlets:

Instances abound were government agencies have ordered the suspension or blocking of media platforms such as *Peoples Gazette* and *Premium Times*, under the guise of national security. These actions interfere with lawful digital expression and violates Sections 24 and 28 of the
Cybercrimes Act, which requires judicial oversight before any digital interception.[58]

3.3.4 Judicial Developments

Despite these infringements, Nigerian courts have occasionally upheld digital rights. In *Digital Rights Lawyers Initiative v. NIMC*, Court affirmed that citizens have a right to data privacy under Section 37 of the Constitution and that the NIMC must comply with national and international data-protection standards.[59]

Similarly, in *Digital Rights Lawyers Initiative v. NITDA*, the court reiterated that violation of digital privacy such as unauthorised collection or sharing of personal data, constitutes an infringement of fundamental rights.[60]

3.4 Bridging Global Norms and Local Realities

Nigeria's experience shows a gap between digital rights law and practice. Despite the Cybercrimes Act and Data Protection Act, government actions such as the Twitter ban and digital surveillance erode public trust. Effective protection therefore requires more than legislation; it demands enforcement, judicial independence, and

[58] Committee to Protect Journalists (CPJ), *Nigeria Blocks Access to Independent News Websites* (2022).< https://cpj.org/africa/nigeria/2022/#> Accessed 2nd November, 2025
[59] Suit No. FHC/ABJ/CS/1447/2020
[60] Suit No. FHC/L/CS/1702/2020

accountability to make privacy, freedom, and data security real rather than theoretical.

4.0 CHALLENGES TO THE ENFORCEMENT OF DIGITAL RIGHTS IN NIGERIA

4.1 Weak Institutions and Poor Governance

Nigeria has a plethora of laws protecting the privacy, data, and freedom online of her citizens. However, in reality these rights are not adequately protected. A major problem that plagues the effective protection of digital rights is weak and inefficient institutions. The NDPC[61] and the NITDA[62] often lack adequate funding, trained staff, or independence[63]

Sometimes, the same agencies responsible for data protection engage in abuses, further eroding public trust[64] Corruption, slow decision-making, and poor inter-agency coordination exacerbate the problem, making digital rights enforcement nearly impossible.

4.2 Weak Judicial Protection

The judiciary plays a central role in the protection of digital rights. They decide how the Constitution and other laws should apply to new digital realities such as privacy, freedom of expression, and the collection of

[61] Nigeria Data Protection Act 2023

[62] National Information Technology Development Act, 2007

[63] Sabo A, Siti A.J, B. Abdullahb and Rozita A, 'Issues and Challenges of Transition to e-Voting Technology in Nigeria' [2015] Vol.[5] No.[4] 96

[64] C.M Umeanwe, 'Corruption, good governance and the digital age: Challenges and opportunities' [2025] *Crowther Journal of Arts and Humanities*, Vol.[2] [3] 125

personal data[65]. In Nigeria, however, judicial protection in this area remains uneven and, at times, uncertain[66].

Some Nigerian courts have made encouraging progress. In *Digital Rights Lawyers Initiative v. National Identity Management Commission*,[67] the Federal High Court confirmed that data protection is a fundamental right under Section 37 of the *1999 Constitution*. The Court held that the handling of citizen's personal information by public authorities must respect the constitutional right to privacy. This judgment marked an important moment in Nigeria's growing recognition that data misuse can amount to a human-rights violation.[68]

However, not all judges share the same level of understanding. Many members of the judiciary are still unfamiliar with modern issues such as artificial intelligence (AI), data mining, and digital surveillance.[69] This knowledge gap is not unique to Nigeria.[70] The African Declaration on Internet Rights and Freedoms (2014) and the UN Human Rights Council Resolution 48/4 (2021) both note that judges worldwide must be trained to interpret existing rights in the context of the internet and emerging technologies.[71] Cases often take several years to conclude and

---

[65] Julius v FRN5[2021] LPELR-54201(CA)

[66] Adeboye Adegoke, 'Digital Rights and Privacy in Nigeria'[2020] (*Paradigin Innitiative Publication)*[4].

[67] *Digital Rights Lawyers Initiative v. National Identity Management Commission* (FHC/L/CS/2020).

[68] Unreported Suit No. ECW/CCJ/APP/23/21, Ruling delivered on 22/06/2021 by J Gberi–Be Outattara J, Keikura
Bangura, Januaria T, Silva Moreira Costa & Mr. Athanase Atannon Community Court of Justice of the Economic
Community of West African States(ECOWAS) Abuja

[69] *Solomon Okedara v A.G Federation* [2019] LCN 12768 (CA) African Declaration on Internet Rights and Freedoms (2014); UN Human Rights Council, *Resolution 48/4 – The Right to Privacy in the Digital Age* (2021).

[70] Custers, B.H.M. 'New Digital Rights: Imagining additional fundamental rights for the digital era'[2022], *Computer Law & Security Review,* Vol [44] p. 1-13

[71] World Bank, 'Doing Business Report – Judicial Efficiency in Nigeria*'*[2020].

this discourages victims of online abuses; such as privacy breaches, identity theft, or defamation; from seeking redress.[72]High litigation costs and the absence of collective or class-action procedures further limit access to justice for ordinary citizens.

Lack of specialised courts or divisions that focus on cyber-related human-rights cases is another issue that effect digital right protection.[73] Matters involving data protection or online speech are usually lumped together with general civil or criminal cases, handled by judges who may not have digital expertise. In contrast, some countries have already made progress in this area. Kenya established an Information and Communication Technology (ICT) Tribunal under its *Kenya Information and Communications Act*,[74] while India's Supreme Court, in *Justice K.S. Puttaswamy v. Union of India,*[75] recognized privacy as a core part of the constitutional right to life and dignity. South Africa's courts have also applied similar reasoning under Section 14 of its *Constitution*, reinforcing privacy in the digital age.

To strengthen judicial protection, Nigeria's courts and legal institutions should invest in capacity-building programmes for judges, magistrates, and lawyers.[76] Continuous legal education should cover digital law, data governance, cybercrime, and human-rights-based approaches to technology regulation. Additionally, the justice sector should modernize its procedures by adopting digital case-management systems, electronic filing, and online dispute-resolution (ODR) tools, as recommended by the National Judicial Council (NJC) in its 2021 digital-transformation

[72] *Justice K.S. Puttaswamy (Retd.) v. Union of India* (2017) 10 SCC 1 (SC India).

[73] A. Sambo, "Cybercrime Adjudication and the Need for Specialized Courts in Nigeria," [2022] *Nigerian Law Review* Vol.[18].

[74] Nyabuti Damaris Kemunto, 'Awareness-Raising Campaign for Tribunals in Kenya: A Case Study of
Communication and Multimedia Appeals Tribunal' (CAMAT) [2023] *International Journal of Research and Innovation in Social Science (IJRISS)*< https://rsisinternational.org/journals/ijriss/> Accessed 5th November, 2025

[75] *Justice K.S. Puttaswamy (Retd.) v. Union of India* (2017) 10 SCC 1 (SC India).

[76] *Supra* [n.73]

policy.[77] In short, while Nigeria's judiciary has taken early steps to protect digital rights, it still struggles to keep pace with rapid technological change.

4.3 Low Awareness and Digital Illiteracy

Most Nigerians are uninformed about digital rights freely share personal information without understanding privacy implications. This ignorance allows private companies and government agencies to exploit data with minimal accountability. Digital literacy and public education are essential to empower citizens to demand their rights.

4.4 Digital Poverty and Unequal Access

Digital rights remain meaningless without access. Millions of Nigerians particularly women, children, and low-income groups, lack affordable internet, reliable devices, and electricity.[78] The National Broadband Plan (2020–2025) aims to improve internet access.

4.5 New Technologies and Ethical Problems

New technologies like Artificial Intelligence (AI), facial recognition, and big data are becoming common in Nigeria, along with the associated risk. Many of these systems are used by private companies and government agencies without transparency.[79]

AI systems can make biased decisions — for example, rejecting job applicants or loan requests based on gender, ethnicity, or location. If these tools are not properly checked, they can harm people's dignity and ethical frameworks and regulatory oversight are required to ensure transparency, fairness, and respect for rights. widen inequality.

---

[77] NIALS, *Report on Judicial Education and Digital Transformation in Nigeria* (2022); National Judicial Council, Policy on Digital Justice Delivery and E-Filing Systems (2021).

[78] <https://www.oecd.org/en/publications/closing-broadband-connectivity-divides-for-all> Accessed 5th November, 2025.

[79] *Okoye & Anor. v Christopher Obiaso & Ors.* [2010] 8 NWLR (Pt. 1195) 145, 168.

4.6 Misuse of Digital Power and Corruption

Digital tools which should improve governance are sometimes used for political or personal gain. Some politicians and public officials use cyber laws or online surveillance to silence critics or journalists. Findings by *Sunday Punch* [80] revealed that aside from Thomas, the authorities have used the cyberstalking section of the Cybercrime Act to justify the arrests of journalists and social media critics. On May 1, 2024, an investigative journalist with the *Foundation for Investigative Journalism*, Daniel Ojukwu, was arrested months after he published a story which exposed alleged misappropriation of funds by the office of the Senior Special Assistant to the President on Sustainable Development Goals. Ojukwu's whereabouts was unknown until May 4 when he was in the custody of state intelligence agents in Lagos. Although the journalist was released on May 10, the authorities alleged that his report violated the Cybercrime Act of 2015.

Also, on March 15, 2024, the former editor of an online newspaper, *First News*, Segun Olatunji, was arrested in his home by some soldiers, who blindfolded and flew him to Abuja on a military aircraft. The journalist was reportedly tortured and kept incommunicado for several days until the Nigerian National Committee of the International Press Institute traced him to the custody of the Defence Intelligence Agency.

The abuse of technological systems can weaken public confidence in governmental institutions and pose risks to democratic governance. When corruption occurs in technology-related initiatives; such as through inflated procurement contracts or the acquisition of non-existent equipment; public funds are squandered that could otherwise strengthen cyber security infrastructure and safeguard citizens' rights. Addressing

[80] https://punchng.com/how-nigerian-authorities-use-cybercrime-act-to-harass-detain-journalists-activists/ accessed 5th November, 2025

these concerns requires greater openness in the formulation and implementation of digital policies in Nigeria. Mechanisms such as independent oversight and regular public disclosure can contribute significantly to restoring and maintaining public trust.

4.7 The Gap between Law and Reality

Nigeria has robust digital laws on paper, but poor enforcement and a culture of weak accountability render them ineffective. Laws were enacted faster than institutional capacities and public awareness could adapt. Bridging this gap requires not only legal reform but also governance and cultural change. This paper explains that protecting digital rights in Nigeria is not just a legal issue; it is a governance and cultural issue. For laws to have force, people in power must respect the values of privacy, freedom, and dignity.

4.8 Building a Fair Digital Future

For digital rights to be meaningful, Nigeria needs to: strengthen the independence and capacity of institutions; train judges, lawyers, and policymakers in digital law; educate citizens about online rights and data protection; make technology more affordable and accessible; and promote ethics, transparency, and accountability in all digital programs.

5.0 RECOMMENDATION

Protecting digital rights in Nigeria is necessary for social justice, democracy, and development in today's digital world. Laws alone cannot guarantee these rights; their enforcement depends on awareness, institutional will, and responsible use of technology. some recommendations to ensure that digital rights truly serve human dignity and inclusion are:

i. Build a Strong and Independent Institutional System

The enactments of the Nigeria Data Protection Act (2023) and the Cybercrimes Act (2025) are steps in the right direction at protecting digital rights in Nigeria, but weak institutions often prevent these laws

from working effectively. The Nigeria Data Protection Commission (NDPC) should operate independently, free from political control. It must have the resources and authority to investigate data misuse, impose penalties, and educate citizens about their digital rights.

Collaborative synergy among key institutions such as the NDPC, the National Information Technology Development Agency (NITDA), and the Nigerian Communications Commission (NCC); should be improved. These bodies must share information and develop consistent digital-rights policies instead of working in isolation.

ii. Invest in Public Awareness and Digital Literacy

One of the biggest challenges is that many Nigerians do not know what digital rights are or that they even have them. Thus, national awareness campaign is pivotal to explaining citizens' rights to privacy, consent, and online safety. Similarly, digital literacy should also be part of the school curriculum so that young people understand how to use the internet safely and ethically. Civil society groups, media organizations, and local community centers can help translate these ideas into simple messages in local languages.

iii. Promote Ethical Technology and Responsible Governance

Nigeria needs clear rules to ensure that artificial intelligence (AI), data analytics, and surveillance technologies are used fairly and transparently. Technology should serve people, not control them. The government should adopt a National Ethical Framework for Artificial Intelligence and Data Use, guided by the UNESCO Recommendation on the Ethics of AI (2021) and the African Union Data Policy Framework (2022). These frameworks emphasize fairness, accountability, and respect for human dignity in technology use.

iv. Foster Regional and Global Cooperation

Digital rights cannot be protected in isolation. Nigeria should take a leading role in African and global forums that shape technology

governance. Ratifying and implementing the African Union's Malabo Convention (2014) would strengthen cross-border cooperation on cyber security and personal-data protection. Through ECOWAS and the United Nations Human Rights Council, Nigeria can exchange ideas and align its digital policies with global human-rights standards. Such collaboration will help address transnational challenges like cybercrime, misinformation, and data trafficking.

v. Encourage Partnership with the Private Sector

Having regard to the fact that most personal data is managed by private companies, they must be active partners in protecting rights. The government should require tech firms, banks, and telecom companies to follow a Digital Rights Code of Conduct that emphasizes transparency, informed consent, and accountability. Businesses should also support research and training on data ethics and digital governance. A cooperative approach where both government and private organizations share responsibility will create a safer digital environment for everyone.

vi. Bridge the Digital Divide

Government must treat digital access as a basic right, similar to education and healthcare as millions of Nigerians, especially in rural and low-income communities, still lack reliable internet or affordable devices. Expanding broadband infrastructure, encouraging low-cost data plans, and providing public Wi-Fi in schools and libraries would reduce inequality and enable citizens to enjoy their digital rights fully. True digital freedom depends on equal access.

vii. Embed Human Dignity in Digital Policy

Government should ensure that all digital policies, from data protection to e-governance, are grounded in human-centered principle. In doing so, technology will become a tool for empowerment rather than control. Every reform should therefore be guided by one core value; human dignity. Protecting digital rights is not just about privacy or technology;

it is about respect for people's autonomy, equality, and freedom from abuse.

6.0 CONCLUSION

Nigeria stands at a turning point. The digital era offers huge opportunities for growth and innovation, but also new forms of inequality and rights violations. Building an inclusive and rights-based digital society requires legal strength, ethical governance, and citizen awareness.

If Nigeria commits to these reforms, it can set an example for Africa and the world; showing that technology, when guided by human dignity, can strengthen both democracy and justice.