

**DIGITAL INFORMATION LAW AND ADMINISTRATIVE RESILIENCE: AN APPRAISAL OF
FEDERAL GOVERNMENT MINISTRIES, DEPARTMENTS AND AGENCIES IN RIVERS
STATE, NIGERIA****ALIKORNWO, Peter Mezenye, PhD**Department of Office Technology and Management, School of Business and Administrative
Studies, Captain Elechi Amadi Polytechnic, Port Harcourt, Rivers State, Nigeria**Email:** peter.alikornwo@portharcourtpoly.edu.ng**ORCID:** <https://orcid.org/0009-0008-7266-3731>**WOS Researcher ID:** PEV-3695-2025**AMADI, Dike Vincent, PhD**Department of Law, School of Legal Studies, Captain Elechi Amadi Polytechnic, Port Harcourt,
Rivers State, Nigeria**Email:** dike.amadi@portharcourtpoly.edu.ng**Abstract**

The migration of public administration from paper-based procedure to electronic and digitally mediated practice has created a body of rules, generally described as digital information law, which now governs how government institutions create, store, transmit, protect and disclose official information. This study examines the applicability of digital information law to the administrative resilience of federal government ministries, departments and agencies domiciled in Rivers State, Nigeria, a state that hosts a significant federal presence on account of its position as the commercial nerve centre of the oil and gas industry in the Niger Delta. Adopting a doctrinal and qualitative approach, the study reviews the Constitution of the Federal Republic of Nigeria 1999, the Freedom of Information Act 2011, the Nigeria Data Protection Act 2023, the National Information Technology Development Agency Act 2007, the Cybercrimes (Prohibition, Prevention, etc) Act 2015 as amended in 2024, and the Evidence Act 2011, alongside comparative material from the United Kingdom, the European Union, South Africa and Ghana. The study relies on resilience theory, originally developed in ecological science and subsequently adapted to public administration, as its theoretical anchor. Findings indicate that although Nigeria now possesses a reasonably developed statutory architecture for digital information governance, federal agencies in Rivers State continue to exhibit administrative fragility on account of infrastructural deficits, inconsistent records management practice, low regulatory enforcement capacity and uneven cybersecurity preparedness. The study argues that administrative resilience in this context depends less on the mere existence of digital information law than on the institutional capacity of federal agencies to internalise and operationalise its requirements. It recommends targeted capacity building, infrastructural investment, closer collaboration between the Nigeria Data Protection Commission and field offices of federal agencies, and a coordinated digitisation policy for public records in Rivers State.

Keywords: *digital information law, administrative resilience, federal ministries, data protection, freedom of information, cybersecurity, e-governance*

1. Introduction

Public administration in Nigeria, as in most jurisdictions, has undergone a gradual but discernible shift from manual, paper-dependent bureaucratic procedure toward electronically mediated administrative practice. Government files that were once kept in bulky registries are increasingly generated, stored and transmitted in digital form, and citizens now interact with public institutions through online portals, electronic mail and digital identity systems. This shift has not occurred in a legal vacuum. It has instead been accompanied, sometimes belatedly, by a body of statutory and regulatory rules that governs how information in digital form is created, accessed, protected and disclosed within the public sector. This body of rules is what this study refers to as digital information

law. This study therefore examines the applicability of digital information law to the administrative resilience of federal government ministries, departments and agencies (MDAs) that maintain an operational presence within Rivers State, including revenue, customs, immigration, maritime and petroleum-related agencies whose functions are concentrated in Port Harcourt on account of the city's status as the commercial capital of the Niger Delta.

Administrative resilience, a concept borrowed from ecological science and progressively absorbed into public administration scholarship, denotes the capacity of an administrative system to anticipate, absorb, adapt to and recover from disruption while continuing to perform its core functions.¹ For federal MDAs operating in Rivers State, a region historically marked by infrastructural strain, security disturbance and administrative improvisation, resilience is not an abstract aspiration but a practical necessity. Digital information law bears directly on this resilience because the manner in which an agency manages its information assets, whether through secure data protection practice, transparent disclosure procedure, or robust cybersecurity posture, substantially determines its capacity to continue functioning under stress.

This study pursues three objectives. First, it clarifies the concepts of digital information law and administrative resilience and situates them within an appropriate theoretical framework. Second, it undertakes a doctrinal review of the principal Nigerian statutes governing digital information, read alongside comparative material from other jurisdictions. Third, it examines how these legal instruments apply, in practical terms, to the administrative resilience of federal MDAs in Rivers State, drawing on records management, infrastructure and cybersecurity literature specific to the state and the wider Niger Delta. The study adopts a doctrinal and qualitative methodology, relying on primary legislation, judicial authority and secondary scholarly and professional literature rather than field survey data.

2. Conceptual Clarification

2.1 Digital Information Law

Digital information law may be defined as the aggregate of statutory, regulatory and judicial rules that govern the creation, processing, storage, transmission, protection and disclosure of information that exists in electronic or digital form. In the Nigerian context, this body of law is not contained in a single code but is instead distributed across several instruments, including the Freedom of Information Act 2011,² which governs the right of access to information held by public institutions, the Nigeria Data Protection Act 2023,³ which governs the processing of personal data by both public and private bodies, the National Information Technology Development Agency Act 2007,⁴ which governs the standardisation and regulation of information technology practice, the Cybercrimes (Prohibition, Prevention, etc) Act 2015 as amended in 2024,⁵ which governs offences committed through computer systems and the protection of critical information infrastructure, and the Evidence Act 2011,⁶ which governs the admissibility of electronically generated documents in judicial and administrative proceedings. Taken together, these instruments constitute the legal architecture within which federal MDAs in Rivers State must conduct their digital information practice.

¹Crawford S Holling, 'Resilience and Stability of Ecological Systems' (1973) 4 *Annual Review of Ecology and Systematics* 1, 14.

²Freedom of Information Act 2011, s 1.

³Nigeria Data Protection Act 2023, s 2.

⁴National Information Technology Development Agency Act 2007, s 6.

⁵Cybercrimes (Prohibition, Prevention, etc) Act 2015, s 3.

⁶Evidence Act 2011, s 84.

2.2 Administrative Resilience

Administrative resilience has attracted increasing scholarly attention as public institutions worldwide confront disruptions ranging from pandemics to cyberattacks. A recent meta-narrative review of the public administration literature

identifies three overlapping narratives of resilience, namely maintenance of core function during disturbance, recovery of function after disturbance, and adaptability of institutional structure and practice in response to changing conditions.⁷ Administrative resilience has also been defined, in a study grounded in the experience of a riverine and hydrologically unstable region of Bangladesh, as the ability of an administrative system to provide appropriate measures against uncertainty and to return to acceptable functioning after exposure to risk, shock or disaster.⁸ This definition carries particular relevance for the Niger Delta, a region whose federal institutions operate under conditions of infrastructural fragility, environmental disturbance and periodic security disruption broadly comparable to those examined in that study.⁹ For the purposes of this study, administrative resilience in federal MDAs in Rivers State is understood as the institutional capacity to maintain continuity of public service delivery, safeguard official and personal information, and adapt administrative practice in the face of infrastructural, technological, security and regulatory disturbance.

3. Theoretical Framework

The theoretical foundation of resilience scholarship traces to the ecological sciences, where it was first articulated as the capacity of a complex system to absorb disturbance without shifting into an alternative and less desirable state of organisation.¹⁰ This ecological conception has since migrated into public administration scholarship, where it has been reframed to describe the capacity of administrative systems, rather than ecosystems, to absorb shocks and reorganise around core functions.¹¹ Applied to the present study, resilience theory suggests that the digital information practice of a federal MDA in Rivers State should be assessed not merely by whether the agency possesses a website or an electronic filing system, but by whether its information architecture is sufficiently robust, secure and adaptable to withstand disruption, whether that disruption takes the form of a cyberattack, a data breach, an electric power failure, or a sudden change in regulatory requirement.

A complementary analytical lens is offered by the Technology-Organisation-Environment framework, which has been applied in recent Nigerian empirical research on digital governance to explain how technological readiness, organisational capacity and the wider policy environment jointly determine the success of digital transformation initiatives in public service delivery.¹² That framework is useful for the present study because it draws attention to the fact that legal reform alone, however well drafted, cannot generate administrative resilience unless it is accompanied by adequate technological infrastructure and organisational capacity within the implementing agency.¹³

⁷Jixiang Li, Shui-Yan Tang and Bo Wen, 'Unpacking Resilience in Public Administration: Insights From a Meta-Narrative Review' (2026) *Public Administration Review* 1, 3.

⁸Md Nazirul Islam Sarker, Min Wu, Roger C Shouse and Chenwei Ma, 'Administrative Resilience and Adaptive Capacity of Administrative System: A Critical Conceptual Review' in *Proceedings of the Thirteenth International Conference on Management Science and Engineering Management*, vol 2 (Springer 2020) 717, 719.

⁹ibid 721.

¹⁰Crawford S Holling, 'Resilience and Stability of Ecological Systems' (1973) 4 *Annual Review of Ecology and Systematics* 1, 14.

¹¹Sarker and others (n 36) 723.

¹²Chinyere N Nwokoroeze, Tochukwu R Onwuekwem and Uchenna H Chukwu, 'Evaluating the Impact of E-Government and Digital Transformation on Public Service Delivery in Nigeria' (2025) 13(2) *Global Journal of Political Science and Administration* 31, 33.

¹³Nwokoroeze and others (n 51) 39.

4. Legal and Regulatory Framework Governing Digital Information in Nigeria

4.1 Constitutional Foundations

The Constitution of the Federal Republic of Nigeria 1999 supplies the foundational normative basis for digital information law. Section 39 guarantees every person the right to freedom of expression, including the right to hold opinions and to receive and impart ideas and information without interference,¹⁴ a provision from which the right of access to public information has been judicially and academically construed to derive. Section 37 separately guarantees the privacy of citizens, their homes, correspondence, telephone conversations and telegraphic communications,¹⁵ a guarantee that has assumed renewed significance in the digital era as the constitutional root from which statutory data protection obligations have grown.

4.2 The Freedom of Information Act 2011

The Freedom of Information Act 2011 establishes the right of any person to request and obtain records or information held by a public institution, subject to defined exemptions, and imposes corresponding obligations on public institutions to proactively and reactively disclose information.¹⁶ The Act has, however, been the subject of sustained scholarly criticism regarding the gap between its statutory promise and its practical implementation. One study has described the Act as a "blunted" instrument whose implementation has been undermined by institutional resistance, judicial hesitancy and a residual culture of official secrecy inherited from the colonial and military periods.¹⁷ A more recent study similarly finds that public institutions frequently fail to comply with their proactive disclosure obligations under the Act, and that the culture of the civil service continues to favour confidentiality over openness notwithstanding the statutory command to the contrary.¹⁸ A comparative study examining the Nigerian experience alongside the United Kingdom and Ghana concludes that the Nigerian Act, unlike its counterparts, lacks a sufficiently robust independent oversight mechanism to compel compliance by reluctant public institutions.¹⁹ For federal MDAs in Rivers State, these implementation deficits translate into practical unpredictability: an agency's compliance with information requests often depends on the disposition of individual desk officers rather than on a settled institutional culture of disclosure, which in turn undermines the transparency dimension of administrative resilience.²⁰

4.3 The Nigeria Data Protection Act 2023

The Nigeria Data Protection Act 2023 repealed the earlier Nigeria Data Protection Regulation of 2019 and established the Nigeria Data Protection Commission as an independent statutory body with regulatory and enforcement powers over data controllers and data processors, including public institutions.²¹ The Act defines a data controller to include any public authority that determines the purposes and means of processing personal data, thereby bringing federal ministries, departments and agencies squarely within its regulatory scope.²² It imposes obligations relating to lawful basis

¹⁴Constitution of the Federal Republic of Nigeria 1999 (as amended), s 39.

¹⁵Constitution of the Federal Republic of Nigeria 1999 (as amended), s 37.

¹⁶Freedom of Information Act 2011, s 1.

¹⁷Uchechukwu Nwoke, 'Access to Information under the Nigerian Freedom of Information Act, 2011: Challenges to Implementation and the Rhetoric of Radical Change' (2019) 63(3) *Journal of African Law* 435, 436.

¹⁸Oludayo John Bamgbose, Oridamilola Adaba Ijiwoye, Juliet Abah and Samson Adeniran, 'Challenges Confronting the Implementation of the Freedom of Information Act (FOIA) in Nigeria' (2025) *International Journal of Legal Information* 1, 2.

¹⁹Nlerum S Okogbule and Bariyima S Kokpan, 'An Overview of the Law and Practice of the Freedom of Information Act in Nigeria: Lessons from UK and Ghana' (2024) 2(4) *Brooklyn Journal of International Law* 1.

²⁰ibid.

²¹Nigeria Data Protection Act 2023, s 2.

²²KPMG Nigeria, *The Nigeria Data Protection Act, 2023: A Review of the Key Compliance Provisions and their Implications for Nigerian Businesses* (KPMG, September 2023) 4.

for processing, data minimisation, security safeguards and breach notification, and prescribes administrative fines of up to two per cent of annual gross revenue for non-compliant organisations.²³ Commentary on the Act observes that it mirrors, though it does not replicate, the structure of the European Union's General Data Protection Regulation, while adapting certain provisions to the Nigerian regulatory and institutional context.²⁴ The Commission has demonstrated a measure of enforcement activity, having in 2025 issued compliance notices to over a thousand organisations across the financial, insurance and gaming sectors and initiated significant enforcement actions against major corporate data controllers.²⁵ It has not yet, however, extended comparable scrutiny to federal government agencies with a significant footprint in personal data processing, such as revenue and immigration authorities operating in Rivers State, a gap that this study considers material to any assessment of administrative resilience.²⁶ Practical compliance guidance issued by professional bodies has emphasised that public institutions, like private organisations, are required to maintain data inventories, appoint data protection officers and generate auditable compliance records,²⁷ obligations that many field offices of federal MDAs in Rivers State are not yet structurally equipped to discharge.²⁸ The absence of dedicated data protection personnel within many local offices increases the likelihood of inadvertent breach and correspondingly reduces institutional resilience against data-related disruption.²⁹

4.4 The National Information Technology Development Agency Act 2007

The National Information Technology Development Agency Act 2007 established the National Information Technology Development Agency and charged it with developing a framework for the planning, standardisation, coordination, monitoring and regulation of information technology practice across public and private sectors in Nigeria.³⁰ The Agency is additionally mandated to render advisory services to public institutions on information technology programmes and to promote the deployment of electronic governance guidelines across government.³¹ It is generally regarded as the primary institutional vehicle for e-government implementation in Nigeria, notwithstanding recurring debate over whether its regulatory mandate is broad enough to compel meaningful digital transformation within resistant public institutions.³² A proposed amendment to the Act, which sought to expand the Agency's licensing and regulatory powers over the wider technology sector, illustrates the continuing effort to strengthen the institutional architecture underpinning digital governance in Nigeria, although the amendment had, as at the time of this study, not been enacted into law.³³

4.5 The Cybercrimes Act 2015 and its 2024 Amendment

The Cybercrimes (Prohibition, Prevention, etc) Act 2015 established a comprehensive framework for the prevention, prohibition and prosecution of cybercrime in Nigeria, and introduced the concept of

²³Nigeria Data Protection Act 2023, ss 24-32.

²⁴G Elias & Co, 'The Nigerian Data Protection Act 2023: A Review' (G Elias & Co, 2023) 3.

²⁵Jones Day, 'Nigeria Launches Investigations into Noncompliance with Nigeria Data Protection Act 2023' (*Jones Day Insights*, 27 August 2025).

²⁶*ibid.*

²⁷Dimeri, 'Nigeria Data Protection Act (NDPA) 2023: Complete Compliance Checklist' (Dimeri, 15 April 2026).

²⁸Planetweb Solutions, 'Nigeria Data Protection Act 2023: Key Features and Legal Framework' (Planetweb Solutions, 27 February 2026).

²⁹Secure Privacy, 'Nigeria Data Protection Law: Complete NDPA Compliance Guide 2025' (*Secure Privacy Blog*, 26 September 2025).

³⁰National Information Technology Development Agency Act 2007, s 6.

³¹National Information Technology Development Agency, 'NITDA Act' (NITDA, 2007).

³²Digital Watch Observatory, 'Nigerian National Information Technology Development Agency (NITDA) Act of 2007' (DiploFoundation, 26 September 2024).

³³Pavestones Legal, 'The Regulation of Technology Companies in Nigeria: The Proposed NITDA Act 2021' (Pavestones Legal, 2021).

Critical National Information Infrastructure, which may be designated by the National Security Adviser for enhanced statutory protection.³⁴ The Cybercrimes (Prohibition, Prevention, etc) (Amendment) Act 2024 revised several provisions of the principal Act, including the offence relating to cyberstalking, which had previously been criticised for its use against journalists and civil society actors, and expanded data retention obligations for service providers in alignment with the Nigeria Data Protection Act 2023.³⁵ Analysis of the amendment observes that organisations classified as Critical Information Infrastructure providers, a category that includes several financial switching and communications entities with which federal revenue and immigration agencies routinely interface, are now required to conduct quarterly vulnerability assessments and appoint dedicated cybersecurity compliance officers.³⁶ Legislative commentary further notes that the amendment expanded the surveillance powers of security agencies, permitting interception of communications without prior judicial authorisation in circumstances described as urgent, a development that has generated concern regarding the balance between national security and civil liberties.³⁷ A separate review observes that the amendment nonetheless leaves unresolved certain structural weaknesses in enforcement capacity, particularly at the sub-national and field-office level where most citizen-facing administrative transactions occur.³⁸ Comparative analysis situates the Nigerian reform within a broader regional trend toward strengthening cybersecurity legislation in response to Nigeria's high global ranking for cybercrime complaints.³⁹ In December 2024, the Federal Government designated specific sectors, including telecommunications, financial systems, power and healthcare infrastructure, as Critical National Information Infrastructure requiring enhanced statutory protection.⁴⁰ International development partners have separately supported capacity-building initiatives directed at improving the ability of Nigerian security institutions to identify and protect critical infrastructure from cyber threats.⁴¹ Sector-specific frameworks, such as the Cyber Resilience Framework introduced by the Nigerian Communications Commission, illustrate a deliberate institutional shift from a purely preventive orientation toward one that explicitly prioritises the capacity of regulated entities to anticipate, withstand and recover from cyber disruption, which is to say, toward resilience in the specific sense this study adopts.⁴²

4.6 The Evidence Act 2011 and Digital Records

The Evidence Act 2011 introduced statutory provision for the admissibility of computer-generated and electronically produced documents, a reform necessitated by the growing prevalence of digital record-keeping in commercial and administrative transactions.⁴³ Section 84 of the Act sets out conditions that a party must satisfy before an electronically generated document may be admitted in evidence, including proof that the computer that produced the document was operating properly at the material time. In the leading authority of *Kubor v Dickson*, the Supreme Court held that a party seeking to tender a computer-generated document must do more than merely produce the document from the bar, and must instead lead evidence establishing the statutory conditions for

³⁴Cybercrimes (Prohibition, Prevention, etc) Act 2015, s 3.

³⁵Cybercrimes (Prohibition, Prevention, etc) (Amendment) Act 2024, s 2.

³⁶AB Legal Practitioners, 'A Review of the Cybercrimes (Prohibition, Prevention, etc) (Amendment) Act, 2024' (AB Legal Practitioners, 5 August 2025).

³⁷National Assembly Legislative Tracking Framework, 'Nigeria's Cybercrime Reform' (NALTF, 17 August 2025).

³⁸DOA Law, 'A Primer on Key Amendments in the Cybercrimes (Amendment) Act 2024' (DOA Law, 10 May 2024).

³⁹Techhive Advisory, 'Nigeria Cybercrimes (Prohibition, Prevention, etc) Act Amendment: Charting Future Direction' (Techhive Advisory Africa, 2024).

⁴⁰FurtherAfrica, 'Safeguarding Nigeria's Critical National Information Infrastructure' (FurtherAfrica, 3 December 2024).

⁴¹Cybil Portal, 'Critical National Infrastructure Threat Assessment and Protection: Defending Nigeria's Critical Assets from Cyber Threats' (Cybil Portal, 11 December 2023).

⁴²The Revealr, 'Cybersecurity as National Security: How NCC's New Framework Targets Telecom Infrastructure Protection' (The Revealr, 10 April 2026).

⁴³Evidence Act 2011, s 84.

admissibility.⁴⁴ The Court's insistence on foundational proof has direct implications for federal MDAs in Rivers State, since administrative records that are generated and stored electronically, including tax assessments, immigration records and customs documentation, must be maintained in a manner that will withstand the evidential scrutiny the Court articulated should such records ever be tendered in proceedings.⁴⁵ This evidential requirement operates alongside the residual restrictions imposed by the Official Secrets Act, which continues, notwithstanding the Freedom of Information Act, to constrain the disclosure of certain categories of official information and thereby introduces a degree of normative tension into the digital information law framework.⁴⁶

5. Comparative Perspectives

5.1 The United Kingdom and the European Union

The United Kingdom's Data Protection Act 2018 supplements the retained European Union General Data Protection Regulation, known domestically as the UK GDPR, and contains provisions specific to public authorities, including tailored rules for law enforcement processing and national security exemptions.⁴⁷ The Information Commissioner's Office is vested with investigative and enforcement powers, including the authority to impose substantial fines and issue enforcement notices against non-compliant public and private bodies.⁴⁸ A 2025 statutory reform, the Data (Use and Access) Act, introduced further adjustments to the UK data protection framework, including refinements to the rules governing automated decision-making, while leaving the foundational structure of the 2018 Act substantially intact.⁴⁹ Commentators note that United Kingdom data protection law imposes an explicit obligation on data controllers to maintain the confidentiality, integrity, availability and resilience of their processing systems, a formulation that places resilience at the very centre of statutory compliance in a manner not yet mirrored with equal explicitness in the Nigerian framework.⁵⁰ The European Union's General Data Protection Regulation, from which the UK framework derives, similarly requires controllers to implement technical and organisational measures ensuring a level of security appropriate to risk, including the ability to restore availability and access to personal data in a timely manner following an incident.⁵¹ These comparative provisions suggest a normative benchmark against which the resilience-orientation of the Nigerian data protection framework may usefully be measured.⁵²

5.2 South Africa and Ghana

South Africa's Promotion of Access to Information Act 2000 has frequently served as a comparative reference point in Nigerian scholarship on freedom of information, principally because both statutes emerged from broadly similar constitutional commitments to transparency and accountable governance.⁵³ Comparative analysis suggests that the South African Act benefits from a more developed judicial enforcement culture, notwithstanding shared criticism regarding the practical accessibility of court-based remedies for ordinary information seekers.⁵⁴ A separate comparative study situates Ghana's approach to freedom of information within a broader West African context,

⁴⁴*Kubor v Dickson* (2013) 4 NWLR (Pt 1345) 534 (SC).

⁴⁵*ibid* 561.

⁴⁶Official Secrets Act, Cap O3, Laws of the Federation of Nigeria 2004, s 1.

⁴⁷Data Protection Act 2018 (UK), s 3.

⁴⁸Securiti, 'The UK GDPR & Data Protection Act 2018: Explained' (Securiti, 2 October 2025).

⁴⁹DLA Piper, 'Data Protection Laws of the United Kingdom' in *Data Protection Laws of the World* (DLA Piper 2025).

⁵⁰TrustArc, 'Difference Between UK Data Protection Act 2018 & GDPR?' (TrustArc, 2 October 2025).

⁵¹CookieYes, 'GDPR vs DPA: Understanding Key Differences in Data Protection' (CookieYes, 3 December 2025).

⁵²Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 (General Data Protection Regulation) [2016] OJ L119/1, art 5.

⁵³Promotion of Access to Information Act 2 of 2000 (South Africa).

⁵⁴Nwoke (n 4) 460.

noting that Ghana's more recent legislative history allowed it to draw lessons from the implementation difficulties experienced in Nigeria and the United Kingdom, particularly around the need for a dedicated oversight institution independent of the public institutions subject to disclosure obligations.⁵⁵ These comparative insights bear directly on this study's conclusion that the absence of a dedicated information commissioner in Nigeria, akin to institutions found in the United Kingdom and increasingly canvassed for Ghana and South Africa, weakens the enforcement architecture available to citizens seeking information from federal MDAs in Rivers State.

6. Digital Information Law and Federal MDAs in Rivers State: Contextual Analysis

6.1 Federal Presence and the Imperative of Digital Reform

Rivers State hosts a dense concentration of federal government presence by virtue of Port Harcourt's status as the principal commercial and logistical hub of the Niger Delta petroleum industry. Federal revenue, customs, immigration, maritime and petroleum-related agencies maintain substantial operational offices within the state, processing significant volumes of personal and commercial data on a continuous basis. At the national level, the Federal Government has in 2026 renewed its commitment to accelerated digitalisation of civil service operations, with the Head of the Civil Service of the Federation setting a target of full digitalisation of ministries, departments and agencies' processes.⁵⁶ This national policy direction places direct pressure on federal offices in Rivers State to modernise their information practice, yet policy pronouncement at the federal centre does not automatically translate into operational capacity at the state or zonal level.⁵⁷

6.2 Records Management and Digitisation Challenges

Empirical research on records management within Nigerian federal ministries indicates persistent capacity deficits, including inadequate staff training, poor security awareness among data administrators and weak institutional performance management of records services.⁵⁸ The National Archives of Nigeria, the federal body constitutionally responsible for records preservation, has itself acknowledged that digitisation of archival material remains an ongoing rather than a completed exercise, requiring sustained investment in microfilming and migration technology to secure long-term preservation of documentary heritage.⁵⁹ These national-level deficits are compounded in Rivers State by the volume and sensitivity of records generated by revenue and immigration functions, which require not only preservation but active protection against unauthorised access, a requirement squarely within the scope of the Nigeria Data Protection Act 2023 discussed above.⁶⁰

6.3 Infrastructure and the Digital Divide

A 2026 national assessment of digital public infrastructure readiness rated Rivers State at medium overall maturity, alongside states such as Lagos, Kano and Enugu, reflecting functional but incomplete digital systems, internet access and digital skills infrastructure.⁶¹ This medium rating indicates that although Rivers State is not among the least digitally prepared states in the federation, it has not yet achieved the infrastructural consistency necessary to fully support the compliance obligations imposed by digital information law on the federal agencies operating within it. Broader

⁵⁵Okogbule and Kokpan (n 6).

⁵⁶Streamlinefeed, 'Federal Government Demands Accelerated Digital Overhaul of Nigeria Civil Service' (Streamlinefeed, 25 May 2026).

⁵⁷Novatia Consulting, 'E-Government Digital Transformation in Nigeria' (Novatia Consulting, 28 July 2025).

⁵⁸Bright E Iwhiwhu, 'Records Managers' Capacity Building for Sustainable Records Management in Federal Ministries' (2020) *International Journal of Library and Information Science*.

⁵⁹National Archives of Nigeria, Federal Ministry of Information and National Orientation, 'National Archives of Nigeria' (fmino.gov.ng, 12 March 2025).

⁶⁰Iwhiwhu (n 53).

⁶¹TheCable, 'Digital but Unequal: Inside Nigeria's State-Level DPI Readiness Divide' (TheCable, 11 May 2026).

assessment of the Niger Delta region identifies unreliable electricity supply, limited broadband penetration and the high cost of digital devices as continuing constraints on digital inclusion, notwithstanding state-level interventions such as technology hub initiatives established to support youth digital skills development.⁶² National commentary similarly attributes much of Nigeria's persistent digital infrastructure gap to the interaction between an unreliable power supply and fragmented policy implementation across federal and state institutions.⁶³ The digital divide, understood broadly as unequal access to information and communications technology infrastructure, therefore continues to condition the practical capacity of federal MDAs in Rivers State to comply with statutory digital information obligations, irrespective of how well drafted those obligations may be in the abstract.⁶⁴

6.4 Cybersecurity and Critical Information Infrastructure

Federal revenue and maritime agencies operating in Rivers State interface routinely with financial switching systems, port logistics platforms and telecommunications infrastructure, categories of infrastructure now formally designated for enhanced protection under the Critical National Information Infrastructure Order of 2024.⁶⁵ The extension of statutory cybersecurity obligations to entities connected with these sectors carries direct implications for federal offices in Port Harcourt, whose data systems interface with nationally designated critical infrastructure. Yet capacity-building assessments of Nigeria's cybersecurity institutions indicate that implementation of critical infrastructure protection frameworks remains at an early stage nationally, with the Office of the National Security Adviser still developing operating models for infrastructure identification and protection as at the most recent reporting period reviewed for this study.⁶⁶ Absent a matching investment in cybersecurity capacity at the state and zonal level, the statutory designation of critical infrastructure risks becoming a formal classification without a corresponding operational safeguard, a gap this study considers material to the administrative resilience of federal MDAs in Rivers State.⁶⁷

7. Findings and Discussion

This study's review of the applicable legal framework and the contextual literature specific to Rivers State yields several interconnected findings. First, Nigeria now possesses a reasonably comprehensive statutory architecture for digital information governance, comprising the Freedom of Information Act 2011, the Nigeria Data Protection Act 2023, the National Information Technology Development Agency Act 2007 and the Cybercrimes Act as amended in 2024. This architecture compares favourably, in structural terms, with comparable frameworks in the United Kingdom and the European Union, notwithstanding the absence of a dedicated information commissioner equivalent to institutions found in those jurisdictions and increasingly canvassed in Ghana.^{68,69} Second, the existence of statutory rules has not translated uniformly into administrative practice. Implementation studies of the Freedom of Information Act consistently document institutional

⁶²Linking Partners for Niger Delta Development, 'Bridging the Digital Divide in the Niger Delta: Youth Pathway for Sustainable Development' (LPND, 14 August 2024).

⁶³Phillips Consulting, 'Bridging the Digital Infrastructure Gap: Smart Transformation for Inclusive Infrastructure' (Phillips Consulting, 24 November 2025).

⁶⁴Wikipedia contributors, 'Digital Divide in Nigeria' (Wikipedia, 2026).

⁶⁵Furtherafrica, 'Safeguarding Nigeria's Critical National Information Infrastructure' (Furtherafrica, 3 December 2024).

⁶⁶Cybil Portal, 'Critical National Infrastructure Threat Assessment and Protection: Defending Nigeria's Critical Assets from Cyber Threats' (Cybil Portal, 11 December 2023).

⁶⁷The Revealer, 'Cybersecurity as National Security: How NCC's New Framework Targets Telecom Infrastructure Protection' (The Revealer, 10 April 2026).

⁶⁸Nlerum S Okogbule and Bariyima S Kokpan, 'An Overview of the Law and Practice of the Freedom of Information Act in Nigeria: Lessons from UK and Ghana' (2024) 2(4) *Brooklyn Journal of International Law* 1.

⁶⁹Okogbule and Kokpan (n 6).

resistance rooted in an inherited culture of official secrecy,⁷⁰⁷¹ while data protection compliance guidance indicates that public sector data controllers, including field offices of federal agencies, remain under-resourced in the specific personnel and procedural infrastructure that statutory compliance requires.⁷²⁷³

Third, the administrative resilience of federal MDAs in Rivers State is constrained less by the absence of law than by the interaction of three non-legal factors, namely infrastructural deficit, human capacity limitation and weak sub-national enforcement presence. The medium digital public infrastructure rating recorded for Rivers State,⁷⁴ combined with continuing electricity and broadband constraints across the Niger Delta,⁷⁵⁷⁶ indicates that the technological foundation for full compliance with digital information law remains incomplete. Records management research further shows that the human capacity required to operationalise digital recordkeeping obligations is unevenly distributed across federal ministries, with security awareness and staff training identified as persistent weaknesses.⁷⁷ Fourth, the Nigeria Data Protection Commission's enforcement activity to date has concentrated on financial, insurance and gaming sector operators, with comparatively limited visible engagement with federal government agencies, notwithstanding the Act's clear application to public institutions as data controllers.⁷⁸⁷⁹ This asymmetry in enforcement focus arguably reduces the practical pressure on federal MDAs in Rivers State to prioritise data protection compliance relative to regulated private sector entities.

Read together, these findings support the conclusion that administrative resilience in this context is not a function of legislative drafting alone but of the institutional capacity of implementing agencies to internalise legal obligations within genuinely functional systems of practice. This conclusion aligns with resilience theory's emphasis on adaptive capacity, understood as the degree to which a system is capable of reorganising itself around new demands rather than merely absorbing formal rule change.⁸⁰⁸¹

8. Recommendations

Arising from the foregoing analysis, this study proposes the following recommendations directed at strengthening the applicability of digital information law to administrative resilience in federal MDAs in Rivers State.

1. The Nigeria Data Protection Commission should extend targeted compliance monitoring and capacity-building engagement to federal government agencies with a significant Rivers State

⁷⁰Uchechukwu Nwoke, 'Access to Information under the Nigerian Freedom of Information Act, 2011: Challenges to Implementation and the Rhetoric of Radical Change' (2019) 63(3) *Journal of African Law* 435, 436.

⁷¹Oludayo John Bamgbose, Oridamilola Adaba Ijiwoye, Juliet Abah and Samson Adeniran, 'Challenges Confronting the Implementation of the Freedom of Information Act (FOIA) in Nigeria' (2025) *International Journal of Legal Information* 1, 2.

⁷²Dimeri, 'Nigeria Data Protection Act (NDPA) 2023: Complete Compliance Checklist' (Dimeri, 15 April 2026).

⁷³Planetweb Solutions, 'Nigeria Data Protection Act 2023: Key Features and Legal Framework' (Planetweb Solutions, 27 February 2026).

⁷⁴TheCable, 'Digital but Unequal: Inside Nigeria's State-Level DPI Readiness Divide' (TheCable, 11 May 2026).

⁷⁵Linking Partners for Niger Delta Development, 'Bridging the Digital Divide in the Niger Delta: Youth Pathway for Sustainable Development' (LPND, 14 August 2024).

⁷⁶Phillips Consulting, 'Bridging the Digital Infrastructure Gap: Smart Transformation for Inclusive Infrastructure' (Phillips Consulting, 24 November 2025).

⁷⁷Bright E Iwhiwhu, 'Records Managers' Capacity Building for Sustainable Records Management in Federal Ministries' (2020) *International Journal of Library and Information Science*.

⁷⁸Jones Day, 'Nigeria Launches Investigations into Noncompliance with Nigeria Data Protection Act 2023' (*Jones Day Insights*, 27 August 2025).

⁷⁹ibid.

⁸⁰Sarker and others (n 36) 723.

⁸¹Li, Tang and Wen (n 38) 9.

presence, rather than concentrating enforcement activity primarily on private sector operators.

2. The National Information Technology Development Agency, in collaboration with the Head of the Civil Service of the Federation, should prioritise infrastructural investment, including reliable power supply and broadband connectivity, for federal offices in Port Harcourt as a precondition for meaningful digitalisation rather than treating digitalisation as a matter of policy declaration alone.
3. Federal MDAs in Rivers State should establish or strengthen dedicated records management and data protection units staffed with personnel trained specifically in electronic recordkeeping standards consistent with the evidential requirements articulated in *Kubor v Dickson* and the substantive obligations of the Nigeria Data Protection Act 2023.
4. The National Assembly should consider legislative amendment to the Freedom of Information Act 2011 to establish an independent information oversight body, drawing on the comparative experience of the United Kingdom's Information Commissioner's Office, to improve enforcement of proactive and reactive disclosure obligations by federal institutions.
5. Security agencies responsible for the protection of Critical National Information Infrastructure should extend operational capacity-building initiatives to Rivers State-based entities connected with designated critical sectors, including port, revenue and telecommunications-linked systems.
6. Federal polytechnics, universities and professional training institutions in Rivers State should be engaged to deliver continuing professional development programmes on digital records management and data protection compliance for civil servants attached to federal MDAs within the state.

9. Conclusion

This study has examined the applicability of digital information law to the administrative resilience of federal government ministries, departments and agencies operating in Rivers State, Nigeria. It has shown that Nigeria's statutory framework, comprising the Freedom of Information Act 2011, the Nigeria Data Protection Act 2023, the National Information Technology Development Agency Act 2007, the Cybercrimes Act 2015 as amended in 2024, and the Evidence Act 2011, provides a structurally sound if imperfect foundation for digital information governance. It has also shown, drawing on resilience theory and comparative material from the United Kingdom, the European Union, South Africa and Ghana, that the practical resilience of federal agencies in Rivers State depends substantially on factors outside the four corners of the statute book, including infrastructural adequacy, institutional capacity and the consistency of regulatory enforcement. Digital information law, properly applied and adequately resourced, holds genuine potential to strengthen the capacity of federal MDAs in Rivers State to anticipate, absorb and recover from administrative disruption. Realising that potential, however, requires sustained institutional commitment that extends well beyond the enactment of statutes to the harder work of building the human, technological and organisational capacity on which resilience ultimately depends.

References

A B Legal Practitioners, 'A Review of the Cybercrimes (Prohibition, Prevention, etc) (Amendment) Act, 2024' (AB Legal Practitioners, 5 August 2025).

Bamgbose OJ, Ijiwoye OA, Abah J and Adeniran S, 'Challenges Confronting the Implementation of the Freedom of Information Act (FOIA) in Nigeria' (2025) *International Journal of Legal Information* 1.

Constitution of the Federal Republic of Nigeria 1999 (as amended).

- CookieYes, 'GDPR vs DPA: Understanding Key Differences in Data Protection' (CookieYes, 3 December 2025).
- Cybercrimes (Prohibition, Prevention, etc) (Amendment) Act 2024.
- Cybercrimes (Prohibition, Prevention, etc) Act 2015.
- Cybil Portal, 'Critical National Infrastructure Threat Assessment and Protection: Defending Nigeria's Critical Assets from Cyber Threats' (Cybil Portal, 11 December 2023).
- Data (Use and Access) Act 2025 (UK).
- Data Protection Act 2018 (UK).
- Digital Watch Observatory, 'Nigerian National Information Technology Development Agency (NITDA) Act of 2007' (DiploFoundation, 26 September 2024).
- Dimeri, 'Nigeria Data Protection Act (NDPA) 2023: Complete Compliance Checklist' (Dimeri, 15 April 2026).
- DLA Piper, 'Data Protection Laws of the United Kingdom' in Data Protection Laws of the World (DLA Piper 2025).
- DOA Law, 'A Primer on Key Amendments in the Cybercrimes (Amendment) Act 2024' (DOA Law, 10 May 2024).
- Evidence Act 2011.
- Freedom of Information Act 2011.
- Furtherafrica, 'Safeguarding Nigeria's Critical National Information Infrastructure' (Furtherafrica, 3 December 2024).
- G Elias & Co, 'The Nigerian Data Protection Act 2023: A Review' (G Elias & Co, 2023).
- Holling CS, 'Resilience and Stability of Ecological Systems' (1973) 4 Annual Review of Ecology and Systematics 1.
- Iwhiwhu BE, 'Records Managers' Capacity Building for Sustainable Records Management in Federal Ministries' (2020) International Journal of Library and Information Science.
- Jones Day, 'Nigeria Launches Investigations into Noncompliance with Nigeria Data Protection Act 2023' (Jones Day Insights, 27 August 2025).
- KPMG Nigeria, The Nigeria Data Protection Act, 2023: A Review of the Key Compliance Provisions and their Implications for Nigerian Businesses (KPMG, September 2023).
- Kubor v Dickson (2013) 4 NWLR (Pt 1345) 534 (SC).
- Li J, Tang S-Y and Wen B, 'Unpacking Resilience in Public Administration: Insights From a Meta-Narrative Review' (2026) Public Administration Review 1.

- Linking Partners for Niger Delta Development, 'Bridging the Digital Divide in the Niger Delta: Youth Pathway for Sustainable Development' (LPND, 14 August 2024).
- National Archives of Nigeria, Federal Ministry of Information and National Orientation, 'National Archives of Nigeria' (fmino.gov.ng, 12 March 2025).
- National Assembly Legislative Tracking Framework, 'Nigeria's Cybercrime Reform' (NALTF, 17 August 2025).
- National Information Technology Development Agency Act 2007.
- National Information Technology Development Agency, 'NITDA Act' (NITDA, 2007).
- Nigeria Data Protection Act 2023.
- Novatia Consulting, 'E-Government Digital Transformation in Nigeria' (Novatia Consulting, 28 July 2025).
- Nwoke U, 'Access to Information under the Nigerian Freedom of Information Act, 2011: Challenges to Implementation and the Rhetoric of Radical Change' (2019) 63(3) Journal of African Law 435.
- Nwokoroeze CN, Onwuekwem TR and Chukwu UH, 'Evaluating the Impact of E-Government and Digital Transformation on Public Service Delivery in Nigeria' (2025) 13(2) Global Journal of Political Science and Administration 31.
- Official Secrets Act, Cap O3, Laws of the Federation of Nigeria 2004.
- Okogbule NS and Kokpan BS, 'An Overview of the Law and Practice of the Freedom of Information Act in Nigeria: Lessons from UK and Ghana' (2024) 2(4) Brooklyn Journal of International Law 1.
- Pavestones Legal, 'The Regulation of Technology Companies in Nigeria: The Proposed NITDA Act 2021' (Pavestones Legal, 2021).
- Phillips Consulting, 'Bridging the Digital Infrastructure Gap: Smart Transformation for Inclusive Infrastructure' (Phillips Consulting, 24 November 2025).
- Planetweb Solutions, 'Nigeria Data Protection Act 2023: Key Features and Legal Framework' (Planetweb Solutions, 27 February 2026).
- Promotion of Access to Information Act 2 of 2000 (South Africa).
- Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 (General Data Protection Regulation) [2016] OJ L119/1.
- Sarker MNI, Wu M, Shouse RC and Ma C, 'Administrative Resilience and Adaptive Capacity of Administrative System: A Critical Conceptual Review' in Proceedings of the Thirteenth International Conference on Management Science and Engineering Management, vol 2 (Springer 2020) 717.

Secure Privacy, 'Nigeria Data Protection Law: Complete NDPA Compliance Guide 2025' (Secure Privacy Blog, 26 September 2025).

Securiti, 'The UK GDPR & Data Protection Act 2018: Explained' (Securiti, 2 October 2025).

Streamlinefeed, 'Federal Government Demands Accelerated Digital Overhaul of Nigeria Civil Service' (Streamlinefeed, 25 May 2026).

Techhive Advisory, 'Nigeria Cybercrimes (Prohibition, Prevention, etc) Act Amendment: Charting Future Direction' (Techhive Advisory Africa, 2024).

The Revealer, 'Cybersecurity as National Security: How NCC's New Framework Targets Telecom Infrastructure Protection' (The Revealer, 10 April 2026).

TheCable, 'Digital but Unequal: Inside Nigeria's State-Level DPI Readiness Divide' (TheCable, 11 May 2026).

TrustArc, 'Difference Between UK Data Protection Act 2018 & GDPR?' (TrustArc, 2 October 2025).

Wikipedia contributors, 'Digital Divide in Nigeria' (Wikipedia, 2026).

Wikipedia contributors, 'National Information Technology Development Agency' (Wikipedia, 2026).

Wikipedia contributors, 'Nigeria Data Protection Commission' (Wikipedia, 2026).