INTELLIGENCE

THE GOVERNANCE AND INNOVATION NETWORK FOR GENERATING ENHANCED REGULATIONS (GINGER)

Evidence Synthesis on the State of Nigeria's Digital Economy and E-Governance Bill

September 2024

hello@apiintelligence.org
www.apiintelligence.org

THIS WORK IS SUPPORTED BY

INCLUDE

KNOWLEDGE PLATFORM ON INCLUSIVE DEVELOPMENT POLICIES

Foreign, Commonwealth
& Development Office

Table Of Content

LIST OF ABBREVIATIONS	03
EXECUTIVE SUMMARY	04
1.0 INTRODUCTION	05
2.0 DIGITAL TRANSACTIONS AND ELECTRONIC COMMERCE	05
2.1 Internet Penetration	05
2.2 Adoption of Mobile Money and E-Payments	08
2.3 Legal Recognition of Electronic Transactions	09
3.0 ELECTRONIC CONTRACTS AND SIGNATURES	11
3.1 Current Legal Framework	11
3.1.1. Legal Provisions Under the Evidence Act	11
3.1.2. Legal Provisions Under Cybercrimes (Prohibition and Prevention) Act	11
3.1.3. Legal Provisions Under Companies and Allied Matters Act (CAMA) 2020	11
3.1.4. Challenges in Adoption	12
1. Lack of Awareness	12
2. Mistrust in Digital Authentication	12
3. Technical Barriers	12
5. Regulatory and Compliance Concerns	13
3.1.5. Overcoming Adoption Barriers	14
4.0 CONSUMER PROTECTION IN DIGITAL COMMERCE	15
4.1 Consumer Awareness and Protection	15
4.1.1. Data Privacy and Protection	15
4.1.2. Consumer Complaints and Regulatory Response	16
4.1.3. Need for Enhanced Consumer Protection Measures	17
4.2 Cybersecurity Threats	18
4.2.1. Rising Cybersecurity Threats	18
4.2.2. Impact on Consumer Trust	19
4.2.3. Strengthening Cybersecurity Measures	19
5.0 DIGITAL GOVERNMENT SERVICES	21
5.1 E-Government Readiness	21
5.1.1 Current Initiatives and Achievements	22
5.1.2. Challenges in E-Government Readiness	22
5.2 Implementation Challenges	22
5.2.1. Inadequate Digital Infrastructure	22
5.2.2. Low Digital Literacy	24
5.2.3. Limited Interoperability Between Government ICT Systems	24
5.2.4. Addressing the Challenges	25

6.0 DIGITAL INFRASTRUCTURE AND ICT SYSTEMS 26
6.1 Current State of Digital Infrastructure 26
6.2 Public Sector ICT Systems 27
7. CYBERSECURITY AND DATA PROTECTION 29
7.1 Regulatory Framework 29
7.1.1. Nigeria Data Protection Act (NDPA) 29
7.1.2. Cybercrimes (Prohibition, Prevention, etc.) Act of 2015 29
7.2 Cybersecurity Incidents 29
7.2.1. Types of Cyber Threats 30
7.2.2. Inadequate Cybersecurity Measures 30
7.2.3. Addressing Cybersecurity Challenges 30
8. DIGITAL LITERACY AND INCLUSION 30
8.1 Digital Literacy Levels 33
8.2 Inclusion Efforts 42
9 OFFENCES AND PENALTIES RELATED TO THE DIGITAL ECONOMY 35
9.1 Enforcement Challenges 35
9.2 Judicial Capacity 35
10. CONCLUSION 37
REFERENCES 38

List Of Abbreviations

APT	**Advanced Persistent Threats**
BVN	**Bank Verification Number**
CBN	**Central Bank of Nigeria**
DML	**Digital Money Lenders**
FCCPA	**Federal Competition and Consumer Protection Act**
FCCPC	**Federal Competition and Consumer Protection Commission**
FMCI&DE	**The Federal Ministry of Communications, Innovations and Digital Economy**
IPPIS	**Integrated Payroll and Personnel Information System**
NBA	**Nigerian Bar Association**
NCC	**Nigeria Communications Commission**
NDPB	**Nigeria Data Protection Bureau**
NDPC	**Nigeria Data Protection Commission**
NDEPS	**National Digital Economy Policy and Strategy**
NDPR	**Nigeria Data Protection Regulation**
NIBBS	**Nigerian Inter-bank Settlement System**
NITDA	**National Information Technology Development Agency**
MNO	**Mobile network operator**
TSA	**Treasury Single Account**
3MTT	**3 Million Technical Talent**

Executive Summary

This paper presents a comprehensive synthesis of key issues addressed in Nigeria's National Digital Economy and E-Governance Bill. As the country embarks on a transformative journey towards a fully digital economy, this bill is poised to play a critical role in shaping the future of digital transactions, electronic commerce, consumer protection, government services, and cybersecurity.

This analysis is based on a thorough review of secondary data from credible sources, including government reports, industry publications, and academic studies. By compiling and analysing this data, the paper provides a baseline assessment of Nigeria's current digital landscape.

The synthesis explores infrastructure and adoption levels of digital transactions and e-commerce, evaluating how deeply these systems are integrated into the daily economic activities of Nigerians. It also examines the legal frameworks and challenges associated with electronic contracts and signatures, identifying gaps in awareness and trust that may hinder broader adoption.

Furthermore, the paper examines consumer protection issues within the digital economy, highlighting concerns over data privacy, cybersecurity threats, and the eff ectiveness of current regulatory measures. It also assesses the readiness and implementation challenges in Nigeria's public sector, highlighting key challenges such as inadequate infrastructure, low digital literacy, and resistance to digital transformation.

The report extends to cybersecurity and data protection, evaluating the strength of existing frameworks and identifying persistent vulnerabilities. Additionally, it considers the state of digital literacy and inclusion, particularly in underserved regions, and ongoing eff orts to bridge these gaps.

This synthesis aims to provide policymakers, stakeholders, and academics with a comprehensive understanding of the challenges and opportunities associated with the National Digital Economy and E-Governance Bill. By presenting an evidence-based perspective, the paper seeks to inform the strategic decisions that will support the successful implementation of the bill, ultimately advancing Nigeria's digital economy and governance.

1.0 Introduction

The National Digital Economy and E-Governance Bill is a crucial legislative eff ort designed to accelerate Nigeria's transition into a digitally driven economy. As digitalisation reshapes industries and economies globally, this bill seeks to position Nigeria competitively by integrating digital technologies across sectors to boost economic growth, improve governance, and increase effi ciency in public and private services.

The bill's core objectives include promoting the validity and adoption of digital transactions, establishing a legal framework for electronic contracts and signatures, and ensuring robust consumer protection in the digital marketplace. It also seeks to streamline government services through digital means, build resilient digital infrastructure, enhance cybersecurity measures, and improve digital literacy across the population.

This paper synthesises existing evidence in these areas, drawing from credible secondary sources to assess Nigeria's digital ecosystem. It also highlights the progress made, the challenges that persist, and the opportunities that lie ahead, off ering valuable insights for policymakers, stakeholders, and researchers.

In the sections that follow, the paper explores the state of digital transactions and electronic commerce in Nigeria, the adoption and challenges of electronic contracts and signatures, and the adequacy of consumer protection measures in the digital space. It also examines the current landscape of digital government services, the infrastructure required to support these services, the state of cybersecurity, and the level of digital literacy among the Nigerian populace. Through this comprehensive analysis, the paper off ers insights that are crucial for shaping the future of Nigeria's digital economy and governance.

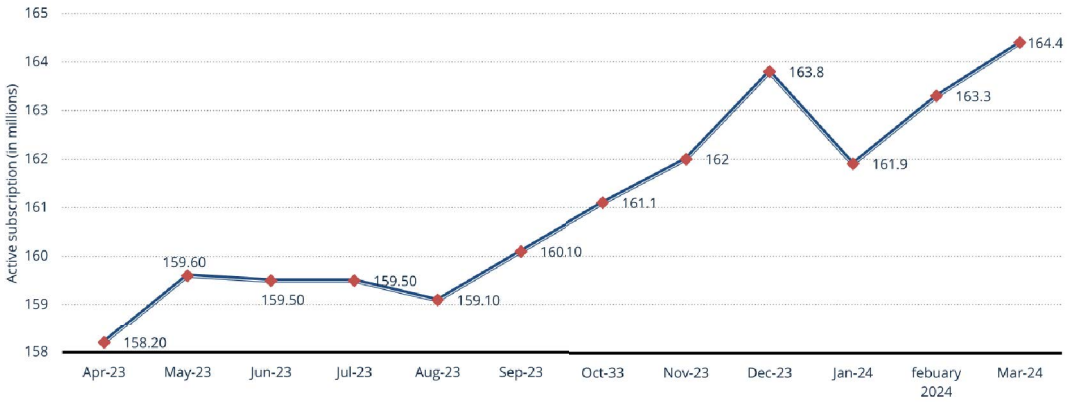
2.0 DIGITAL TRANSACTIONS AND ELECTRONIC COMMERCE

2.1 Internet Penetration

Internet penetration is a critical driver for digital transactions and the broader e-commerce ecosystem. The Internet provides the foundational infrastructure that allows individuals and businesses to engage in the digital economy, facilitating online transactions, digital communication, and access to e-services. As of January 2024, Nigeria's internet penetration rate was estimated at approximately 45.5%. However, data from NCC confi rms a decline of 1.9 million internet users compared to December 2023, with the total number dropping from 163.8 million to 161.9 million[1]. Despite this decline, the adoption of newer network technologies like 4G and 5G continues to progress signifi cantly[2].

[1] Nigerian Communication Commission, "Subscriber Data," ncc.gov.ng, 2024, https://ncc.gov.ng/statistics-reports/subscriber-data.
[2] Nigerian Communication Commission, ""Percentage(%) Market Share by Generation," ncc.gov.ng. https://ncc.gov.ng/industry-statistics
[3] Ibid

Active Internet subscription in Nigeria (April 2023- March 2024)



Description: The chart shows the fl uctuations in the number of active subscriptions over this period, highlighting the increase and decrease each month. The highest record in this time period is March 2024. However, subscription is predicted to fall in the second and third quarters due to sim barring in August 2024.

Note(s): Nigeria, April 2024

Source(s): Nigerian Communication Commission (2024)[3]

This growing user base represents a signifi cant opportunity for the expansion of digital commerce and the adoption of electronic transactions. Increase in the penetration rate is driven by increased access to aff ordable mobile devices, the proliferation of internet service providers (ISPs), and the expansion of broadband services, particularly in urban areas[4]. Mobile internet, in particular, has played a major role in this growth, with many Nigerians relying on smartphones as their primary means of internet access[5].

However, internet access remains unevenly distributed across the country. While urban centres like Lagos, Abuja, Kano and Port Harcourt enjoy relatively high penetration rates and robust internet infrastructure, rural areas lag signifi cantly behind[6].

This digital divide poses a challenge to the equitable adoption of digital services and the implementation of the National Digital Economy and E-Governance Bill. Without addressing these disparities, the full potential of digital transactions and e-commerce cannot be realised, particularly in underserved regions where internet access remains limited or unreliable.

The growth in internet penetration also raises important considerations for digital literacy and cybersecurity. As more Nigerians come online, there is an increased need for education on safe internet practices and the protection of personal data. There is also a need for policies and regulations that promote online safety and internet freedom. Furthermore, the growing internet access rates also present an opportunity to enhance digital inclusion. By addressing the digital divide, more citizens can actively participate in the digital economy, access government services online, and engage in e-governance initiatives[7]. These initiatives would also collectively contribute to social and economic equality in Nigeria.

While Nigeria's internet penetration - particularly in urban areas - has witnessed commendable growth, achieving a more uniform and inclusive digital landscape remains a key challenge. Addressing the digital divide and ensuring that all regions of the country have adequate internet access is important for the success of the National Digital Economy and E-Governance Bill and for fostering a truly inclusive digital economy.

[4] Nigeria's Mobile Growth Telegeography. (2023, December 5). Nigeria: Africa's mobile giant. Telegeography.https://blog.telegeography.com/nigeria-africas-mobile-giant. Smartphone Penetration in Nigeria Premise. (2023, October). Smartphone penetration in Nigeria. Premise. https://premise.com/wp-content/uploads/Smartphone-penetration-Nigeria.pdf

[5] Dorcas Agambila, "10 countries with the highest percentage of web traffi c from mobile phones," Business Insider Africa, February 24, 2025, https://africa.businessinsider.com/local/lifestyle/10-countries-with-the-highest-percentageof- web-traffi c-from-mobile-phones

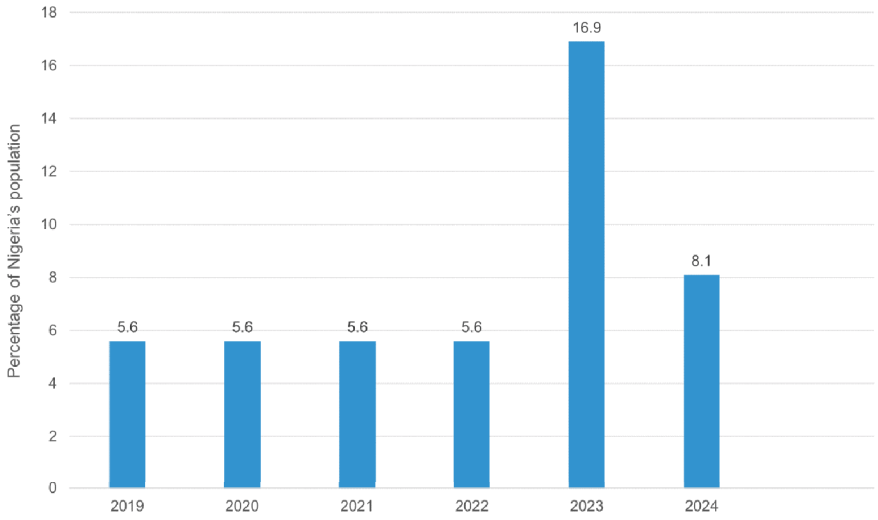
[6] Richard Adeleke, "Digital Divide in Nigeria: The Role of Regional Diff erentials," African Journal of Science, Technology, Innovation and Development 13, no. 3 (May 13, 2020): 1–14, https://doi.org/10.1080/20421338.2020.1748335.

[7] World Bank Group, "Nigeria Digital Economy Diagnostic: A Plan for Building Nigeria's Inclusive Digital Future," World Bank (World Bank Group, February 10, 2020), https://www.worldbank.org/en/country/nigeria/publication/nigeria-digital-economy-diagnostic-a-plan-for-bui lding-nigerias-inclusive-digital-future#:~:text=The%20Nigeria%20Digital%20Economy%20Diagnostic%20sa ys%20that%20with%20improvements%20in.

2.2 Adoption of Mobile Money and E-Payments

The adoption of mobile money and e-payments in Nigeria has experienced remarkable growth in recent years, signalling a signifi cant shift in how financial transactions are conducted within the country. According to the Central Bank of Nigeria (CBN), mobile money transactions reached a milestone of over ₦6 trillion in 2023, underscoring the increasing reliance on digital financial services [8]. This surge in digital transactions refl ects a broader movement toward financial inclusion and digital transformation within Nigeria's economy, and an increasing adoption of financial digital tools.

Description:



Description: Share of the population reporting to use mobile money accounts in Nigeria from 2019 to 2024

Note(s): Nigeria, February 2024

Source(s): Statista

Several factors have driven this growth, with fintech companies playing a pivotal role. Companies such as Paystack and Flutterwave have revolutionised Nigeria's financial landscape by providing innovative and accessible payment solutions[9]. These platforms have made it easier for businesses and individuals to conduct transactions online, accept payments, and transfer money with greater convenience and security[10]. Their user-friendly interfaces and robust payment gateways have lowered barriers to entry for digital financial services, particularly for small and medium-sized enterprises (SMEs) that previously relied on cash-based transactions.

The impact of mobile money and e-payments extends beyond urban centres, reaching even remote and rural areas where traditional banking infrastructures are limited or non-existent[11]. NIBSS highlighted that Opay and Palmpay, two mobile fintech companies, were the most prominent Non-Mobile Network Operator (NMO) transaction providers and have gained signifi cant market share in Nigeria since receiving their Mobile Money Operators licences in 2018 and 2019 respectively[12]. As of October 2023, OPay was the most downloaded app in the country, with over 30 million users, 500,000 agents, and about 300,000 merchants in both urban and rural centres in Nigeria[13].

[8] Central Bank of Nigeria, Annual Report 2023.
[9] Deloitte, "Nigeria Cybersecurity Outlook 2024," Deloitte
[10] Ernest, B. (2024). The Rise of Fintech: How Africa is Leading the Digital Finance Revolution. African Leadership Magazine. Available at: https://www.africanleadershipmagazine.co.uk/the-rise-of-fintech-how-africa-is-leading-the-digital-finan ce-revolution/ [Accessed 1 Apr. 2025].
[11] Osabutey, E.L.C. and Jackson, T., 2024. Mobile money and financial inclusion in Africa: Emerging themes, challenges and policy implications. Technological Forecasting and Social Change, [online] Available at: https://www.sciencedirect.com/science/article/pii/S0040162524001355 [Accessed 1 Apr. 2025].
[12] Saka Olalekan, "Nigeria Recorded N600 Trillion E-Payment Transactions in 2023," NIBSS, February 9, 2024, https://nibss-plc.com.ng/nigeria-recorded-n600-trillion-e-payment-transactions-in-2023/.
[13] Temitayo Jaiyeola, "Analysis: How Telcos, Fintechs Are Driving Nigeria's Mobile Money Growth - Businessday NG," Businessday NG, March 25, 2024, https://businessday.ng/technology/article/analysis-how-telcos-fintechs-are-driving-nigerias-mobilemoney- growth/#:~:text=As%20of%20 October%202023.; Stefano Venza, "Let's Meet OPay, the SoftBank-Backed Fintech That Is Outstanding Even TikTok," Inclusivemoney.com (NeoBanking EN,December 12, 2023), https://inclusivemoney.com/fintech/opay#:~:text=According%20to%20Data.Ai%2C%20OPay%20isn%E2%80%99t%20just%20 Nigeria%E2%80%99s%20most.

The growth of mobile money and e-payments has also been fueled by regulatory support from the CBN, which has created a conducive environment for fintech innovation. The introduction of policies aimed at promoting cashless transactions, such as the National Financial Inclusion Strategy (NFIS), has further accelerated the adoption of digital payment methods.

However, despite these advancements, challenges remain.

The security of e-payments and mobile money services remains a concern, especially as cyber threats become more sophisticated[14]. Additionally, interoperability challenges between diff erent mobile money platforms can hinder seamless transactions across networks. The digital divide limits the reach of these services in some rural and underserved areas, where internet access and digital literacy are low. These populations are also at high risk of financial scams, cybersecurity threats, and other malicious activities relating to digital products.

The adoption of mobile money and e-payments in Nigeria is a critical step towards achieving a more inclusive and effi cient financial system[15]. The sector's rapid growth highlights the transformative potential of digital financial services. However, to sustain and expand this growth, ongoing eff orts are needed to address security challenges, enhance interoperability, and ensure that the benefi ts of digital finance reach all segments of the population.
The continued support of fintech innovation and regulatory oversight will be crucial in driving the success of mobile money and e-payments as part of Nigeria's broader digital economy strategy.

2.3 Legal Recognition of Electronic Transactions

The legal recognition and enforceability of electronic transactions are critical components of a functioning digital economy. In Nigeria, while the adoption of digital transactions has grown substantially, the legal infrastructure supporting these transactions has not fully matured, leading to ongoing challenges[16]. Cybercrimes (Prohibition, Prevention, etc.) Act of 2015 was a signifi cant legislative eff ort to provide a framework for the legal recognition of electronic transactions, yet several gaps and inconsistencies remain in its enforcement [17].

The Cybercrimes Act addresses various aspects of electronic transactions, including the use of electronic signatures, digital contracts, and the prevention of cybercrimes. However, despite these provisions, the practical enforceability of electronic contracts is still a work in progress[18]. The Act provides for the admissibility of electronic evidence in legal proceedings, which is crucial for resolving disputes arising from electronic transactions. Nonetheless, the practical extent to which courts and other legal institutions are equipped to handle these issues varies, and the interpretation of 'electronic evidence' can be inconsistent.

[14] Deloitte. (2025). Nigeria's cybersecurity landscape in 2025. [online] Available at: https://www.deloitte.com/ng/en/services/risk-advisory/perspectives/Nigerias-cybersecurity-landscape-in-2025.html [Accessed 1 Apr. 2025].
[15] Osabutey, E.L.C. and Jackson, T., 2024. Mobile money and financial inclusion in Africa: Emergingthemes, challenges and policy implications. Technological Forecasting and Social Change, 202,123339. Available at: https://www.sciencedirect.com/science/article/pii/S0040162524001355[Accessed 1 Apr. 2025].
[16] Global Law Experts, "E-commerce in Nigeria: Legal Framework and Challenges," Global Law Experts, August 12, 2024,"E-commerce in Nigeria: Legal Framework and Challenges," Global Law Experts
[17] Cybercrimes (Prohibition, Prevention, etc.) Act. 2015.
[18] Ibid p.8

A major challenge in Nigeria's digital economy is the inconsistent enforcement of existing laws[19]. While the Cybercrimes Act provides a legal framework, its enforcement varies across jurisdictions and sectors. This inconsistency creates uncertainty among businesses and consumers, who may be hesitant to fully engage in digital transactions due to concerns about legal protection and dispute resolution[20].

Public trust in electronic transactions is also still developing. Many consumers and businesses remain wary of the reliability and security of digital contracts and signatures[21]. This scepticism has grown alongside the rise in digital transactions, highlighting the clear disconnect between legal recognition and user confi dence. Despite the provisions of the Cybercrimes Act, many Nigerians remain cautious of fraud, data breaches and other cyber threats, unsure whether the system can truly safeguard their interests.

Beyond these enforcement and trust issues, the current legal framework also fails to address all the complexities associated with modern electronic transactions. Critical areas such as cross-border e-commerce, digital identity verifi cation, and the use of emerging technologies like blockchain remain largely unregulated or inadequately addressed. These gaps necessitate ongoing legislative updates and regulatory enhancements to ensure that the legal infrastructure keeps pace with technological advancements.

While Nigeria has made important strides in the legal recognition of electronic transactions through the Cybercrimes Act of 2015, signifi cant challenges remain in the consistent enforcement of these laws and in building public trust. To support the continued growth of the digital economy, it is essential to strengthen legal frameworks, improve enforcement mechanisms, and enhance public awareness and confi dence in the security and reliability of electronic transactions[22]. Addressing these issues will be crucial for the successful implementation of the National Digital Economy and E-Governance Bill and for fostering a robust and trusted digital marketplace in Nigeria.

[19] Yejide Gbenga-Ogundare, "Despite legislations, poor enforcement mechanism militate against fight against cybercrimes," Nigerian Tribune, September 27, 2023,https://tribuneonlineng.com/despite-legislations-poor-enforcement-mechanism-militate-against-fight-against-cybercrimes
[20] Robinson Sibe, "Council Post: Cybercrime and the Challenge of Static Legislations in Nigeria," Forbes, August 12, 2024.
[21] Anugbum Onuoha, James Agbadufi shim, and Peter Ortese, "A Critical Analysis of the Validity and vEnforceability of Electronic Contract in Nigeria: Need for Reforms," Global Journal of Politics and Law Research 8, no. 5 (2020): 13–30
[22] Robinson, sibe. Cybercrime and the Challenge of Static Legislations

3.0 ELECTRONIC CONTRACTS AND SIGNATURES

3.1 Current Legal Framework

The Evidence Act of 2011 legally recognises electronic signatures, marking a signifi cant step in aligning Nigeria's legal framework to the demands of a digital economy. The Act explicitly acknowledges the validity of electronic signatures, providing a legal foundation for the use of electronic contracts in various commercial and administrative transactions.[23] This legal recognition is vital for facilitating e-commerce, digital communications, and online agreements which rely on electronic authentication.

3.1.1. Legal Provisions Under the Evidence Act

Under the provisions of the Evidence Act,[24] electronic signatures are deemed legally equivalent to handwritten signatures, provided they meet certain criteria for authenticity and reliability. Specifi cally, the Act requires that electronic signatures must be:

- Created in a manner that ensures their authenticity,
- Linked to the signatory in a way that is uniquely attributable,
- Capable of being verifi ed by all parties involved.

This legal framework is essential as it underpins the legitimacy of digital contracts and allows businesses to operate in the digital space with the confi dence that their electronic transactions are legally binding and enforceable.

3.1.2. Legal Provisions Under Cybercrimes (Prohibition and Prevention) Act

On the issue of the validity of electronic contracts and e-signatures, this is established in section 17 (1)(a) of the Cybercrimes (Prohibition and Prevention) Act, 2015, The Cybercrimes (Prohibition and Prevention) Act 2015[25] makes provisions for the use of electronic signature in Nigeria for general business use, other business transactions including, NDA, employee contracts, privacy notice, commercial agreements, and customer agreements. On the other hand, section 17(2) of the Cybercrimes Act makes exemption on its usage in;

- wills, codicils, and other testamentary documents
- death and birth certifi cates,
- matters of family law such as divorce, adoption
- issuance of court orders and legal requirements in affi xing a signature, etc.

3.1.3. Legal Provisions Under the Companies and Allied Matters Act (CAMA) 2020

Section 101 of the Companies and Allied Matters Act (CAMA) 2020 further strengthens the legal foundation for electronic signatures in corporate transactions and filings.[26] The Act permits documents to be signed electronically by directors and other authorised offi cers of the company, eliminating the need for execution as a deed. The Corporate Aff airs Commission (CAC) now accepts e-signatures for the registration and incorporation of business entities, with handwritten signatures being electronically uploaded via the Company Registration Portal (CRP) during the registration process[27]. This contends the pre-existing CAMA 1990 which lacked provisions for e-signatures in the registration process.

Under the CAMA Act 2020, companies must ensure compliance with the following electronic execution requirements:

- Lawyers handling the registration of new companies are required to advise their clients to incorporate electronic signatures into the company's constitutional documents, particularly the Articles of Association.

[23] Evidence Act, 2011.
[24] Ibid see Section 1(a)
[25] Cybercrimes (Prohibition and Prevention) Act 2015. CyberCrime__Prohibition_Prevention_etc__Act__2015.pdf (cert.gov.ng)
[26] Companies and Allied Matters Act (CAMA). 2020
[27] Companies and Allied Matters Act (CAMA). 2020

- Before proceeding with electronic execution, companies should review their Articles to ensure that the constitutional documents do not explicitly require in-person execution or prohibit the use of electronic signatures.

- For added certainty, some companies may choose to expressly authorise the electronic execution of documents through a board resolution.

3.1.4. Challenges in Adoption

Despite legal recognition, the adoption of electronic contracts and signatures among businesses, particularly small and medium-sized enterprises (SMEs), remains relatively low. This reluctance can be attributed to several interrelated factors:

1. Lack of Awareness

Many businesses, especially SMEs, are unaware of the legal validity of electronic signatures and contracts. A 2021 survey by the Nigerian Bar Association in 2021 found that over 60% of SME respondents were either unaware or unsure about the legal status of electronic signatures in Nigeria [28]. This widespread lack of understanding prevents businesses from leveraging digital contracts, missing out on quicker processing times and lower transaction costs.

2. Mistrust in Digital Authentication

Even among businesses that are aware of electronic signatures, there is often a deep-seated mistrust in the security and reliability of digital authentication processes[29]. Concerns about the potential for fraud, hacking, and unauthorised use of digital signatures discourage many businesses from embracing this technology[30]. High-profi le cases of cybercrime and data breaches have further fueled these fears, leading to a preference for traditional, paper-based contracts.[31] According to a 2022 report by the National Information Technology Development Agency (NITDA), over 45% of businesses cited identity theft and data breaches as key risks associated with electronic signatures.

3. Technical and Cost Barriers

Implementing and verifying electronic signatures requires infrastructure, software and technical expertise. This may pose signifi cant challenges, especially for smaller businesses with limited resources. The cost of acquiring digital signature tools in Nigeria can range from ₦50,000 to ₦150,000 per user annually and this is often seen as prohibitive for SMEs [32]. Additionally, the need for technical expertise to manage these tools and ensure their proper use can be a signifi cant barrier for businesses with limited IT capacity. Furthermore, inconsistencies in the application and enforcement of the legal framework across diff erent jurisdictions create uncertainty and may deter businesses from adopting electronic contracts[33].

[28] Nigerian Bar Association. . Survey on the Use of Electronic Contracts and Signatures among Legal Practitioners in Nigeria. Nigerian Bar Association. 2021
29 Godfrey George, "How fake alerts, network glitches undermine digital trust in Lagos markets,"Punch, February 15, 2025, https://punchng.com/how-fake-alerts-network-glitches-undermine-digital-trust-in-lagos-markets
[30] Anugbum Onuoha, James Agbadufi shim, And Peter Ortese, "A Critical Validity And Enforceability Of Electronic Contract
[31] NITDA ,Annual Report 2022
[32] Purple Digitals, "7 Best e-Signature Platforms for Every Nigerian Business in 2024," Purple Digitals, March 27, 2024.https://purpledigitals.com/best-e-signature-platforms/
[33] Anugbum Onuoha, James Agbadufi shim, And Peter Ortese, "A Critical Validity And Enforceability Of Electronic Contract

4. Uncertainty in E-signature Requirements for Different Transactions

The current regulatory frameworks in Nigeria lack clear guidelines on the type of e-signatures required for diff erent transactions[34]. Unlike in other jurisdictions, there are no defi ned standards on the validity and formality of e-signatures; verifi cation mechanism as outlined in section 93 (2) of the Evidence Act; identity verifi cation of signatories; and cross-border recognition and admissibility of e-signatures (where executed in Nigeria). In the absence of a robust framework that addresses these complexities, customers may continue to carry out complex transactions with simple e-signatures which puts them at risk of cybersecurity threats, breaches and disputes.

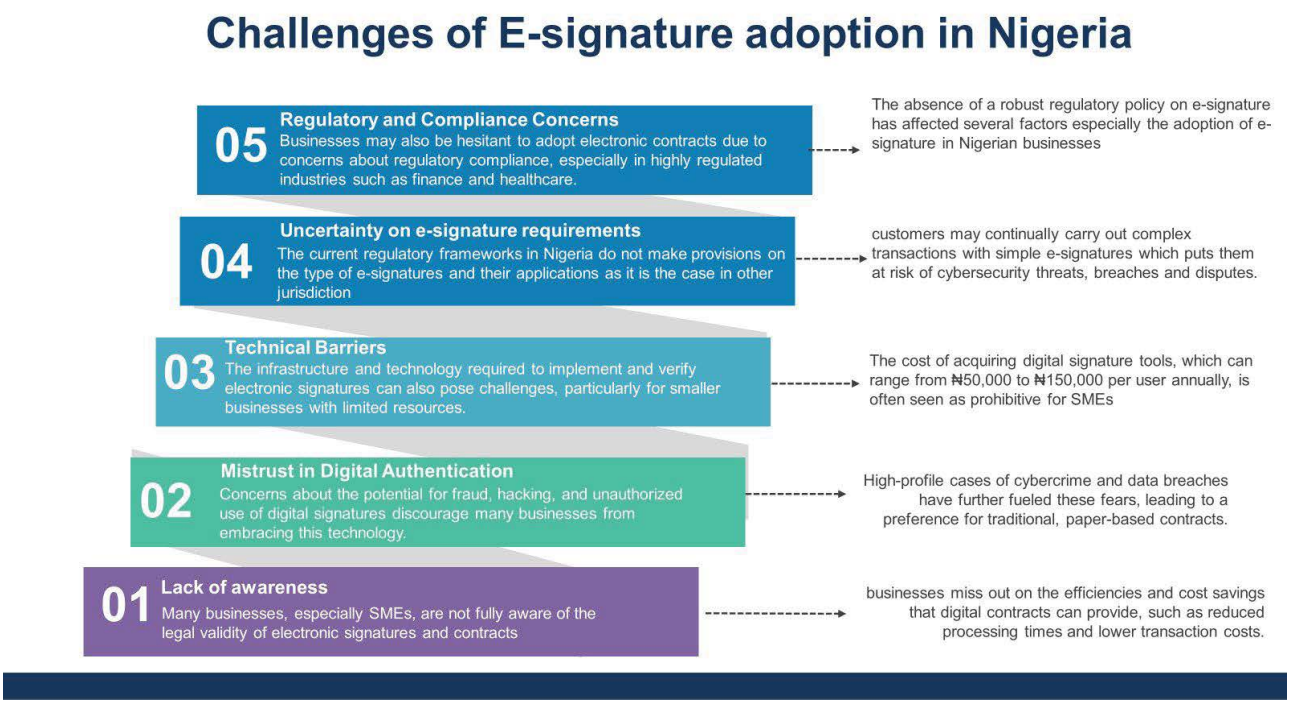
5. Regulatory and Compliance Concerns

Businesses operating in highly regulated industries - such as finance and healthcare - may also be hesitant to adopt electronic contracts due to concerns about regulatory compliance.[35] The lack of clear guidelines on how electronic signatures should be implemented and verifi ed can create legal ambiguities, which businesses prefer to avoid.

For instance, financial sector regulations often demand a high level of document security and verifi cation, which some businesses feel electronic signatures may not fully satisfy under the current framework.[36]
Further complicating the issues is the stalled Electronic Transaction Bill (2017)[37] which was passed by the Senate in 2017 but has yet to receive presidential assent. The bill seeks to provide regulatory oversight and establish a legal framework for electronic transactions in Nigeria.

Overall, the absence of a robust regulatory policy on e-signature has aff ected several factors including; the growth and adoption of e-signature on digital platforms; the use of digital signature in Nigerian businesses, especially SMEs and financial organisations; and the progress of Nigeria as a digital economy[38].

[34] Trusted Advisors. (2024). Understanding Electronic Contracts and Signatures in Nigeria: Legal Insights. Trusted Advisors Law. Available at:https://trustedadvisorslaw.com/understanding-electronic-contracts-and-signatures-in-nigeria-legal-insights/ [Accessed 1 Apr. 2025].
[35] Aidonojie, P.A., Majekodunmi, T.A. and Adeyemi-Balogun, O.J., 2023. The Legal Issues Concerning the Operation of Fin-Tech in Nigeria. Jurnal Media Hukum, 30(2), pp.78–97. Available at:https://doi.org/10.18196/jmh.v30i2.18337 [Accessed 1 Apr. 2025].
[36] NBA, Survey on Electronic contract
[37] National Assembly, "Electronic Transaction Bill" (2017).
[38] Mondaq, "Revisiting Electronic Contracts and Signatures: Perspectives on Digitisation and the Law in Nigeria," Mondaq.com (Marcus-Okoko & Co, March 25, 2022),https://www.mondaq.com/nigeria/contracts-and-commercial-law/1175714/revisiting-electronic-contracts-and-signatures-perspectives-on-digitisation-and-the-law-in-nigeria#:~:text=The%20interaction%20between%20the%20parties%20in%20forming%20the%20contract%20can.



Description: The image shows the challenges that face the adoption of e-signatures and e-contracts in Nigeria

Note(s): Nigeria, September 2024

Source(s): API, GINGER project

3.1.5. Overcoming Adoption Barriers

Addressing the challenges that limit the adoption of electronic signatures requires a multi-pronged approach which will focus on awareness, security, accessibility and regulatory clarity.

Raising awareness about the legal validity and practical benefi ts of electronic signatures while highlighting their security features[39] is crucial. Especially for SMEs, targeted educational campaigns and training programs can help demystify electronic signatures and increase its use. Additionally, developing user-friendly digital signature platforms that are accessible to SMEs could help lower the barriers to adoption. Building trust and reliability in digital authentication is also important.

Digital authentication processes can be strengthened, for instance, through advanced encryption methods and blockchain technology for secure digital signatures.

Finally, clearer regulatory guidelines and consistent enforcement are needed to provide businesses with the confi dence that electronic contracts are legally binding and enforceable across all sectors. Strengthening the judiciary's capacity to handle disputes involving electronic contracts will also be essential in building trust and ensuring that businesses feel secure in using electronic contracts.

While the Evidence Act of 2011[40] provides a strong legal foundation for electronic signatures and contracts, the actual uptake among businesses, particularly SMEs, has been limited. Overcoming the barriers of awareness, trust, technical challenges, and regulatory concerns is essential for realising the full potential of electronic transactions in Nigeria's digital economy. By addressing these challenges, Nigeria can fully leverage digital authentication to enhance business operations, increase effi ciency, and drive economic growth.

[39] Mondaq, "Revisiting Electronic Contracts and Signatures: Perspectives on Digitisation and the Law in Nigeria,"
[40] Evidence Act, 2011.

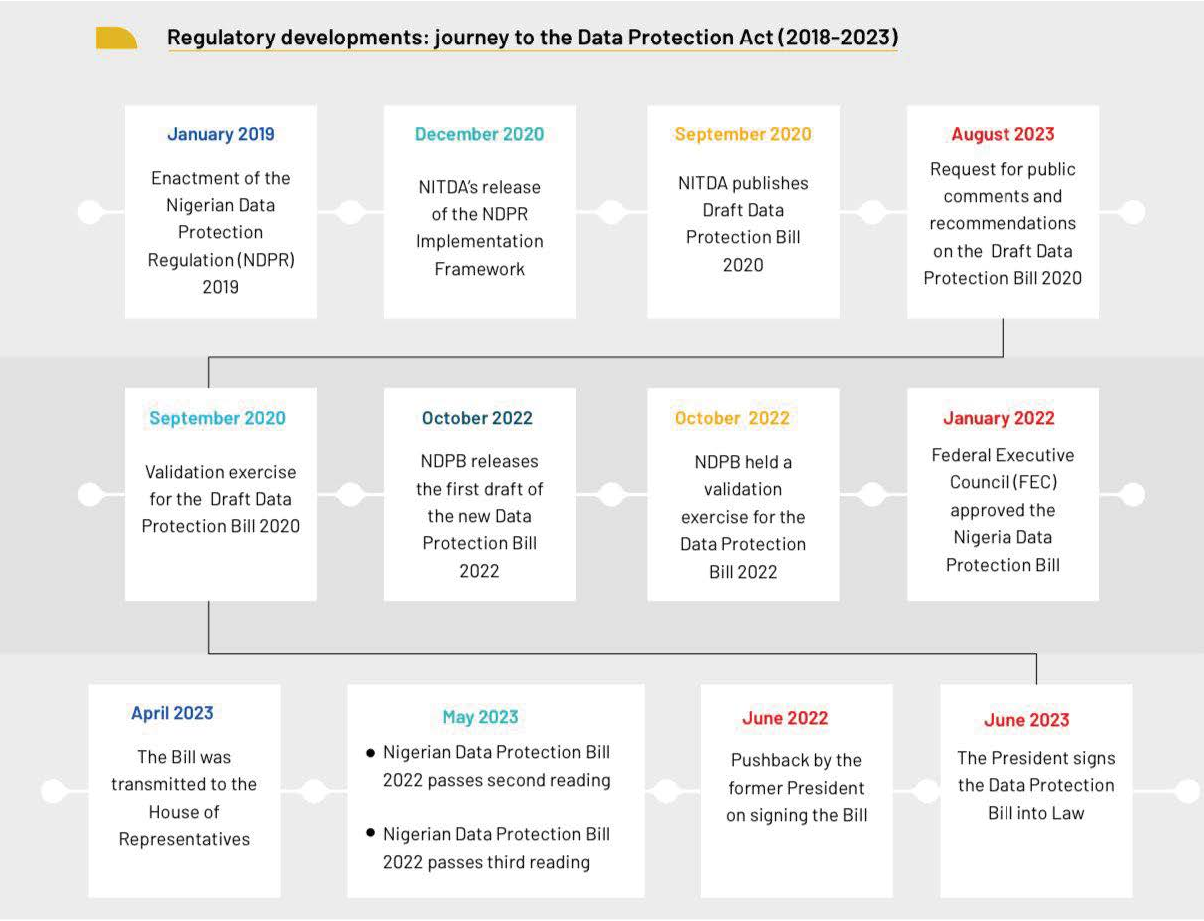
4.0 CONSUMER PROTECTION IN DIGITAL COMMERCE

4.1 Consumer Awareness and Protection

As Nigeria's digital economy continues to expand, consumer protection in digital commerce has become increasingly important. As more consumers engage in online transactions, concerns regarding data privacy and protection have grown, revealing the need for stronger safeguards and greater public awareness in the digital space. [41]

4.1.1. Data Privacy and Protection

The Nigeria Data Protection Act (NDPA), which replaced the Nigeria Data Protection Regulation (NDPR), remains a primary legal framework for personal data protection. The NDPA sets out clear requirements for the collection, processing, and storage of personal information, aiming to ensure that data is handled securely and confi dentially. It mandates that organisations involved in data processing must implement measures to protect data against unauthorised access, breaches, and misuse[42].



Description: The figure shows the regulatory journey of the Data Protection Act from 2018 to 2023. The supervising authority for the Act has also seen signifi cant changes since its initiation from NITDA to NDPD to NDPC.

Note(s): Nigeria, December 2023

Source(s): Tech Hive Advisory and Ikigai Innovation Initiative

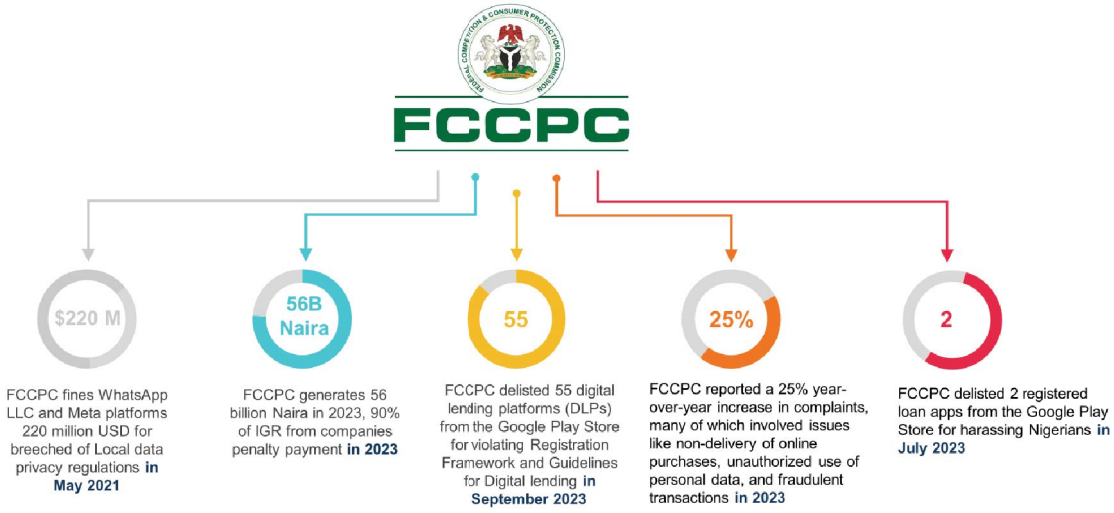
[41] KPMG, "The Consumers Right Awareness and Protection: A Means to Economic Development," KPMG (KPMG, June 2, 2021), https://kpmg.com/ng/en/home/media/press-releases/2021/04/the-consumers-right-awareness-and-protection-a-means-to-economic-development.html#:~:text=The%20Consumers%20Right%20Awareness%20and%20Protection:%20A%20Means%20to%20Economic.
[42] Nigeria Data Protection Commission, "NIGERIA DATA PROTECTION ACT," 1 § (2023)

Despite the NDPA's robust framework, enforcement has been inconsistent, limiting its overall eff ectiveness[43]. The National Information Technology Development Agency (NITDA) is tasked with ensuring compliance, but many businesses, especially small and medium-sized enterprises (SMEs), struggle with the technical and financial resources needed to fully adhere to the Regulation[44]. As a result, there have been several reported cases of data breaches that have compromised consumer information, highlighting the need for stronger enforcement and support for businesses to achieve compliance[45].

4.1.2. Consumer Complaints and Regulatory Response

The Federal Competition and Consumer Protection Commission (FCCPC) has observed a signifi cant increase in consumer complaints related to digital transactions. In 2023 alone, the FCCPC reported a 25% year-over-year increase in complaints, many of which involved issues like non-delivery of online purchases, unauthorised use of personal data, and fraudulent transactions[46]. This rise in complaints underscores the growing risks that consumers face in the digital marketplace and the urgent need for enhanced consumer protection measures.

Within the digital lending space, FCCPC has enacted sanctions and delisted digital apps for violating the Registration Framework and Guidelines for Digital Lending[47].



Description: The figure shows recent data from FCCPC relating to consumer protection and security in the digital landscape

Note(s): Nigeria, September 2024

Source(s): API, GINGER project

A key issue highlighted by the FCCPC is the lack of transparency and accountability among some digital service providers which makes dispute resolution diffi cult especially when it comes to recovering funds lost to fraudulent activities[48]. The cross-border nature of many digital transactions further complicates the enforcement of consumer rights, making it diffi cult for regulators to protect consumers eff ectively.

[43]Sami Tunji, "Nigeria's data privacy breaches surge amid regulatory pressure," Punch Newspaper, February 10, 2025. https://punchng.com/nigerias-data-privacy-breaches-surge-amid-regulatory-pressure
[44] Omaplex Law Firm, "An Assessment of the Effect of the Nigerian Data Protection Act (NDPA), 2023 on Data Privacy in Nigeria," Omaplex Law Firm, July 17, 2024, https://omaplex.com.ng/an-assessment-of-the-effect-of-the-nigerian-data-protection-act-ndpa-2023-on-data-privacy-in-nigeria
[45] National Information Technology Development Agency, "NATIONAL DIGITAL LITERACY FRAMEWORK FEDERAL MINISTRY of COMMUNICATIONS and DIGITAL ECONOMY," 2023, https://nitda.gov.ng/wp-content/uploads/2023/07/Digital-Literacy-Framework.pdf.
[46] Federal Competition and Consumer Protection Commission (2023). Annual Report.
[47] Federal Competition & Consumer Protection Commission, "Registration Of Digital Money Lenders Under The Inter Agency Joint Task Force's Limited Interim Regulatory/Registration Framework And Guidelines For Digital Lending 2022
[48] Federal Competition & Consumer Protection Commission, 2023,

4.1.3. Need for Enhanced Consumer Protection Measures

Addressing these challenges requires a multifaceted approach that combines strong regulatory enforcement, increased consumer awareness and the promotion of secure digital practices.

First, there is a need for more robust enforcement of existing regulations like the NDPA. Strengthening the capacity of regulatory bodies such as NITDA and the FCCPC to monitor compliance and take swift action against violations is crucial in ensuring compliance. This includes increasing the penalties for non-compliance to deter lax data protection practices.

Beyond enforcement, raising consumer awareness about their rights in the digital economy is important. The FCCPC has initiated several public education campaigns aimed at informing consumers about how to protect their personal data and navigate digital transactions safely. However, more targeted eff orts are needed, particularly in reaching vulnerable populations who may be less familiar with digital technologies[49].

Additionally, promoting the adoption of secure payment methods and encouraging the use of platforms that comply with international best practices in data protection can help mitigate risks. The introduction of a centralised complaint resolution platform, as proposed by the FCCPC, could also streamline the process for consumers to report issues and seek redress[50].

[49] Federal Competition and Consumer Protection Commission . (2023). Annual Report.
[50] " In accordance with section 17 (h) and (S) of the FCCPA 2018 Federal Competition and Consumer Protection Commission (FCCPC). (2023). Annual Report on Consumer Complaints and Digital Transactions. Retrieved from FCCPC Offi cial Website.https://fccpc.gov.ng/consumers/complaint-handling/International Journal of Computer Applications (0975-8887) Volume 186-N0. 55, December 2024:https://www.ijcaonline.org/archives/volume186/number55/ogene-2024-ijca-924275.pdf

4.2 Cybersecurity Threats

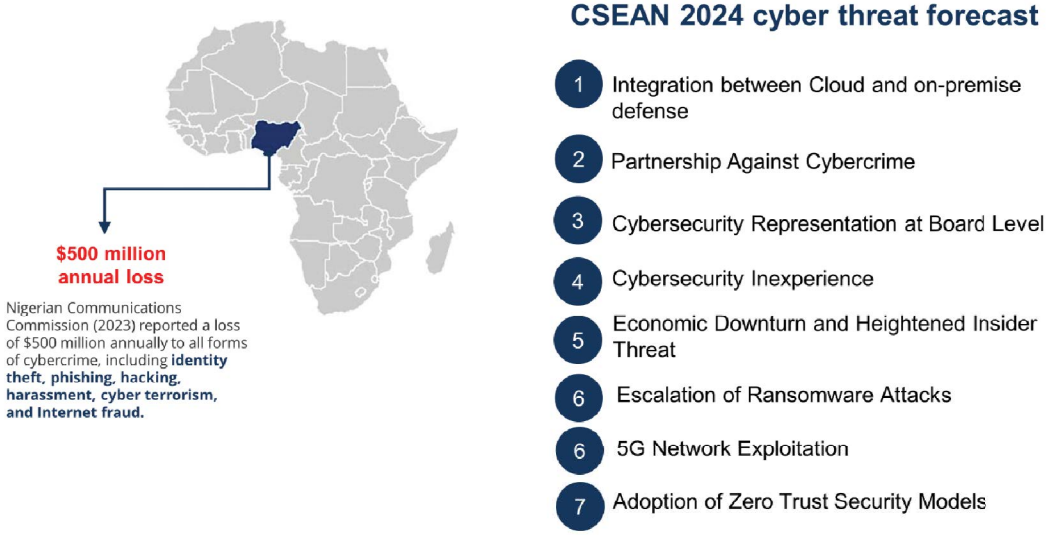
Cybersecurity has emerged as a critical challenge for Nigeria as the country continues to expand its digital economy. With the increasing reliance on digital platforms for commerce, finance, and communication, Nigeria has become an attractive target for cybercriminals[51]. The growing incidence of cyberattacks poses significant risks not only to businesses but also to consumers, undermining trust in digital transactions and potentially stalling the progress of the country's digital transformation. Implementing a strong cybersecurity architecture in Nigeria is a complex but beneficial endeavour that would require collaboration, commitment and smart technologies.

4.2.1. Rising Cybersecurity Threats

According to the Serianu Cybersecurity Report, Nigeria experienced substantial financial losses due to cybercrime in 2022, with the total estimated cost reaching approximately $500 million[52]. This figure underscores the severity of the threat posed by cybercriminals, who employ a variety of tactics ranging from phishing attacks and ransomware to more sophisticated forms of cyber intrusion targeting financial institutions, government agencies, and private enterprises[53].

The report highlights that phishing remains one of the most prevalent forms of cyber threats in Nigeria, accounting for a significant portion of reported incidents. Cybercriminals use deceptive emails and websites to trick individuals into disclosing sensitive information, such as passwords and credit card details, which are then used to commit fraud54. The widespread nature of these attacks has made them a major concern for both consumers and businesses[55].

Ransomware attacks have also become more common, with cybercriminals encrypting victims' data and demanding payment in exchange for decryption keys[56]. These attacks have affected businesses of all sizes, from small enterprises to large corporations and public institutions, leading to disruptions in operations and substantial financial losses. The healthcare and financial sectors have been particularly vulnerable to ransomware, given the sensitive nature of the data they handle[57].



Description: The figure shows the 2024 cyber threat forecast for Nigeria

Source(s): Cyber Security Experts Association of Nigeria (CSEAN)

[51] Serianu. (2022). Nigeria Cybersecurity Report 2022: Trends, Challenges, and Recommendations. Serianu Ltd.
[52] Serianu. (2022). Nigeria Cybersecurity Report 2022: Trends, Challenges, and Recommendations. Serianu Ltd.
[53] Robinson Sibe, Cybercrime and the Challenge of Static Legislations
[54] CSEAN 2024 cyber threat forecast
[55] CSEAN 2024 cyber threat forecast
[56] Tobi Tunji, "Nigerian organisations battle 3,759 weekly cyber-attacks – Report," Nairametrics, November 22, 2024, https://nairametrics.com/2024/11/22/nigerian-organisations-battle-3759-weekly-cyber-attacks-report/
[57] Ibid p.5

Moreover, advanced persistent threats (APTs) have emerged as a major concern with cybercriminals gaining unauthorised access to networks and remaining undetected for extended periods[58], gathering sensitive data or disrupting critical infrastructure. These sophisticated attacks are often linked to organised crime groups or state-sponsored actors, posing a signifi cant threat to national security and economic stability.

In 2023, the Minister of Communications, Innovation and Digital Economy forecasted incidences of high-profi le cyber-attacks during the general election[59]. As predicted, Nigeria's digital landscape was marked by cyber incidents ranging from phishing attacks, third-party attacks[60], insider-enabled attacks and ransomware attacks.

This underscores the urgent need for stronger cybersecurity measures and guidelines that directly address these rapidly evolving threats. Adopting best practices from more developed countries might also be helpful in strengthening Nigeria's cyber resilience.

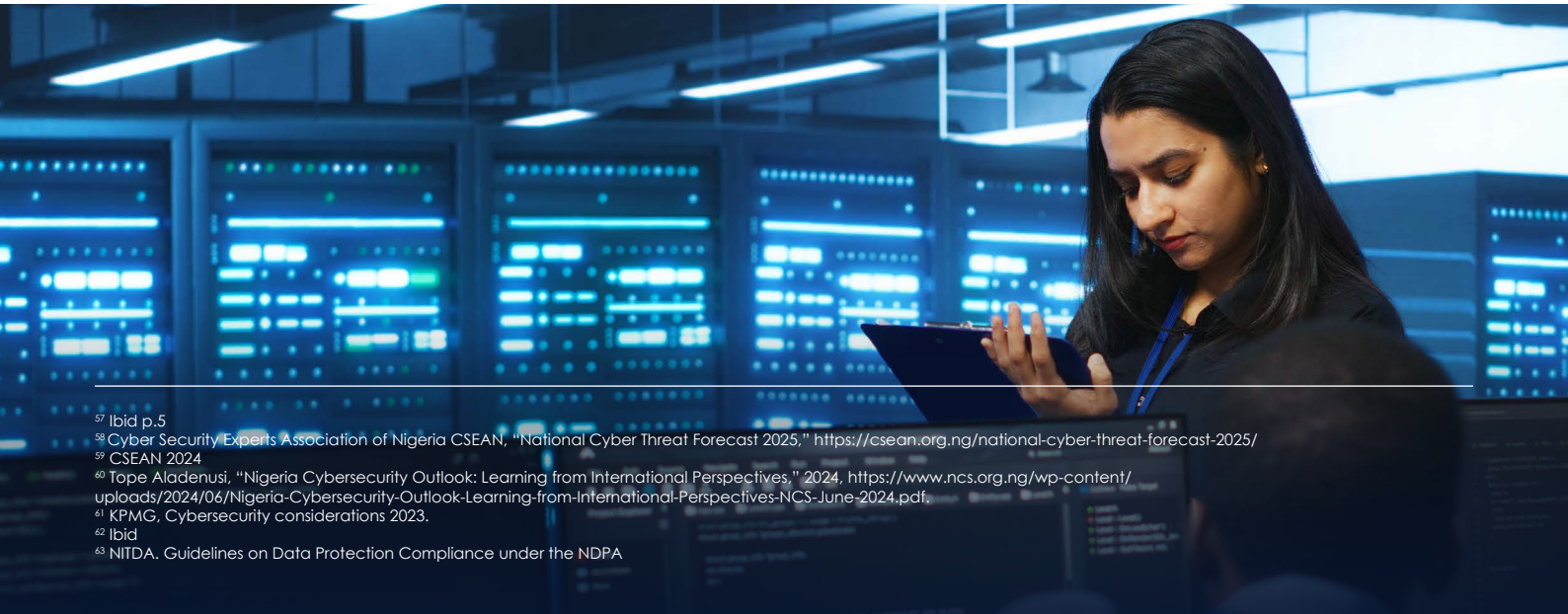
4.2.2. Impact on Consumer Trust

The rise in cybercrime has signifi cantly impacted consumer trust in digital commerce. With data breaches and fraudulent transactions, consumers are becoming more wary of engaging in online activities, particularly those that involve sharing personal and financial information. A KPMG Nigeria survey[61] found that over 60% of Nigerian consumers expressed concerns about the security of their data when engaging in online transactions, with many citing cybercrime as a primary reason for their apprehension[62].

This erosion of trust can have far-reaching implications for the digital economy. If consumers lose confi dence in the security of digital platforms, they may revert to cash-based transactions or avoid online services altogether, stifl ing the growth of e-commerce and other digital industries. The success of the National Digital Economy and E-Governance Bill, which aims to promote digital transactions and services, is therefore closely tied to the eff ectiveness of cybersecurity measures in protecting consumers.

4.2.3. Strengthening Cybersecurity Measures

To address the growing cybersecurity threats, there is a pressing need for enhanced cybersecurity frameworks and strategies that are tailored to the unique challenges facing Nigeria. The government, through agencies like the National Information Technology Development Agency (NITDA) and the Nigerian Communications Commission (NCC), has been working to strengthen cybersecurity regulations and promote best practices among businesses and consumers. A key part of this eff ort was the implementation of the Nigeria Cybersecurity Strategy (2021-2025) which aims to improve the country's resilience to cyber threats and enhance collaboration between public and private sectors.[63]



[57] Ibid p.5
[58] Cyber Security Experts Association of Nigeria CSEAN, "National Cyber Threat Forecast 2025," https://csean.org.ng/national-cyber-threat-forecast-2025/
[59] CSEAN 2024
[60] Tope Aladenusi, "Nigeria Cybersecurity Outlook: Learning from International Perspectives," 2024, https://www.ncs.org.ng/wp-content/uploads/2024/06/Nigeria-Cybersecurity-Outlook-Learning-from-International-Perspectives-NCS-June-2024.pdf.
[61] KPMG, Cybersecurity considerations 2023.
[62] Ibid
[63] NITDA. Guidelines on Data Protection Compliance under the NDPA

Additionally, there is a need for increased investment in cybersecurity infrastructure. The adoption of advanced technologies such as artifi cial intelligence and machine learning can help to detect and respond to cyber threats in real-time. However, technology alone is not suffi cient. There is a need for a joint eff ort by the government, businesses and individuals to bridge the cybersecurity skill gap in Nigeria by capacity building through cybersecurity education and training. This would ensure that both businesses and consumers are aware and equipped with the knowledge and skills to protect themselves against cyber threats. Public awareness campaigns and initiatives that enlighten consumers on topics such as passwords, two-factor authentication and secure payment methods can also help build resilience against cyber threats.

There is also a need for these initiatives to be supported by strong regulatory frameworks that propel businesses to take safer and secure cyber security measures, develop cyber resilience, and build good cyber hygiene.

Cybersecurity threats pose a signifi cant risk to Nigeria's digital economy, with cybercrime costing the country approximately $500 million in 2022 alone[64].

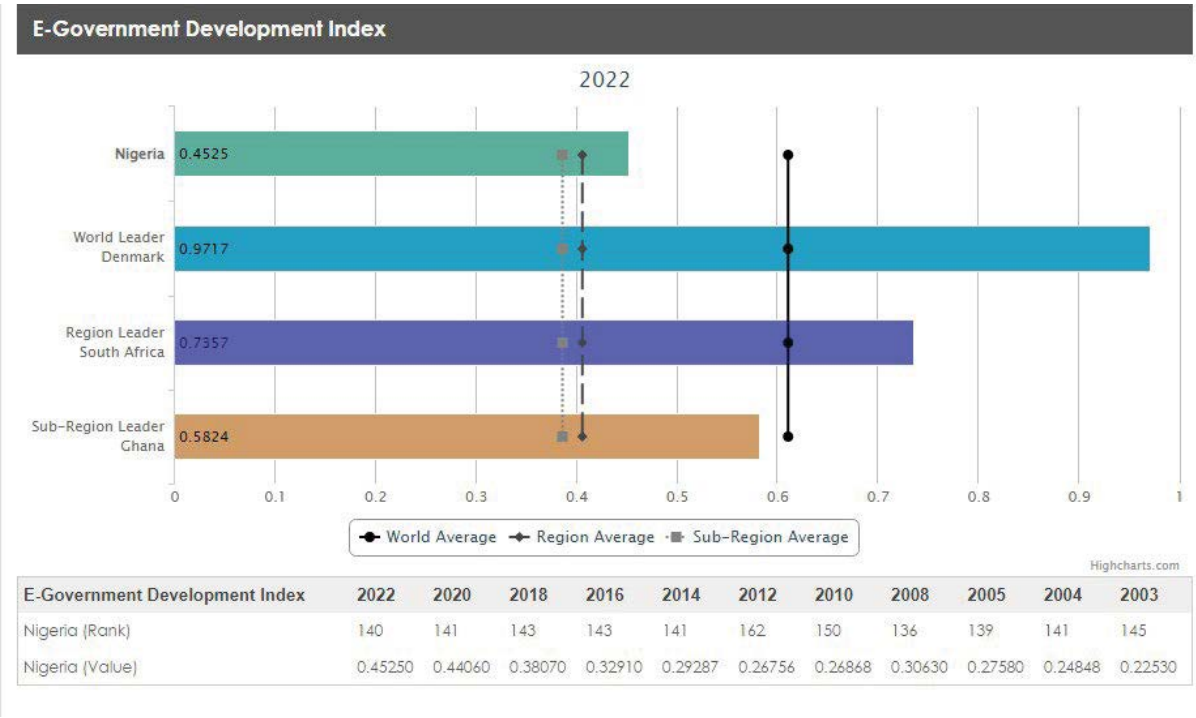
These threats undermine consumer trust in digital commerce and highlight the need for stronger cybersecurity measures. To safeguard the progress of Nigeria's digital transformation, it is imperative to enhance cybersecurity frameworks, invest in advanced technologies, and promote a culture of cybersecurity awareness. By addressing these challenges, Nigeria can create a safer digital environment that supports the growth and sustainability of its digital economy.

[64] Tope Omogbolagun, "Senate Laments Nigeria's Loss of $500m Annually to Cybercrime," Punch Newspapers, November 22, 2023, https://punchng.com/senate-laments-nigerias-loss-of-500m-annually-to-cybercrime/.

5.0 DIGITAL GOVERNMENT SERVICES

5.1 E-Government Readiness

Nigeria's readiness for e-government is pivotal to the success of its digital governance initiatives across the country. The 2022 United Nations E-Government Development Index (EGDI) ranks Nigeria 140th out of 193 countries in e-government development and 117th in e-participation, highlighting the need for substantial improvements to its digital governance infrastructure[65]. This ranking reflects the challenges the country faces in building a robust digital environment that supports efficient, transparent, and accessible government services.



E-Government Development Index	2022	2020	2018	2016	2014	2012	2010	2008	2005	2004	2003
Nigeria (Rank)	140	141	143	143	141	162	150	136	139	141	145
Nigeria (Value)	0.45250	0.44060	0.38070	0.32910	0.29287	0.26756	0.26868	0.30630	0.27580	0.24848	0.22530

Description: E-Government Development Index comparison between Nigeria, the global leader Denmark, the regional leader South Africa, and the sub-regional leader Ghana.

Note(s): December 2023

Source(s): United Nations

5.1.1 Current Initiatives and Achievements

Despite the relatively low ranking, Nigeria has made notable progress in certain areas of e-government through initiatives such as the Treasury Single Account (TSA) and the Integrated Payroll and Personnel Information System (IPPIS). These programs have been instrumental in improving financial management and accountability within the public sector. The TSA, for instance, has centralised government receipts and payments, reducing leakages and enhancing transparency in public finance[66]. Similarly, IPPIS has streamlined payroll processes, ensuring that government employees are paid accurately and promptly, which has helped reduce ghost workers and payroll fraud [67].

These successes demonstrate the potential of e-government initiatives to transform public administration in Nigeria. However, the broader adoption and integration of digital governance tools remain challenging, presenting key barriers that must be addressed to fully realise the benefits of e-governments.

[65] UN E-Government Survey, 202 EGOVKB | United Nations > Data > Country Information
[66] Deji Elumoye, "FG: We Saved over N10trn Through Treasury Single Account Implementation," Thisday, 2022, https://www.thisdaylive.com/index.php/2022/06/24/fg-we-saved-over-n10trn-through-treasury-single-account-implementation/
[67] Federal Ministry of Finance, 2023

5.1.2. Challenges in E-Government Readiness

One of the most pressing challenges is the lack of digital literacy among government staff . Many employees in the public sector are not adequately trained to use digital tools and platforms and this hampers the eff ective implementation of e-government services [68].

This digital skills gap is particularly pronounced in lower levels of government, where there is often resistance to transitioning from traditional, paper-based systems to digital processes[69].

Moreover, there is institutional resistance to change within the public sector, where entrenched practices and bureaucratic inertia pose obstacles to the adoption of new technologies [70]. This resistance is often rooted in a lack of understanding of the benefi ts of digital transformation, as well as concerns about job security and the potential displacement of workers due to automation and digitalisation[71].

The inadequacy of digital infrastructure especially in rural areas further compounds these challenges. The digital divide between urban and rural regions makes it diffi cult to ensure equitable access to e-government services, thereby limiting citizen participation. Social factors such as age, income, and education are still widening disparities in internet access and perpetuating digital exclusion. This infrastructure gap also aff ects the quality and reliability of e-government services, leading to frustrations among users and undermining confi dence in the system[72].

Additionally, the lack of interoperability between various government systems and databases presents a signifi cant hurdle. Many government agencies operate in isolated silos, using disparate systems that do not communicate eff ectively with one another. This lack of integration leads to ineffi ciencies, duplication of eff orts, and diffi culties in sharing data across departments, all of which hinder the seamless delivery of e-government services[73].

5.2 Implementation Challenges

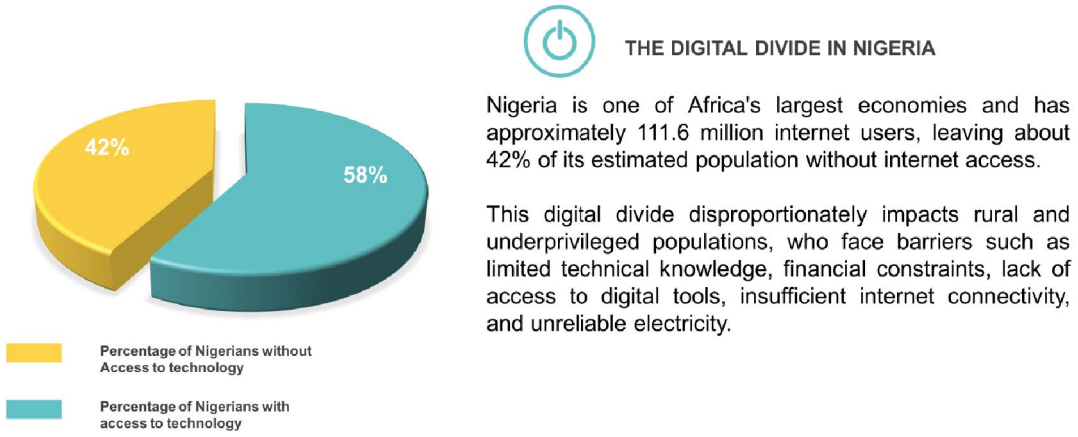
The implementation of digital government services in Nigeria is a crucial step towards strengthening public administration and improving service delivery. However, the journey towards a fully digital government is fraught with signifi cant challenges such as inadequate digital infrastructure, low digital literacy, and limited interoperability between government ICT systems. These challenges have collectively hindered the eff ectiveness of e-government initiatives and the seamless delivery of public services.

5.2.1. Inadequate Digital Infrastructure

A major obstacle to the eff ective implementation of digital government services is the inadequacy of digital infrastructure across the country[74]. Although cities like Lagos and Abuja enjoy relatively better digital infrastructure, rural and remote regions continue to suff er from poor internet connectivity, unreliable power supply, and inadequate hardware and software resources. This divide not only limits access to e-government services for a signifi cant portion of the population but also undermines eff orts to create an inclusive digital economy.

The World Bank[75] reports that only about 42% of Nigeria's population has access to the internet, with broadband penetration even lower in rural areas. This lack of widespread, reliable digital infrastructure makes it diffi cult for government agencies to deploy and maintain eff ective digital services. As a result, many citizens, especially those in underserved areas, remain excluded from the benefi ts of e-governance, perpetuating existing inequalities in access to public services.

[68] World Bank. (2022). Nigeria Digital Economy Diagnostic: Building Digital Infrastructure and Governance. World Bank Group. Retrieved from World Bank Documents.
[69] World Bank. (2022). Nigeria Digital Economy Diagnostic: Building Digital Infrastructure and Governance. World Bank Group. Retrieved from World Bank Documents.
[70] Njoku, F. O., & Okafor, F. I. (2017). "The Role of Bureaucratic Culture in Organizational Change: Insights from Nigeria." International Journal of Public Administration and Management Research,7(4), 50-63.
[71] Adebayo Adekele, "The Digital Landscape and E-Governance in Nigeria," Businessday NG, July 5, 2023, https://businessday.ng/opinion/article/the-digital-landscape-and-e-governance-in-nigeria/
[72] Shuaib M Abdulnabi, "Issues and Challenges of Implementing E-Governance in Developing Countries: A Comprehensive Analysis of Civil Service Models," Cogent Business & Management 11, no. 1 (April 15, 2024), https://doi.org/10.1080/23311975.2024.2340579.
[73] Ibid
[74] Akinyemi, O., & Olojede, O. (2023). "The Challenges of E-Government Implementation in Nigeria: Digital Infrastructure and Policy Gaps." International Journal of Public Administration and Management Research, 8(2), 24-38.
[75] The World Bank. Nigeria Digital Economy Diagnostic Report, 2022 Journal of development Communication Volume 33(1) © 2022 AIDCOM



Description: Percentage of Nigerians without access to technology vs those with access to technology

5.2.2. Low Digital Literacy

Low levels of digital literacy of the majority of Nigeria's populace as well as government employees present yet another signifi cant barrier to the successful implementation of e-government services. Digital literacy - defi ned as the ability to eff ectively use digital tools and technologies - is essential for both accessing and delivering digital services[76]. However, a large portion of Nigeria's population, particularly in rural areas, lacks the basic digital skills necessary to engage with e-government platforms[77].

This challenge extends to government employees, many of whom are not adequately trained to use digital systems eff ectively. According to the World Bank[78], low digital profi ciency among civil servants has led to a reliance on traditional, paper-based processes, even when digital alternatives are available. The absence of ongoing training and capacity-building programs exacerbates this issue, leaving government agencies ill-equipped to manage and maintain the digital systems necessary for eff ective e-governance.

5.2.3. Limited Interoperability Between Government ICT Systems

The limited interoperability between diff erent government ICT systems poses another signifi cant challenge to the implementation of digital government services. Interoperability refers to the ability of various ICT systems and software applications to communicate, exchange data, and use the information that has been exchanged. In the context of e-government, it is essential to ensure that diff erent government departments and agencies can work together seamlessly.[79]

However, in Nigeria, many government ICT systems operate in silos, using disparate technologies and standards that do not communicate eff ectively with one another[80]. This lack of interoperability leads to ineffi ciencies, such as the duplication of data entry, delays in service delivery, and an increased risk of errors and inconsistencies in public records. Additionally, it limits the government's ability to provide integrated services, where citizens can access multiple services through a single platform or portal.

The challenge of interoperability is further compounded by the absence of a unifi ed national data management framework that could facilitate data sharing and integration across government agencies. Without such a framework, eff orts to harmonise and standardise ICT systems across diff erent levels of government remain fragmented and slow.

[76] Gideon Seun Olanrewaju et al., "Left Behind? The Effects of Digital Gaps on E-Learning in Rural Secondary Schools and Remote Communities across Nigeria during the COVID19 Pandemic," International Journal of Educational Research Open 2 (January 1, 2021): 100092, https://doi.org/10.1016/j.ijedro.2021.100092.
[77] The World Bank. Nigeria Digital Economy Diagnostic Report, 2022 Journal of development Communication Volume 33(1) © 2022 AIDCOM
[78] The World Bank. Nigeria Digital Economy Diagnostic Report, 2022
[79] United Nations Development Programme, E-Government Interoperability: Overview, 1st ed. (Bangkok, Thailand : UNDP, 2007).
[80] Zakariyya Adaramola, "MDAs work in silos, neglect e-government, NITDA says," Daily Trust, May 23, 2018, https://dailytrust.com/mdas-work-in-silos-neglect-e-government-nitda-says-4/

5.2.4. Addressing the Challenges

To overcome these challenges and enhance the eff ectiveness of e-government initiatives, a multifaceted approach is required:

1. **Change Management:** Overcoming resistance within the public sector requires eff ective change management strategies. This can involve communicating the benefi ts of e-government, engaging stakeholders early in the process, and providing assurances about job security. Leadership commitment to digital transformation is also crucial for fostering a culture that embraces change.

2. **Investment in Digital Infrastructure:** The government must prioritise investments in expanding and upgrading digital infrastructure, particularly in rural and underserved areas. Public-private partnerships (PPPs) can play a key role in financing and accelerating the deployment of broadband networks, improving internet connectivity, and ensuring a stable power supply to support digital services.

3. **Enhancing Digital Literacy:** There is an urgent need for comprehensive digital literacy programs targeted at both the general population and government employees. These programs should not only focus on building basic digital skills but also off er advanced training for civil servants who manage and operate e-government systems. Incorporating digital literacy into the national education curriculum can further prepare future generations for a digital economy.

4. **Improving Interoperability:** Developing a national interoperability framework is crucial for enabling seamless data exchange and collaboration between diff erent government ICT systems. This framework should include standardised protocols for data management, clear guidelines for system integration, and a centralised governance structure to oversee its implementation. Additionally, adopting cloud-based solutions and open-source technologies can further help facilitate interoperability while reducing costs.

5. **Strengthening Governance and Coordination:** The implementation of e-government initiatives requires strong governance and coordination across various levels of government. Establishing a centralised agency responsible for overseeing digital transformation eff orts, setting standards, and ensuring compliance can help align diff erent e-government projects and prevent the fragmentation of eff orts.

The successful implementation of digital government services in Nigeria is crucial for enhancing the effi ciency and accessibility of public services. However, signifi cant challenges related to inadequate digital infrastructure, low digital literacy, and limited interoperability between government ICT systems continue to impede progress. By addressing these challenges through targeted investments, capacity-building initiatives, and the development of a national interoperability framework, Nigeria can overcome these obstacles and build a more eff ective and inclusive digital government.

6.0 DIGITAL INFRASTRUCTURE AND ICT SYSTEMS

6.1 Current State of Digital Infrastructure

Nigeria's digital infrastructure is the backbone of its digital transformation, yet it remains signifi cantly underdeveloped, particularly in broadband access. As of 2023, broadband penetration in Nigeria stood at approximately 42%, which is far below the ambitious targets set by the National Broadband Plan (2020-2025).

The Plan, which aims to achieve 90% broadband penetration by 2025, highlights the critical role of robust digital infrastructure in driving economic growth, enhancing connectivity, and supporting e-government initiatives[81]. Without signifi cant progress in this regard, Nigeria risks losing its competitiveness and profi tability in the global digital economy. According to UNCTAD, citizens of developing countries risk becoming suppliers of raw data to digital platforms while having to pay for the insights derived from their own data [82].

A major challenge is the urban-rural disparity in broadband access. While major cities like Lagos and Abuja enjoy relatively high levels[83] of connectivity, rural and underserved regions lag behind, with limited access to high-speed internet, deepening pre-existing socio-economic inequalities. Deploying broadband infrastructure in these areas is further restricted by factors such as poor electricity supply, high costs of infrastructure development, and geographical barriers. On the other hand, national and sub-national budgets in Nigeria remain overstretched and limited to support large-scale infrastructural development. As such, only high-risk investors are willing to fund such initiatives.[84]

The underdevelopment of digital infrastructure also aff ects businesses and consumers across the country. For businesses, especially small and medium-sized enterprises (SMEs), inadequate internet access limits their ability to engage in e-commerce, access digital tools, and compete in the global market[85]. For consumers, it restricts access to essential services, including online education, telemedicine, and digital financial services, further entrenching socio-economic disparities. These gaps also expose vulnerable consumers to cyber frauds and other hazards encountered through digital platforms[86]

Addressing these challenges requires signifi cant investment in digital infrastructure. This includes expanding broadband networks, improving the reliability of Internet services, and ensuring equitable access to digital infrastructure. However, developments of this scale may require alternative and modular approaches that would ensure Nigeria attains its maximum potential. According to the World Bank, Nigeria would need to invest 3 Trillion dollars by 2050 in order to provide all the digital infrastructure the country requires to attain competitive advantage[87]. Investment of this scale may not be feasible due to overarching economic and financial challenges and several barriers to implementation. To bridge this gap, Public-Private partnerships (PPPs) are crucial in mobilising the resources needed to accelerate infrastructure development and achieve the goals set out in the National Broadband Plan.

[81] Nigerian Communications Commission. National Broadband Plan 2020-2025.
[82] United Nation Trade and Development , "Inequalities Threaten Wider Divide as Digital Economy Data Flows Surge | UNCTAD," unctad.org, 2021,
[83] United Nations Trade and Development , "Inequalities Threaten Wider Divide as Digital Economy Data Flows Surge | UNCTAD," unctad.org, 2021, https://unctad.org/news/inequalities-threaten-wider-divide-digital-economy-data-fl ows-surge.
[84] Seun Kolade , Neta Hanien, and Natalie Beinisch, "Nigeria's Digital Future Will Be Decided by Physical Infrastructure," IE Insights, April 14, 2023, https://www.ie.edu/insights/articles/nigerias-digital-future-will-be-decided-by-physical-infrastructure/.
[85] United Nation Trade and Development , "Inequalities Threaten Wider Divide as Digital Economy Data Flows Surge | UNCTAD," unctad.org, 2021,
[86] Ayodeji Adegboyega, "Journalists Highlight Gaps in Nigeria's Digital Infrastructure, Proffer Solutions," Premium Times Nigeria, April 24, 2024, https://www.premiumtimesng.com/news/top-news/688915-journalists-highlight-gaps-in-nigerias-digital-infrastructure-proffer-solutions.html.
[87] World Bank Group, "Nigeria's Need to Spend More and Better," World Bank, 2022, https://www.worldbank.org/en/news/feature/2022/11/21/nigeria-needs-to-spend-more-and-better.

6.2 Public Sector ICT Systems

The integration and interoperability of public sector ICT systems are crucial for the eff ective delivery of digital government services. However, in Nigeria, the lack of integration and limited interoperability among these systems has led to signifi cant ineffi ciencies and duplication of eff orts[88]. Many government agencies still rely on outdated ICT systems with limited functionality, preventing the transition to a cohesive and responsive digital government framework[89].

The persistence of siloed ICT systems across diff erent government departments and agencies means that there is often little to no communication or data exchange between these systems. This fragmentation leads to several challenges:

- Duplication of Eff orts: Without integrated systems, the same data is often manually re-entered into multiple systems, leading to ineffi ciencies and increased administrative costs[90].
- Inconsistent Data: The lack of a unifi ed data management framework results in discrepancies and errors in government records, making it diffi cult to maintain accurate and up-to-date information across agencies[91].
- Delayed Service Delivery: The inability to share data seamlessly between departments can cause delays in service delivery, as information needs to be manually transferred or reconciled, slowing down processes that could otherwise be automated.

These challenges are further exacerbated by the outdated nature of many of the ICT systems currently in use. Some government agencies still operate with legacy systems that are not equipped to handle modern digital applications, limiting their ability to adopt new technologies and integrate with more advanced systems[92]. This technological lag not only impedes the implementation of e-government services but also reduces the overall effi ciency and transparency of government operations.

To overcome these issues, there is a need for a comprehensive overhaul of the public sector's ICT infrastructure. This includes upgrading outdated systems, establishing standards for interoperability, and creating a centralised data management framework that allows for seamless data exchange between government agencies. Such improvements would enhance government operations, reduce redundancies, and enhance the delivery of public services.

Moreover, the adoption of cloud-based solutions and the use of open standards can facilitate greater interoperability and fl exibility, allowing government systems to evolve alongside technological advancements. This approach would also support the integration of emerging technologies, such as artifi cial intelligence and blockchain, into public sector operations which could further enhance the capabilities of Nigeria's digital government.

[88] Adetola Bademosi, "Nigeria's patchy journey towards interoperable identifi cation system," Nigerian Tribune, November 09, 2023, https://tribuneonlineng.com/nigerias-patchy-journey-towards-interoperable-identifi cation-system/
[89] NITDA, 2022.
90Ugochukwu David Abasilim, Lawrence I. Edet, "E-Governance and Its Implementation Challenges in the Nigerian Public Service," Acta Universitatis Danubius. Administratio, Vol. 7, No. 1 (2015), https://journals.univ-danubius.ro/index.php/administratio/article/view/2899/2913.
[91] Ugochukwu David Abasilim, Lawrence I. Edet, "E-Governance and Its Implementation Challenges in the Nigerian Public Service," Acta Universitatis Danubius. Administratio, Vol. 7, No. 1 (2015), https://journals.univ-danubius.ro/index.php/administratio/article/view/2899/2913.
[92] Challenges and Opportunities in Implementing Digital Transformation in Nigerian Public Service. (2024). Journal of the Management Sciences, 60(3), 296-308. https://journals.unizik.edu.ng/jfms/article/view/3731.

7. CYBERSECURITY AND DATA PROTECTION

7.1 Regulatory Framework

Nigeria's regulatory framework for data protection and cybersecurity is built on key legislation, most notably the Nigeria Data Protection Act (NDPA) and the Cybercrimes (Prohibition, Prevention, etc.) Act of 2015. These laws are fundamental in safeguarding personal data and addressing cyber threats within the country. However, inconsistent enforcement of these regulations and a reactive approach to cyber incidents have limited their effectiveness[93].

7.1.1. Nigeria Data Protection Act (NDPA)

The Nigeria Data Protection Act (NDPA)[94], which replaced the Nigeria Data Protection Regulation (NDPR), establishes the legal framework for data protection in Nigeria. It sets out obligations for organisations that process personal data, mandating that such data must be handled in a secure, confidential manner and only for the purposes for which it was collected. The NDPA requires organisations to obtain explicit consent from individuals before processing their data and to implement stringent security measures to prevent unauthorised access or breaches[95].

Despite the comprehensive nature of the NDPA, its enforcement has been uneven. The National Information Technology Development Agency (NITDA), responsible for overseeing the implementation of the NDPA, faces challenges in ensuring compliance across Nigeria's diverse economic landscape. Many organisations, particularly small and medium-sized enterprises (SMEs), lack the technical and financial resources to fully comply with the regulation[96]. Moreover, inconsistent application of penalties for non-compliance has reduced the NDPA's deterrent effect, allowing poor data protection practices to persist[97].

7.1.2. Cybercrimes (Prohibition, Prevention, etc.) Act of 2015

The Cybercrimes Act of 2015 is Nigeria's primary legislation addressing cyber threats, including crimes such as hacking, identity theft, and cyberstalking. The Act provides a legal framework for prosecuting cybercriminals and outlines the responsibilities of various stakeholders in combating cybercrime[98]. It also includes provisions for the protection of critical national information infrastructure and mandates the reporting of cyber incidents.

However, the approach to combating cyber threats under the Cybercrimes Act has largely been reactive rather than proactive[99]. While the Act establishes a solid legal foundation, its implementation has been less effective due to limited resources, lack of technical expertise, and inadequate coordination among law enforcement agencies. As a result, many cyber incidents are addressed only after they occur, leaving organisations and individuals vulnerable to attacks[100].

7.2 Cybersecurity Incidents

Nigeria has increasingly become a target for various cyber threats, reflecting the growing global trend of sophisticated and frequent cyberattacks. The Nigerian Cybersecurity Outlook report reveals that many organisations in the country lack adequate cybersecurity measures, making them highly vulnerable to these attacks[101].

[93] Yejide Gbenga-Ogundare, "Despite legislations, poor enforcement mechanism militate against fight against cybercrimes," Nigerian Tribune, September 27, 2023, https://tribuneonlineng.com/despite-legislations-poor-enforcement-mechanism-militate-against-fight-against-cybercrimes/.
[94] Nigeria Data Protection Regulation (NDPR). (2019).
[95] Ibid
[96] Omoruyi Edoigiawerie, Esq, "Beyond compliance: Data protection and privacy concerns in Nigeria's tech space," This Nigeria, September 23, 2024,https://thisnigeria.com/beyond-compliance-data-protection-and-privacy-concerns-in-nigerias-tech-space/.
[97] Samson Akintaro, "Data protection: NDPC to sanction executives of MDAs for data breaches," Nairametrics, July 3, 2023,https://nairametrics.com/2023/07/03/data-protection-ndpc-to-sanction-executives-of-mdas-for-data-breaches/.
[98] Cybercrimes Act, 2015
[99] Sahara Reporters, "ECOWAS Court Declares 'Nigeria's Cybercrime Act Section 24 Vague, Arbitrary, Unlawful'," Sahara Reporters, March 22, 2023. https://saharareporters.com/2023/03/22/ecowas-court-declares-nigerias-cybercrime-act-section-24-vague-arbitrary-unlawful .
[100] Godfrey George, "Bank customers, companies lose billions to Nigeria's weak cybersecurity," Punch, April 2, 2023. https://punchng.com/bank-customers-companies-lose-billions-to-nigerias-weak-cybersecurity/.
[101] Serianu. Nigerian Cybersecurity Outlook Report. 2022

7.2.1. Types of Cyber Threats

Several types of cyber threats are prevalent in Nigeria, posing signifi cant risks to organisations and individuals:

- **Phishing:** One of the most widespread cyber threats in Nigeria, phishing involves cybercriminals using deceptive emails or websites to trick individuals into disclosing sensitive information such as login credentials, financial details, or personal identifi cation information[102]. The stolen details are often used for fraudulent activities, leading to financial losses and identity theft.

- **Ransomware:** Ransomware attacks have increased in Nigeria with attackers encrypting a victim's data and demanding payment for its release. The cyber security threat forecast 2024[103] highlights the perverse eff ects that ransomware attacks have on both public and private sector entities, including healthcare providers, financial institutions, and educational institutions. These disruptions often exploit vulnerabilities such as outdated software, reliance on cracked and unlicensed software and poor patching practices and this can lead to signifi cant operational and financial damage.

- **Advanced Persistent Threats (APTs):** APTs are sophisticated, targeted attacks where cybercriminals gain unauthorised access to a network and remain undetected for an extended period. The primary goal of APTs is usually to steal sensitive information or disrupt critical infrastructure. These attacks are often associated with state-sponsored groups and pose a signifi cant threat to national security and economic stability.

- **AI-Powered Scams:** Cybercriminals are increasingly leveraging AI tools to carry out personalised phishing attacks and automate large-scale cyberattacks, making these scams more sophisticated and diffi cult to detect[104].

7.2.2. Inadequate Cybersecurity Measures

The Serianu report highlights that most Nigerian organisations are not adequately prepared to defend against these cyber threats. Many organisations lack essential cybersecurity infrastructure, such as firewalls, intrusion detection systems, and secure data backup solutions[105]. Additionally, there is a signifi cant shortage of skilled cybersecurity professionals in the country, which further exacerbates the vulnerability of organisations to cyberattacks[106]. This skills gap is a major concern, as it limits the ability of organisations to detect, respond to, and recover from cyber incidents eff ectively.

Additionally, there is a general lack of cybersecurity awareness among employees, which is a critical vulnerability[107]. Many cyberattacks, particularly phishing and ransomware, exploit human error—such as clicking on malicious links or opening infected attachments. Without proper cybersecurity training and awareness programs, employees can inadvertently become the weakest link in an organisation's defence against cyber threats.

7.2.3. Addressing Cybersecurity Challenges

To mitigate the risks posed by these cybersecurity threats, Nigeria needs to strengthen its regulatory framework and improve the implementation of existing laws like the NDPA and the Cybercrimes Act. This includes enhancing enforcement mechanisms, increasing penalties for non-compliance, and providing support to organisations—especially SMEs—to help them achieve compliance.

[102] Tobi Tunji, "Nigerian organisations battle 3,759 weekly cyber-attacks – Report ," Nairametrics, November 22, 2024. https://nairametrics.com/2024/11/22/nigerian-organisations-battle-3759-weekly-cyber-attacks-report/.
[103] CESAN, Cyber security Outlook 2024
[104] Data Group IT, "Nigeria's Cyber Security Battleground: Inside the Rise of Ransomware and AI-Powered Scams - DataGroupIT," DataGroupIT, March 20, 2024, https://datagroupit.com/nigerias-cyber-security-battleground-inside-the-rise-of-ransomware-and-ai-powered-scams/.
[105] CESAN, Cyber security Outlook 2024
[106] Ghislain de Salins and Anat Lewin, "Hacking" the cybersecurity skills gap in developing countries,"World Bank Blogs, November 22, 2023. https://blogs.worldbank.org/en/digital-development/hacking-cybersecurity-skills-gap-developing-countries?
[107] Ayegba, Abdullahi and Juliet, Iruemi Olohimai and Ale, Felix and A.O., Agboola, Assessing Cybersecurity Awareness and Experiences in the Workplace: Nigeria as a Case Study. Available at SSRN: https://ssrn.com/abstract=4959959 or http://dx.doi.org/10.2139/ssrn.4959959

Investing in cybersecurity infrastructure and skills development is also critical. Organisations need to adopt standard digital security practices such as multi-factor authentication, encryption, and regular security audits. Building cybersecurity capacity within the workforce through targeted training and certifi cation programs is equally important.

Public-Private Partnerships (PPPs) can play a vital role in enhancing Nigeria's cybersecurity posture. Collaboration between the government, private sector, and international partners can facilitate the sharing of threat intelligence, best practices, and resources, helping to build a more resilient cybersecurity ecosystem.

Nigeria's regulatory framework for data protection and cybersecurity, while robust in design, suff ers from inconsistent enforcement and a largely reactive approach to cyber threats. The increasing frequency and sophistication of cybersecurity incidents, including phishing, ransomware, and APTs, underscore the urgent need for stronger cybersecurity measures. By addressing these challenges through improved regulation, investment in infrastructure, and skills development, Nigeria can better protect its digital economy and enhance trust in its digital services.

8. DIGITAL LITERACY AND INCLUSION

8.1 Digital Literacy Levels

Digital literacy is the ability to effectively use digital tools and technologies. Digital literacy is essential for the adoption of digital government services and electronic transactions yet, it remains low in Nigeria, particularly in rural areas where access to education and digital infrastructure is limited. According to the National Bureau of Statistics (NBS), only 30% of Nigerians possess basic digital skills[108]. This low level of digital proficiency hampers the widespread adoption of digital services, limiting the ability of many Nigerians to engage with and benefit from e-government initiatives, online banking, e-commerce, and other digital platforms.

The digital literacy gap is more pronounced in rural and underserved areas, where limited access to the internet, digital devices, and educational resources creates further barriers to participation in the digital economy. A recent study conducted in Nigeria which employed data from UNDP and the Bureau of Statistics provided evidence of a disparity between regions and the rate of internet usage[109]. They found a high concentration of internet usage among Kano, Kaduna, Abuja, Oyo, Ogun and Lagos, while states like Ekiti, Bayelsa and Ebonyi state reported significantly lower usage rates.[110] The study also identified a linear progression along economic and social divides between the north and south, alongside urban and rural areas. Factors such as market size, employment, income, access to electricity, urbanisation, gender (female), age (60 years and above), and telephone density significantly emerged as key factors influencing Internet usage.[111] This digital divide deepens existing socio-economic inequalities, as individuals with limited digital skills are less likely to access the information, resources, and opportunities available online.

The low level of digital literacy among government employees further complicates efforts to implement e-government services. Many civil servants, particularly those in lower administrative positions, struggle to use digital platforms efficiently, which leads to continued reliance on traditional, paper-based processes[112]. This not only slows down the digital transformation of government services but also reduces the efficiency and accessibility of digitally delivered public services.

[108] National Bureau of Statistics (NBS). (2022). Nigeria Literacy and Digital Skills Survey. Retrieved from NBS Official Website.
[109] Richard Adeleke, "Digital Divide in Nigeria: The Role of Regional Differentials," African Journal of Science, Technology, Innovation and Development 13, no. 3 (May 13, 2020): 1–14, https://doi.org/10.1080/20421338.2020.1748335.
[110] National Bureau of Statistics, "NATIONAL BUREAU of STATISTICS," Nigerianstat.gov.ng, 2019, https://nigerianstat.gov.ng/elibrary?queries.; United Nations Development Programme, "Achieving Human Development in North East Nigeria National Human Development Report 2018," 2019,http://hdr.undp.org/sites/default/files/hdr_2018_nigeria_finalfi nalx3.pdf.
[111] Ibid.,7
[112] NITDA, "FG Launches Digital Literacy Skills for Federal Civil Servants," info@nitda.gov.ng,February 10, 2025. https://nitda.gov.ng/fg-launches-digital-literacy-skills-for-federal-civil-servants/8747/

8.2 Inclusion Efforts

Recognising the critical role of digital literacy in national development, the Nigerian government has launched several initiatives aimed at improving digital skills across the population. One of the key programs is the Digital Nigeria Programme, spearheaded by the Federal Ministry of Communications and Digital Economy. This initiative aims to equip Nigerians with the essential skills including basic digital literacy, coding, software development and other ICT-related competencies.[113]

The Digital Nigeria Programme seeks to create a digitally literate population by off ering a variety of learning opportunities, including online courses, in-person workshops, and partnerships with educational institutions and private sector organisations. These training programs are designed to be accessible to a wide range of participants, including youths, women, and individuals in rural communities who may have limited prior exposure to digital technologies.

Another buoyant initiative that has been piloted by NITDA is the National Digital Literacy Framework (NDLF) which aims to enhance digital literacy through skills training, capacity building and initiatives. The Federal Government of Nigeria through the National Digital Economy Policy and Strategy (NDEPS), has set an ambitious goal of attaining 90% digital literacy in 2030[114]. The NDLF provides a structured approach for developing both basic and advanced digital skills and targets various stakeholders including the general public, development partners, professional bodies, ICT product and service providers and the government. As highlighted by the Director General of NITDA, the framework aims to achieve 70% national digital literacy levels by 2027, serving as a stepping stone towards the 95% target by 2030[115]. This will be achieved through collaborative eff orts with partners like GIZ, the UK government and the Ministry of Education to consummate initiatives like the 3 million Tech Talents (3MTT)[116].

Despite these efforts, progress has been slow due to several factors including the scale of the challenge, insuffi cient funding, and the need for more targeted interventions[117]. For instance, while online courses are a valuable resource, their eff ectiveness is limited in areas with poor internet connectivity or among populations with low baseline literacy levels.

Furthermore, the government's digital literacy initiatives are still in the early stages of implementation, and it will take time for their full impact to be realised. To ensure long-term success and that they meet the evolving needs of the population, continuous monitoring, evaluation, and adaptation of these programs are essential.

To enhance the eff ectiveness of these initiatives, a more integrated and multi-stakeholder approach is required. This could involve deeper collaboration between government agencies, educational institutions, the private sector, and non-governmental organisations (NGOs) to scale up digital literacy training and make it more accessible.

Additionally, leveraging existing infrastructure, such as community centres, schools, and libraries, could help extend the reach of digital literacy programs to more remote areas.
Increasing digital literacy is not just about providing training; it also requires creating an enabling environment where individuals are encouraged to use digital skills in everyday activities. Addressing these challenges will be essential in ensuring that all Nigerians can fully participate and benefi t from the digital economy.

[113] Federal Ministry of Communications and Digital Economy, 2022
[114] NITDA,National Digital Literacy Framework ,22
[115] Mercy Chukwudiebere, "NITDA Targets 95% Digital Literacy in Nigeria by 2030," Voice of Nigeria, February 26, 2024, https://von.gov.ng/nitda-targets-95-digital-literacy-in-nigeria-by-2030/.
[116] Ibid
[117] Oladipupo BELLO and Abdulazeez O. Ajao, "Digital Literacy and Skills Development in Nigeria: Policies, Barriers and Recommendations," researchgate.net, September, 2024. https://www.researchgate.net/publication/383860373_Digital_Literacy_and_Skills_Development_in_Nigeria_Policies_Barriers_and_Recommendations#full-text

9. OFFENCES AND PENALTIES RELATED TO THE DIGITAL ECONOMY

9.1 Enforcement Challenges

The enforcement of penalties for digital crimes and non-compliance with digital regulations in Nigeria remains a signifi cant challenge. Despite the existence of laws and regulations aimed at curbing digital fraud, cybercrime, and data breaches, the actual enforcement of these laws has been inconsistent and largely ineff ective. This weak enforcement has created a sense of impunity among off enders, further eroding public trust in the digital economy.

According to the Federal Competition and Consumer Protection Commission (FCCPC), the numerous reports of digital fraud and data breaches have resulted in little to no repercussions for perpetrators. The lack of stringent enforcement measures has emboldened cybercriminals and contributed to a perception that digital crimes can be committed with relative impunity. This situation is particularly concerning in an environment where the digital economy is expanding rapidly, as it poses a signifi cant risk to consumer confi dence and the overall stability of digital transactions[118].

Several factors contribute to these enforcement challenges. First, there is a lack of resources and technical expertise within law enforcement agencies to eff ectively investigate and prosecute digital crimes[119]. Many agencies are still adapting to the complexities of cybercrime, which often requires specialised knowledge and tools that are currently in short supply.
Second, while the existing legal framework is comprehensive on paper, it is not always fully supported by the necessary infrastructure or trained personnel to enforce it eff ectively.

Moreover, corruption and bureaucratic ineffi ciencies further weaken enforcement eff orts[120]. In some cases, perpetrators of digital crimes may escape punishment due to connections or infl uence within the legal system, eroding public confi dence in the rule of law. This lack of accountability has serious implications for the growth of Nigeria's digital economy, as businesses and consumers may become increasingly reluctant to engage in online transactions if they believe that their rights and data are not adequately protected.

9.2 Judicial Capacity

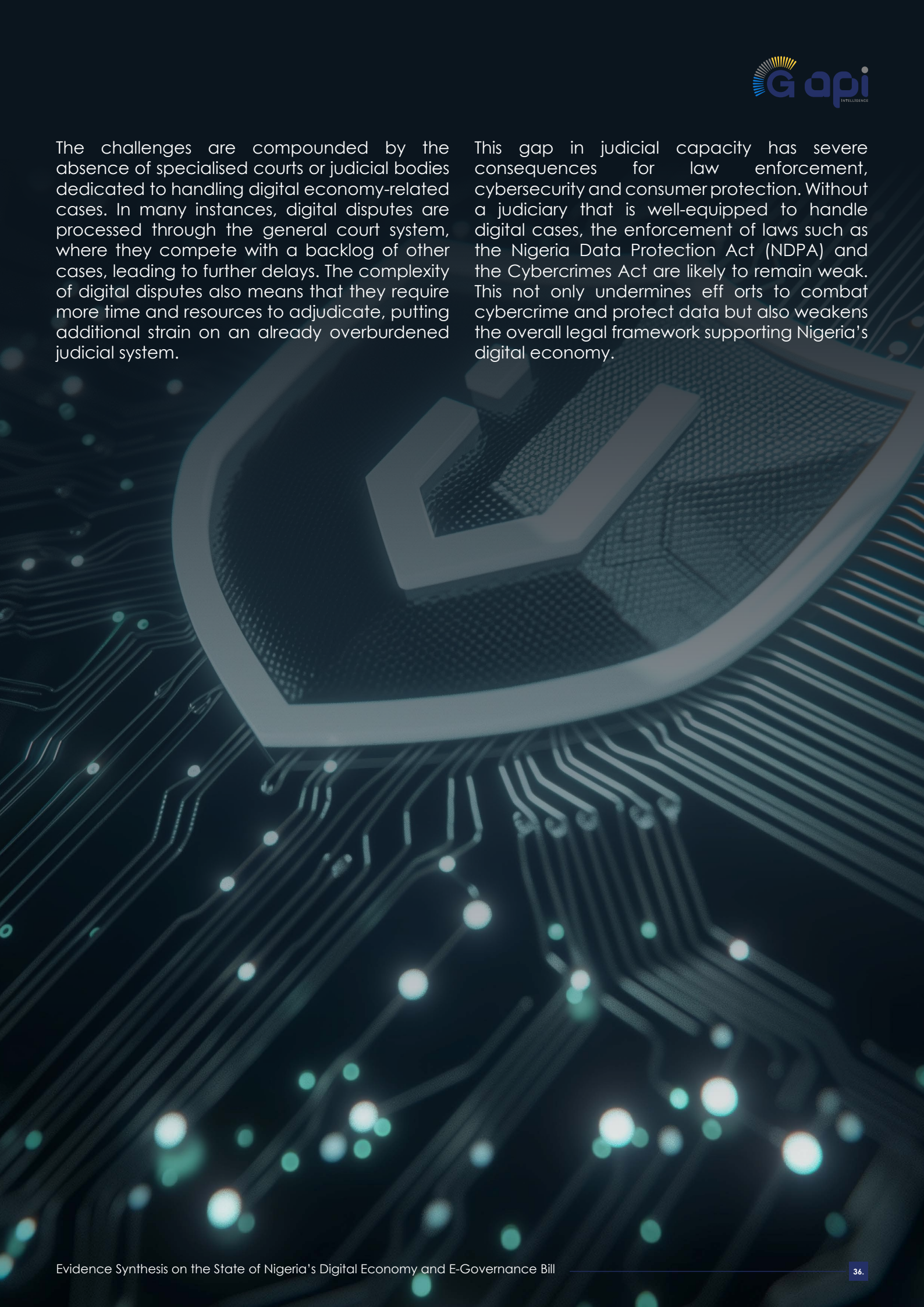
The capacity of Nigeria's judiciary to handle cases related to the digital economy is another critical challenge. The rapid evolution of digital technologies and the complexity of cyber-related legal issues have outpaced the development of judicial expertise in these areas. As a result, the Nigerian judiciary often struggles to eff ectively adjudicate cases involving digital crimes, data protection breaches, and other technology-related disputes[121].

A report by the World Bank (2022) highlights the signifi cant gap in the judiciary's understanding of digital laws and technologies. Many judges and legal practitioners lack the necessary training and experience to navigate the intricacies of digital disputes, leading to delays in dispute resolution and, in some instances, miscarriages of justice. This lack of capacity has created a bottleneck in the legal system, where digital cases are either postponed indefi nitely or resolved without the appropriate application of relevant laws[122].

[118] Federal Competition and Consumer Protection Commission (FCCPC) (2023). Annual Report.
[119] Federal Competition and Consumer Protection Commission (FCCPC) (2023). Annual Report.
[120] Jordan Ayotunde and Saheed Martin, "The Effectiveness of Cybercrime Investigations and Prosecution in Nigeria," researchgate.net, June, 2022. https://www.researchgate.net/publication/388658641_The_Effectiveness_of_Cybercrime_Investigations_and_Prosecution_in_Nigeria
[121] Adedeji, O., & Adebayo, M. (2021). E-Governance and Judiciary in Nigeria: Opportunities and Challenges. Retrieved from ResearchGate.
[122] World Bank. (2022). Nigeria Digital Economy Diagnostic: Building Digital Infrastructure and Governance. World Bank Group. Retrieved from World Bank Documents.

The challenges are compounded by the absence of specialised courts or judicial bodies dedicated to handling digital economy-related cases. In many instances, digital disputes are processed through the general court system, where they compete with a backlog of other cases, leading to further delays. The complexity of digital disputes also means that they require more time and resources to adjudicate, putting additional strain on an already overburdened judicial system.

This gap in judicial capacity has severe consequences for law enforcement, cybersecurity and consumer protection. Without a judiciary that is well-equipped to handle digital cases, the enforcement of laws such as the Nigeria Data Protection Act (NDPA) and the Cybercrimes Act are likely to remain weak. This not only undermines eff orts to combat cybercrime and protect data but also weakens the overall legal framework supporting Nigeria's digital economy.



10. Conclusion

This evidence synthesis on Nigeria's National Digital Economy and E-Governance Bill underscores the complex interplay between the country's aspirations for a robust digital economy and the signifi cant challenges that persist. The analysis reveals that while Nigeria has made commendable progress in several areas—such as the adoption of mobile money, the establishment of legal frameworks for digital transactions, and the implementation of e-government initiatives—there are several critical gaps that could hinder the full realisation of the bill's objectives.

Among the most pressing challenges is the inconsistent enforcement of existing digital regulations, which has led to a pervasive sense of impunity among cybercriminals and undermined public trust in the digital economy. The judiciary's limited capacity to eff ectively adjudicate digital-related cases further complicates the enforcement landscape, necessitating urgent capacity-building eff orts and the possible establishment of specialised courts to handle the unique complexities of digital crimes.

The state of digital infrastructure, particularly the urban-rural broadband divide, remains a signifi cant barrier to achieving inclusive digital transformation. This digital divide not only limits the reach of e-government services but also worsens socio-economic inequalities, leaving large segments of the population without access to the benefi ts of digitalisation. Additionally, the low levels of digital literacy, particularly in rural areas, and the challenges in the adoption of electronic contracts and signatures among SMEs highlight the need for targeted educational campaigns and the development of more accessible and secure digital tools. These eff orts must be complemented by stronger cybersecurity measures to protect against the rising threat of cybercrime, which poses a serious risk to the stability and growth of Nigeria's digital economy.

To move forward, Nigeria must adopt a holistic approach that addresses these interrelated challenges. This includes enhancing regulatory enforcement, improving judicial capacity, investing in digital infrastructure, and fostering digital literacy and cybersecurity awareness across the population. Public-private partnerships and international collaborations will be crucial in mobilising the necessary resources and expertise to drive these initiatives.

Ultimately, the successful implementation of the National Digital Economy and E-Governance Bill will depend on Nigeria's ability to navigate these challenges and capitalise on the opportunities presented by digital transformation. By building a secure, inclusive, and well-regulated digital economy, Nigeria can position itself as a leader in the global digital landscape, driving economic growth, improving governance, and enhancing the quality of life for all its citizens.

References

- Abdulnabi, Shuaib M. "Issues and Challenges of Implementing E-Governance in Developing Countries: A Comprehensive Analysis of Civil Service Models." Cogent Business & Management 11, no. 1 (April 15, 2024). https://doi.org/10.1080/23311975.2024.2340579.
- Adekele, Adebayo. "The Digital Landscape and E-Governance in Nigeria." Businessday NG, July 5, 2023. https://businessday.ng/opinion/article/the-digital-landscape-and-e-governance-in-nigeria/.
- Adeleke, Richard. "Digital Divide in Nigeria: The Role of Regional Diff erentials." African Journal of Science, Technology, Innovation and Development 13, no. 3 (May 13, 2020): 1–14. https://doi.org/10.1080/20421338.2020.1748335.
- Aladenusi, Tope. "Nigeria Cybersecurity Outlook: Learning from International Perspectives," 2024. https://www.ncs.org.ng/wp-content/uploads/2024/06/Nigeria-Cybersecurity-Outlook-Learning-from-International-Perspectives-NCS-June-2024.pdf.
- Ayodeji Adegboyega. "Journalists Highlight Gaps in Nigeria's Digital Infrastructure, Proff er Solutions." Premium Times Nigeria, April 24, 2024. https://www.premiumtimesng.com/news/top-news/688915-journalists-highlight-gaps-in-nigerias-digital-infrastructure-proff er-solutions.html.
- BusinessDay. "The Digital Landscape and E-Governance in Nigeria." Businessday NG, July 5, 2023. https://businessday.ng/opinion/article/the-digital-landscape-and-e-governance-in-nigeria/.
- Central Bank of Nigeria (CBN). (2023). Annual Report 2023.
- Chukwudiebere, Mercy. "NITDA Targets 95% Digital Literacy in Nigeria by 2030." Voice of Nigeria, February 26, 2024. https://von.gov.ng/nitda-targets-95-digital-literacy-in-nigeria-by-2030/.
- Companies and Allied Matters Act (CAMA). (2020)
- Cybercrimes (Prohibition, Prevention, etc.) Act. (2015).
- Cybercrimes (Prohibition, Prevention, etc.) Act. (2015). An Act to Provide for the Prohibition, Prevention, Detection, Prosecution, and Punishment of Cybercrimes in Nigeria. Federal Republic of Nigeria.
- Data Group IT. "Nigeria's Cyber Security Battleground: Inside the Rise of Ransomware and AI-Powered Scams - DataGroupIT." DataGroupIT, March 20, 2024. https://datagroupit.com/nigerias-cyber-security-battleground-inside-the-rise-of-ransomware-and-ai-powered-scams/.
- Doloitte. "Nigeria Cybersecurity Outlook 2024." Deloitte . Deloitte, 2024. https://www.deloitte.com/ng/en/services/risk-advisory/perspectives/Nigeria-Cybersecurity-Outlook-2024.html#:~:text=This%20article%20delves%20into%20the%20key%20cybersecurity%20predictions%20for%20Nigeria.
- Evidence Act, 2011.
- Evidence Act. (2011). An Act to Repeal the Evidence Act Cap. E14, Laws of the Federation of Nigeria 2004, and Enact a New Evidence Act 2011; and for Related Matters. Federal Republic of Nigeria.
- Evidence Act. (2011). An Act to Repeal the Evidence Act Cap. E14, Laws of the Federation of Nigeria 2004, and Enact a New Evidence Act 2011; and for Related Matters. Federal Republic of Nigeria.
- Federal Competition and Consumer Protection Commission (FCCPC). (2023). Annual Report.
- Federal Competition and Consumer Protection Commission (FCCPC). (2023). Annual Report on Consumer Complaints and Digital Transactions. Retrieved from FCCPC Offi cial Website.
- Federal Competition & Consumer Protection Commission. "REGISTRATION of

DIGITAL MONEY LENDERS under the INTER AGENCY JOINT TASK FORCE'S LIMITED INTERIM REGULATORY/REGISTRATION FRAMEWORK and GUIDELINES for DIGITAL LENDING 2022 - Federal Competition & Consumer Protection Commission." Federal Competition & Consumer Protection Commission, August 2, 2023. https://fccpc.gov.ng/registration-of-digital-money-lenders-under-the-inter-agency-joint-task-forces-limited-interim-regulatory-registration-framework-and-guidelines-for-digital-lending-2022/#:~:text=Wednesday.

- Federal Ministry of Communications and Digital Economy. (2022). Annual Report on the Digital Nigeria Programme. Retrieved from Ministry of Communications and Digital Economy Website.
- Federal Ministry of Communications and Digital Economy. (2022). Digital Nigeria Programme Report.
- Federal Ministry of Communications and Digital Economy. (2023). Annual Report on the State of Digital Infrastructure and E-Government Implementation in Nigeria. Federal Republic of Nigeria.
- Federal Ministry of Finance. (2023). Annual Report on the Treasury Single Account (TSA) and Integrated Payroll and Personnel Information System (IPPIS). Federal Republic of Nigeria. Retrieved from Ministry of Finance Offi cial Website.
- Freedom House. "Nigeria: Freedom on the Net 2023 Country Report." Freedom House, 2023. https://freedomhouse.org/country/nigeria/freedom-net/2023.
- Kolade , Seun , Neta Hanien, and Natalie Beinisch. "Nigeria's Digital Future Will Be Decided by Physical Infrastructure." IE Insights, April 14, 2023. https://www.ie.edu/insights/articles/nigerias-digital-future-will-be-decided-by-physical-infrastructure/.
- KPMG. "The Consumers Right Awareness and Protection: A Means to Economic Development." KPMG. KPMG, June 2, 2021. https://kpmg.com/ng/en/home/media/press-releases/2021/04/the-consumers-right-awareness-and-protection-a-means-to-economic-development.html#:~:text=The%20Consumers%20Right%20Awareness%20and%20Protection:%20A%20Means%20to%20Economic.
- KPMG Nigeria. (2023). Consumer Insights Survey: Cybersecurity Concerns in the Digital Economy. KPMG Nigeria.
- KPMG. "Cybersecurity Considerations 2023," 2023. https://assets.kpmg.com/content/dam/kpmg/xx/pdf/2023/02/cyber-considerations-report-2023.pdf.
- National Assembly. Electronic Transaction Bill (2017).
- National Bureau of Statistics (NBS). (2022). Nigeria Literacy and Digital Skills Survey. Retrieved from NBS Offi cial Website.
- National Bureau of Statistics. "NATIONAL BUREAU of STATISTICS." Nigerianstat.gov.ng, 2019. https://nigerianstat.gov.ng/elibrary?queries.
- Nigeria Data Protection Commission. NIGERIA DATA PROTECTION ACT, 1 § (2023). https://assets.kpmg.com/content/dam/kpmg/ng/pdf/nigeria-data-protection-act2023.pdf#:~:text=NIGERIA%20DATA%20PROTECTION%20ACT,%202023.%20EXPLANATORY%20l'v1EMORANDUM.%20This%20Act%20provides.
- National Information Technology Development Agency (NITDA). (2022). NITDA Annual Report 2022. Retrieved from NITDA Offi cial Website.
- National Information Technology Development Agency (NITDA). (2022). NITDA Annual Report 2022. Retrieved from NITDA Offi cial Website.
- National Information Technology Development Agency (NITDA). (2022). Public Sector ICT Systems Report: Challenges and Opportunities for Integration. National Information Technology Development Agency. Retrieved from NITDA Offi cial Website.
- National Information Technology Development Agency (NITDA). (2023). Guidelines on Data Protection Compliance under the NDPA. Retrieved from NITDA Offi cial Website.
- National Information Technology Development Agency (NITDA). (2023). Annual Compliance Report. Retrieved from NITDA Offi cial Website.
- National Information Technology Development Agency (NITDA). (2023). Nigeria

Cybersecurity Strategy (2021-2025) Implementation Report. Retrieved from NITDA Offi cial Website.
- National Information Technology Development Agency. "NATIONAL DIGITAL LITERACY FRAMEWORK FEDERAL MINISTRY of COMMUNICATIONS and DIGITAL ECONOMY," 2023. https://nitda.gov.ng/wp-content/uploads/2023/07/Digital-Literacy-Framework.pdf.
- Nigeria Communications Commission (NCC). (2023). Internet Penetration Report.
- Nigeria Data Protection Regulation (NDPR). (2019).
- Nigeria Inter-Bank Settlement System (NIBSS). (2023).
- Nigerian Bar Association. (2021). Survey on the Use of Electronic Contracts and Signatures among Legal Practitioners in Nigeria. Nigerian Bar Association.
- Nigerian Bar Association. (2021). Survey on the Use of Electronic Contracts and Signatures among Legal Practitioners in Nigeria. Nigerian Bar Association.
- Nigerian Bureau of Statistics (NBS). (2022). Annual Labour Force Survey.
- Nigerian Communication commission. "Subscriber Data." ncc.gov.ng, 2024. https://ncc.gov.ng/statistics-reports/subscriber-data.
- Nigerian Communications Commission (NCC). (2023). National Broadband Plan 2020-2025.
- Nigerian Communications Commission. (2023). Annual Report on Broadband Penetration and Infrastructure Development in Nigeria. Nigerian Communications Commission. Retrieved from NCC Offi cial Website.
- NITDA. (2022). National Information Technology Development Agency Report.
- Olalekan, Saka. "Nigeria Recorded N600 Trillion E-Payment Transactions in 2023." NIBSS, February 9, 2024. https://nibss-plc.com.ng/nigeria-recorded-n600-trillion-e-payment-transactions-in-2023/.
- Olanrewaju, Gideon Seun, Seun Bunmi Adebayo, Abiodun Yetunde Omotosho, and Charles Falajiki Olajide. "Left Behind? The Eff ects of Digital Gaps on E-Learning in Rural Secondary Schools and Remote Communities across Nigeria during the COVID19 Pandemic." International Journal of Educational Research Open 2 (January 1, 2021): 100092. https://doi.org/10.1016/j.ijedro.2021.100092.
- Omogbolagun, Tope. "Senate Laments Nigeria's Loss of $500m Annually to Cybercrime." Punch Newspapers, November 22, 2023. https://punchng.com/senate-laments-nigerias-loss-of-500m-annually-to-cybercrime/.
- Onuoha, Anugbum, James Agbadufi shim, and Peter Ortese. "A CRITICAL ANALYSIS of the VALIDITY and ENFORCEABILITY of ELECTRONIC CONTRACT in NIGERIA: NEED for REFORMS." Global Journal of Politics and Law Research 8, no. 5 (2020): 13–30. https://eajournals.org/wp-content/uploads/A-Critical-Analysis-of-the-Validity-and-Enforceability-of-Electronic-Contract-in-Nigeria.pdf#:~:text=Many%20Nigerian%20businesses%20and%20individuals%20embrace%20the%20benefi ts%20of%20electronic.
- Robinson Sibe. "Council Post: Cybercrime and the Challenge of Static Legislations in Nigeria." Forbes, August 12, 2024. https://www.forbes.com/councils/forbestechcouncil/2024/04/29/cybercrime-and-the-challenge-of-static-legislations-in-nigeria/#:~:text=Cybercrime%20And%20The%20Challenge%20Of%20Static%20Legislations%20In.
- Serianu. (2022). Nigeria Cybersecurity Report 2022: Trends, Challenges, and Recommendations. Serianu Ltd.
- Serianu. (2022). Nigerian Cybersecurity Outlook Report.
- Temitayo Jaiyeola. "Analysis: How Telcos, Fintechs Are Driving Nigeria's Mobile Money Growth - Businessday NG." Businessday NG, March 25, 2024. https://businessday.ng/technology/article/analysis-how-telcos-fintechs-are-driving-nigerias-mobile-money-growth/#:~:text=As%20of%20October%202023.
- United Nation Trade and Development . "Inequalities Threaten Wider Divide as Digital Economy Data Flows Surge | UNCTAD." unctad.org, 2021. https://unctad.org/news/inequalities-threaten-wider-divide-digital-economy-data-fl ows-surge.

- United Nations Development Programme. "Achieving Human Development in North East Nigeria National Human Development Report 2018," 2019. http://hdr.undp.org/sites/default/files/hdr_2018_nigeria_finalfinalx3.pdf.
- United Nations E-Government Survey. (2022).
- United Nations E-Government Survey. (2022). E-Government Development Index 2022. United Nations Department of Economic and Social Aff airs. Retrieved from UN E-Government Survey.
- United Nations Trade and Development . "Inequalities Threaten Wider Divide as Digital Economy Data Flows Surge | UNCTAD." unctad.org, 2021. https://unctad.org/news/inequalities-threaten-wider-divide-digital-economy-data-fl ows-surge.
- Venza, Stefano . "Let's Meet OPay, the SoftBank-Backed Fintech That Is Outstanding Even TikTok." Inclusivemoney.com. NeoBanikng EN, December 12, 2023. https://inclusivemoney.com/fintech/opay#:~:text=According%20to%20Data.Ai%2C%20OPay%20isn%E2%80%99t%20just%20Nigeria%E2%80%99s%20most.
- World Bank Group. "Nigeria Digital Economy Diagnostic: A Plan for Building Nigeria's Inclusive Digital Future." World Bank. World Bank Group, February 10, 2020. https://www.worldbank.org/en/country/nigeria/publication/nigeria-digital-economy-diagnostic-a-plan-for-building-nigerias-inclusive-digital-future#:~:text=The%20Nigeria%20Digital%20Economy%20Diagnostic%20says%20that%20with%20improvements%20in.
- World Bank Group. "Nigeria's Need to Spend More and Better." World Bank, 2022. https://www.worldbank.org/en/news/feature/2022/11/21/nigeria-needs-to-spend-more-and-better.
- World Bank. (2022). Nigeria Digital Economy Diagnostic Report.
- World Bank. (2022). Nigeria Digital Economy Diagnostic: Building Digital Infrastructure and Governance. World Bank Group. Retrieved from World Bank Documents.

api INTELLIGENCE

THE GOVERNANCE AND INNOVATION NETWORK FOR GENERATING ENHANCED REGULATIONS (GINGER)

Technology Enabled and MSME Business Perspectives Across Nigeria

advocacy for policy and innovation hello@apiintelligence.org advocacyforpolicyandinnovation advocacy for policy and innovation