UNIPORT JOURNAL OF BUSINESS, ACCOUNTING & FINANCE MANAGEMENT
DEPARTMENT OF ACCOUNTING,
UNIVERSITY OF PORT HARCOURT,
CHOBA PORT HARCOURT, RIVERS STATE
NIGERIA
VOL. 17 NO. 3 JUNE 2026

ARTIFICIAL INTELLIGENCE ADOPTION AND PUBLIC SERVICE DELIVERY: A CRITICAL EVALUATION OF GOVERNMENT IMPLEMENTATION, DATA GOVERNANCE, AND INSTITUTIONAL REALITIES IN NIGERIA

IHEMADU MICHAEL CHINAZAM N., PhD
Department of Public Administration,
Imo State University, Owerri.
ihemadumichael@ gmail.com

&

ATASIE CHINYERE ODICHE, PhD
Federal Polytechnic Nekede Owerri, Imo State.
atasiechinyere76@gmail.com

Abstract

The strategic adoption of artificial intelligence (AI) and AI-adjacent algorithmic systems within public sector governance is increasingly framed by international development agencies and national governments as a transformative mechanism for enhancing efficiency, transparency, and administrative responsiveness. In Nigeria, successive post-1999 civilian administrations have aggressively pursued digital transformation through foundational e-government initiatives, biometric identity databases, treasury consolidation, and automated electoral management systems, culminating in recent explicit national AI policy frameworks. However, the operational effectiveness of these high-tech interventions remains deeply contested within an institutional landscape characterized by persistent infrastructural deficits, endemic administrative rent-seeking, fragile legal oversight, and low public trust. This paper presents a rigorous qualitative analysis evaluating the extent to which government implementation of AI and AI-adjacent technologies has modified public service delivery in Nigeria. Grounded in a synthesized theoretical framework combining the Technology–Organisation–Environment (TOE) model, Heeks's Design–Reality Gap model, and the Public Values Management (PVM) paradigm, this study critically examines the legal, structural, and socio-political determinants of technological adoption. The findings reveal that the primary impediment to public service delivery in Nigeria is not the absence of advanced algorithmic technology, but rather the structural misalignment between normative technology designs and the institutional realities of the state bureaucracy. Without robust data governance,

algorithmic accountability, and institutional integrity, AI deployments risk automating existing administrative dysfunctions, entrenching socio-economic exclusion, and facilitating novel forms of tech-mediated rent extraction. The paper concludes with an actionable institutional framework for achieving responsible, transparent, and contextually grounded AI adoption in Sub-Saharan African public administration.

Keywords: Artificial Intelligence, Public Service Delivery, Digital Government, Algorithmic Accountability, Data Governance, Technology–Organisation–Environment (TOE), Design–Reality Gap.

Introduction

The fast-growing integration of digital technologies into the core machinery of the administrative state is a representation of one of the most defining structural shifts in global public administration during the early twenty-first century. Following the initial wave of new public management (NPM) and preliminary e-government reforms throughout the 1990s and 2000s, global governance paradigms have increasingly pivoted toward data-driven, algorithmic, and artificial intelligence (AI) systems. Contemporary public bureaucracies across both developed and emerging economies now routinely deploy automated decision-making platforms, machine learning algorithms, natural language processing models, and computer vision systems to optimize tax administration, streamline social benefit allocations, manage urban traffic, automate security surveillance, and process citizen queries (Wirtz et al., 2019; Zuiderwijk et al., 2021).

According to Zuiderwijk et al. (2021), the core normative premise that underscores AI adoption in the public realm hinges on the assertion that algorithmic systems can process vast administrative datasets at unprecedented scales, eliminate human discretion and corrupt discretion, minimize operational overhead, and deliver personalized public services to historically marginalized populations.

For developing nations in the Global South, particularly in Sub-Saharan Africa, the prospective promises of AI-driven administrative modernization possess profound strategic appeal. As the most populous nation and largest economy on the African continent, Nigeria operates a complex federal structure comprising 36 states, 774 local government areas, and a massive federal bureaucracy tasked with servicing over 220 million citizens. However, since the historic return to civilian democratic rule in May 1999, public service delivery across vital socio-economic sectors—including primary healthcare, basic education, national identity management, public revenue collection, and electoral administration—has consistently failed to meet public expectations regarding the democratic dividend (Aluaigba, 2016). According to Obi (2022), the Nigerian public service has historically been crippled by entrenched bureaucratic red tape, pervasive ghost-worker payroll fraud, institutional rent-seeking, systemic opacity, and severe spatial disparities in service access between urban centers and rural peripheries.

In direct response to these long-standing structural crises, successive Nigerian federal administrations have repeatedly treated digital technology as an institutional panacea or shortcut to administrative integrity and operational efficiency. Over the past two decades, state authorities have designed and deployed an array of major technological interventions. These range from mandatory biometric identity registers under the National Identity Management Commission (NIMC) and the Integrated Payroll and Personnel Information System (IPPIS), to the Treasury Single Account (TSA), Bank Verification Number (BVN) systems, and sophisticated electoral technologies including the Bimodal Voter

Accreditation System (BVAS) and the INEC Result Viewing (IReV) portal. Most recently, following the reorganization of the Federal Ministry of Communications, Innovation and Digital Economy, Nigeria has articulated an explicit national ambition to harness artificial intelligence as a primary engine for administrative modernization, economic growth, and public service innovation.

However, scholarly research examining technology implementation within developing bureaucracies suggests that high-tech interventions frequently produce paradoxical, unintended, or disruptive administrative outcomes. According to Heeks (2002), an overwhelming majority of e-government and digital transformation projects in developing countries experience either complete or partial failure. Heeks (2006) argues that these failures stem primarily from severe "design–reality gaps"—the profound mismatch between the idealized institutional conditions assumed by system developers and the actual, volatile operational realities of the target public organizations. In environments where fundamental electricity infrastructure is unstable, broadband internet access is geographically unequal, technical expertise is scarce within the civil service, and legal safeguards for data protection are weakly enforced, the introduction of advanced AI systems presents immense structural risks. Rather than automatically improving service delivery, advanced algorithms introduced into weak institutional settings may merely accelerate existing bureaucratic dysfunctions, codify historical biases, deepen citizen exclusion, and generate lucrative new avenues for procurement fraud and state capture.

Furthermore, technology deployment within the Nigerian public administration is inextricably entangled with broader political dynamics of institutional trust, state legitimacy, and democratic consolidation. As demonstrated by Aluaigba (2016) in his landmark analysis of electoral malpractices and democratic consolidation in Nigeria, technical and procedural innovations introduced to safeguard process integrity can be easily undermined or neutralized when institutional actors lack systemic integrity or operate under perverse political incentives. The introduction of biometric voter accreditation and electronic results transmission mechanisms was designed to eliminate human manipulation; yet, operational breakdowns, selective technical failures, and opaque administrative decisions during election cycles revealed that technological sophistication cannot serve as a structural substitute for institutional integrity and democratic accountability. The exact same analytical logic applies to the deployment of AI algorithms in public service delivery: an automated credit assessment tool, tax audit algorithm, or identity verification system is only as fair, impartial, and effective as the state institution that designs, configures, and oversees its execution.

This paper addresses critical scholarly and policy gaps by providing a rigorous, qualitative assessment of artificial intelligence adoption within the Nigerian public sector. Specifically, the paper addresses four central research questions:

1. In what ways has the implementation of digital, automated, and AI-adjacent systems impacted the efficiency, equity, and transparency of public service delivery in Nigeria since 1999?
2. What specific technological, organizational, and environmental factors enable or constrain the sustainable adoption of AI technologies within the Nigerian civil service?
3. To what extent can the normative promises of AI-driven public administration be realized in an environment characterized by fragile data governance, persistent infrastructural deficits, and low public trust in state institutions?

4. What legal, policy, structural, and operational frameworks are required to chart a credible, contextually grounded path toward responsible, accountable, and inclusive AI adoption in Nigerian governance?

To address these questions, this study employs an analytical framework that integrates the Technology–Organisation–Environment (TOE) framework developed by Tornatzky and Fleischer (1990), Heeks's (2002, 2006) Design–Reality Gap model, and Bannister and Connolly's (2014) Public Values Management framework. Methodologically, the paper synthesizes qualitative policy analysis, legislative evaluations, public expenditure reports, administrative records, and extensive secondary scholarly literature.

A crucial conceptual caveat regarding scope must be established at the outset. While current national policy rhetoric heavily emphasizes "Artificial Intelligence," much of what has actually been operationalized across the Nigerian public sector to date is more accurately categorized as foundational digitalization, database integration, or rule-based software automation rather than dynamic, self-learning artificial intelligence in the strict machine-learning sense. Nevertheless, this paper explicitly treats these existing digital, biometric, and automated administrative networks as "AI-adjacent systems." They constitute the essential data infrastructure, organizational habits, and regulatory baseline upon which any future generation of public sector AI applications must be built.

The remainder of this paper is organized into seven distinct structural sections:

- Section 2 presents a comprehensive conceptual clarification differentiating digitalization, rule-based automation, and artificial intelligence, alongside an analysis of public service delivery metrics and digital-era governance paradigms.
- Section 3 establishes the integrated theoretical framework guiding the analysis.
- Section 4 critically evaluates the evolving legal, regulatory, and institutional framework governing digital technology, data privacy, and AI in Nigeria.
- Section 5 traces the historical evolution and phases of digital technology adoption in the Nigerian public sector from 1999 to 2026.
- Section 6 delivers an empirical and theoretical critique of the impacts of adoption across key administrative domains, emphasizing efficiency, exclusion, bias, discretion, and public trust.
- Section 7 articulates an actionable institutional roadmap and policy recommendations for responsible AI deployment.
- Section 8 provides a synthesis of conclusions and outlines a future research agenda.

LITERATURE REVIEW AND CONCEPTUAL CLARIFICATIONS

Disentangling Digitalization, Rule-Based Automation, and Artificial Intelligence

A central conceptual challenge in contemporary public administration scholarship is the frequent blurring of boundaries between basic digital conversion, deterministic automation, and genuine artificial intelligence. To evaluate the true impact of public sector technology, precise theoretical definitions are required.

THE DIGITAL EVOLUTION SPECTRUM		
1. DIGITALIZATION	2. RULE-BASED AUTOMATION	3. ARTIFICIAL INTELLIGENCE
- Paper to Digital	- Fixed "If-Then" Logic	- Machine Learning/NLP
- Database Creation	- IPPIS, TSA, Standard Portals	- Probabilistic Predictions
- Scanning & Indexing	- Deterministic Execution	- Adaptive & Self-Learning

Digitalization, in its primary technical sense, refers to the organizational process of converting non-digital, paper-based information, administrative logs, and manual workflows into binary digital formats (Mergel et al., 2019). It represents the foundational transition from analogue record-keeping to computer-readable databases. In contrast, *Rule-Based Automation* involves the execution of fixed, deterministic, pre-programmed software instructions designed to perform repetitive tasks without human intervention. Standard administrative workflows—such as automated payroll deductions under Nigeria's Integrated Payroll and Personnel Information System (IPPIS) or automated bank sweeps via the Treasury Single Account (TSA)—are classic examples of deterministic automation. They operate strictly on explicit "if-then" computational logic designed directly by human programmers; the software possesses zero capacity to adapt its execution based on underlying patterns in the data processed.

Conversely, *Artificial Intelligence (AI)* in public administration represents a fundamentally distinct category of sociotechnical systems. As defined by Wirtz et al. (2019), AI encompasses an interrelated constellation of advanced technologies—including statistical machine learning (ML), deep neural networks, natural language processing (NLP), computer vision, and cognitive expert systems—that enable computational machines to execute tasks historically requiring human cognitive intelligence.

According to Bullock (2019), four core technical and operational features distinguish AI from previous generations of public sector IT systems:

1. **Inference and Learning from Data:** Unlike deterministic rule-based software, AI models do not rely solely on hard-coded human logic. Instead, machine learning algorithms analyze historical administrative datasets to independently identify latent patterns, construct probabilistic prediction models, and generate predictive outputs or administrative decisions for novel, unseen cases (Zuiderwijk et al., 2021).
2. **Operational Scale and Velocity:** AI systems are capable of processing and analyzing vast, non-linear administrative datasets (Big Data) across millions of citizen records in real-time, executing classifications or fraud detection tasks at speeds unattainable by human civil servants.
3. **Algorithmic Opacity ("Black Box" Problem):** The mathematical reasoning through which deep learning models arrive at specific predictions or outputs is frequently opaque, complex, and non-interpretable even to the software engineers who constructed the underlying code. This creates unprecedented challenges for administrative law, procedural due process, and public justification (Pasquale, 2015; Floridi et al., 2018).
4. **Shift in Administrative Discretion:** AI adoption fundamentally relocates discretionary power within the public bureaucracy. Rather than front-line civil servants exercising subjective human discretion at the service counter, discretion is effectively migrated upstream to data scientists, algorithm designers, and private software vendors who determine model parameters, training data choices, and risk thresholds (Bullock, 2019; Dunleavy et al., 2006).

Understanding this continuum is vital for analyzing developing democracies like Nigeria. As Obi (2023) observes, the vast majority of digital systems deployed across Nigerian federal and state ministries between 2000 and 2020 belong firmly to the categories of basic digitalization and rule-based automation. However, examining these foundational systems is indispensable because they generate the digital records, biometric identity registries,

and organizational data pipelines upon which any subsequent deployment of public sector AI must depend.

Reconceptualizing Public Service Delivery and Public Values

Public service delivery constitutes the primary interface through which citizens experience the authority, capability, and legitimacy of the administrative state. It encompasses the institutional mechanisms through which governments supply essential public goods, services, and regulatory oversight that citizens are legally entitled to or dependent upon. These include primary healthcare, public education, civil registration, land title verification, tax administration, public safety, business licensing, and electoral administration.

In traditional public administration and NPM paradigms, the quality of public service delivery was evaluated almost exclusively through narrow, transactional micro-economic metrics: cost reduction, processing speed, operational efficiency, and throughput volume. However, contemporary public value scholars argue that assessing technology in the public realm requires a significantly broader normative framework. Bannister and Connolly (2014) assert that public sector IT deployment must be evaluated against the overarching paradigm of **Public Values Management (PVM)**. From a public values perspective, public services cannot be treated merely as transactional commercial products, nor can citizens be reduced to mere consumers.

Rather, government technology must actively safeguard and promote fundamental democratic values, including:

- **Administrative Equity and Justice:** Ensuring services are distributed impartially, preventing algorithmic discrimination, and ensuring that vulnerable or digitally illiterate populations are not systematically excluded from state benefits.
- **Procedural Transparency and Explainability:** Guaranteeing that citizens understand how administrative decisions affecting their rights or entitlements were made, particularly when automated algorithms are utilized.
- **Accountability and Contestability:** Maintaining clear mechanisms of administrative appeal, human oversight, and legal redress when technology platforms fail or produce erroneous outputs.
- **Institutional Trust and Legitimacy:** Ensuring that technological adoption reinforces, rather than erodes, citizen confidence in the integrity, impartiality, and benevolence of public institutions.

As Obi (2022) notes in his analysis of bureaucratic reforms in West Africa, the central crisis of public service delivery in Nigeria is fundamentally a crisis of institutional integrity and equity rather than a simple problem of computational speed. Therefore, evaluating AI adoption in Nigeria through a public values lens is critical for determining whether technology strengthens democratic statehood or merely optimizes autocratic efficiency.

Digital-Era Governance (DEG) in the Post-NPM Landscape

The theoretical evolution of public administration over the past three decades provides crucial context for understanding current AI policy trajectories. Dunleavy et al. (2006) formulated the **Digital-Era Governance (DEG)** framework as an explicit theoretical counterweight to the fragmented, marketized, and privatized administrative paradigms of New Public Management (NPM) that dominated the 1980s and 1990s. Dunleavy et al. (2006) argued that NPM reforms heavily fragmented the public sector into isolated executive agencies, generated excessive transaction costs, and eroded institutional

memory. DEG posits that contemporary public sector reform is driven by three key operational pillars:

1. **Re-integration:** Joining up fragmented state agencies and databases through shared digital platforms, centralized data repositories, and interoperable administrative networks.
2. **Holism:** Organizing public service workflows around citizen life-events and holistic needs rather than rigid, isolated departmental silos.
3. **Digitalisation:** Embedding digital platforms, automated workflows, and data analytics into the core operational fabric of state administration.

AI deployment represents the ultimate technological extension of Digital-Era Governance. However, as Mergel et al. (2019) critically emphasize, achieving meaningful digital transformation under DEG requires far more than purchasing software or building websites; it necessitates fundamental structural shifts in organizational culture, administrative law, civil service skills, and state-citizen relations.

In a developing federal polity such as Nigeria—where federal, state, and local government tiers frequently operate under severe political friction, administrative jealousy, and uncoordinated technology procurement—the systemic integration demanded by DEG faces immense structural barriers.

Part 2

Theoretical Framework

To rigorously analyze the adoption, implementation, and administrative impacts of artificial intelligence (AI) and AI-adjacent technologies within the Nigerian public sector, this study adopts an integrated multi-theoretical framework. Public sector technology implementation in developing states is rarely a purely technical endeavor; rather, it is a deeply sociotechnical process embedded in complex historical, political, structural, and legal environments. To capture this multi-dimensional complexity, the study synthesizes three complementary analytical models:

1. The **Technology–Organisation–Environment (TOE) Framework** (Tornatzky & Fleischer, 1990).
2. The **Design–Reality Gap Model** (Heeks, 2002, 2006).
3. The **Public Values Management (PVM) Framework** (Bannister & Connolly, 2014).

The Technology–Organisation–Environment (TOE) Framework

The Technology–Organisation–Environment framework, originally formulated by Tornatzky and Fleischer (1990), posits that the adoption and structural implementation of technological innovations in an organization are conditioned by three distinct context domains:

1. Technological Context

This domain encompasses both the internal and external technologies available to, or already utilized by, the organization. Crucial elements include:

- Equipment availability and technical architecture.
- Data quality, structure, and integrity.
- Bandwidth connectivity and system compatibility/interoperability.

In evaluating public sector AI in Nigeria, the technological context focuses on whether state agencies possess clean, standardized administrative datasets, reliable cloud/server infrastructure, and interoperable software frameworks required to run machine learning models. As Sun and Medaglia (2019) emphasize in their analysis of public

sector AI challenges, algorithmic tools are fundamentally dependent on the maturity of underlying data pipelines; without robust technological foundations, AI algorithms yield erratic or biased outputs.

2. Organisational Context

This domain relates to the internal structural characteristics, resource availability, administrative culture, and managerial capabilities of the adopting state institution. Key indicators include:

- Top-management leadership and political drive.
- Administrative capacity and technical skills within the civil service.
- Organizational size, structural flexibility, and resource allocation.
- Pre-existing bureaucratic culture and institutional resistance to change.

In the Nigerian civil service, organizational capacity is frequently constrained by skill deficits in computational data science, institutional inertia, and resistance from staff who perceive automated, audit-capable platforms as threats to informal rent-seeking opportunities (Obi, 2022).

3. Environmental Context

This domain encompasses the external arena in which the government agency operates, including:

- The macroeconomic condition and legal/regulatory framework.
- Political pressures, donor influence, and public expectations.
- Private vendor market dynamics and technological dependence.

For Nigeria, the environmental context involves national legislation (such as data protection and cybercrime laws), executive political mandates, international development agency pressures, and the influence of global commercial software vendors. Zuiderwijk et al. (2021) observe that environmental pressures often drive public agencies in developing countries to adopt fashionable technologies symbolically before the requisite legal and regulatory safeguards are established.

Heeks's Design–Reality Gap Model

While the TOE framework provides a multi-dimensional inventory of adoption drivers, Richard Heeks's (2002, 2006) Design–Reality Gap model provides a precise diagnostic tool for evaluating why technology projects in developing countries succeed, partially fail, or fail totally. Heeks argues that information systems designed for public sector administration inherently embed specific normative assumptions about the context in which they will operate. When there is a profound mismatch or "gap distance" between the **design assumptions** embedded in the technology and the **operational reality** of the adopting context, project failure is virtually inevitable.

Heeks (2006) categorizes these context gaps across seven distinct administrative dimensions, conceptualized under the **ITPOSMO** acronym:

1. **Information:** The gap between the clean, centralized, digitized data assumed by AI system designers and the fragmented, paper-based, incomplete, or corrupted records prevalent in Nigerian ministries.
2. **Technology:** The gap between the assumed infrastructure (continuous power, high-speed fiber-optic internet, edge computing) and the operational reality of erratic power supply and patchy internet connectivity across Nigerian states and local government areas.

3. **Processes:** The gap between the streamlined, rationalized administrative workflows assumed by software developers and the informal, highly discretionary, paper-driven routines deeply entrenched within the bureaucracy.
4. **Objectives and Values:** The gap between the public values built into software design (transparency, objective merit, meritocratic processing) and the actual objectives of political actors or bureaucrats (patronage, rent-extraction, political control).
5. **Staffing and Skills:** The gap between the high-level computational, analytical, and ethical skills required to oversee AI systems and the actual skill profile of civil servants operating the platform.
6. **Management Systems and Structures:** The gap between the integrated, agile management structures required for data-driven governance and the rigid, hierarchical, siloed departmental structures characteristic of Nigerian public administration.
7. **Other Resources:** The gap between the financial and temporal resources required for continuous system maintenance, software updating, and cybersecurity, and the actual, erratic budgetary allocations provided by state treasuries.

According to Heeks (2002), the wider the gap between design assumptions and context realities across these seven dimensions, the higher the probability that the technology will fail or produce severe unintended dysfunctions.

The Public Values Management (PVM) Framework

To evaluate whether technology adoption genuinely improves the *quality* of public service delivery, this study incorporates the Public Values Management paradigm formulated by Bannister and Connolly (2014). Unlike traditional administrative theories that evaluate technology strictly through metrics of speed, cost reduction, and processing volume, the PVM framework asserts that public sector technology must be judged by its contribution to fundamental democratic and administrative values.

Bannister and Connolly (2014) categorize public values into three core domains:

- **Duty-Oriented Values:** Including administrative fairness, statutory lawfulness, equity, procedural due process, and human rights protection. In the context of AI, this requires algorithmic transparency, non-discrimination, and the protection of citizens' privacy.
- **Service-Oriented Values:** Including operational efficiency, service timeliness, cost-effectiveness, accessibility, and administrative responsiveness.
- **Relational Values:** Including public trust in state institutions, administrative openness, democratic accountability, and state legitimacy.

Applied to the Nigerian public sector, the PVM framework serves as a critical normative standard. It provides the analytical tools to question whether an AI-driven payroll system, identity register, or voter accreditation platform that increases administrative speed (a service-oriented value) simultaneously erodes citizen trust or disenfranchises vulnerable demographics (relational and duty-oriented values).

Synthesis and Theoretical Hypotheses

By integrating the TOE framework, Heeks's Design–Reality Gap model, and Bannister and Connolly's Public Values Management framework, this study constructs a comprehensive analytical lens for evaluating AI implementation in Nigeria. The synthesis leads to three central theoretical propositions that guide the empirical analysis in subsequent sections:

Proposition 1: The successful adoption and operationalization of AI and AI-adjacent systems in the Nigerian public sector are directly constrained by structural deficits in the technological context (data quality and infrastructure) and organizational context (civil service skills and administrative incentives), regardless of political policy declarations.

Proposition 2: Where large design–reality gaps exist across Heeks's ITPOSMO dimensions—particularly regarding process, values, and technological infrastructure—the introduction of automated or AI-driven systems will not eliminate administrative dysfunction. Instead, it will displace corruption and discretion to higher, less visible administrative levels (such as technology procurement, database administration, and algorithmic configuration).

Proposition 3: Technology adoption in Nigerian governance enhances public service delivery if and only if it balances operational efficiency gains with duty-oriented public values (data privacy, non-discrimination, procedural fairness) and relational public values (transparency, accountability, and citizen trust).

LEGAL, REGULATORY, AND POLICY FRAMEWORK FOR DIGITAL GOVERNMENT AND AI IN NIGERIA

The trajectory of digital government and AI adoption in Nigeria is bounded by a fragmented, multi-layered assemblage of constitutional provisions, statutory enactments, executive orders, sector-specific regulations, and national policy strategies. Unlike some developed jurisdictions that have enacted unified, comprehensive statutory frameworks specifically governing artificial intelligence (such as the European Union AI Act), Nigeria's legal landscape governs AI indirectly through a patchwork of statutes covering information technology development, telecommunications, national identity, data protection, cybercrime, public procurement, and electoral administration.

Institutional Foundations: NITDA and Telecommunications Regulation

The legal foundation for digital public administration in Fourth Republic Nigeria was laid with the adoption of the National Information Technology Policy in 2001 and the subsequent establishment of the **National Information Technology Development Agency (NITDA)**. The agency's administrative mandate was formally codified into law through the **NITDA Act of 2007**. The Act empowers NITDA to:

- Formulate national IT guidelines, standards, and regulations.
- Oversee public sector IT procurement and system integration.
- Coordinate the development of electronic governance infrastructure across federal ministries, departments, and agencies (MDAs).

Simultaneously, the liberalisation and regulatory architecture of the telecommunications market—established under the **Nigerian Communications Act 2003** and overseen by the **Nigerian Communications Commission (NCC)**—created the essential digital connectivity infrastructure upon which all subsequent e-government, biometric, and AI platforms depend. The NCC's regulatory oversight over Mobile Network Operators (MNOs), broadband spectrum auctions, and subscriber identification module (SIM) registration protocols created the primary connectivity backbone that links citizens to digital public services.

However, legal scholars and public administration experts point to significant structural overlap and jurisdictional friction between NITDA, the Ministry of Communications, Innovation and Digital Economy, and sector-specific regulators (Obi, 2023). According to Obi (2023), NITDA's statutory enforcement powers have historically

been weakened by institutional conflicts with line ministries, which frequently procure proprietary IT and software architecture independently of NITDA's standardisation guidelines.

Identity Infrastructure: The NIMC Act 2007

A foundational prerequisite for deploying AI systems in public administration—particularly in automated service delivery, social welfare targeting, and law enforcement—is the existence of a accurate, verifiable national identity database. The **National Identity Management Commission (NIMC) Act of 2007** established NIMC, charging it with the statutory responsibility to:

- Create, operate, and maintain the National Identity Database.
- Issue a unique National Identification Number (NIN) to all legal residents and citizens.
- Integrate existing disparate biometric databases across state institutions.

Section 27 of the NIMC Act renders the presentation of a NIN mandatory for carrying out key administrative and financial transactions, including:

- Applying for or renewing international passports.
- Opening bank accounts and accessing public credit.
- Registering SIM cards with telecommunications providers.
- Accessing social safety net transfers and public pension schemes.

Through executive orders and regulatory directives between 2020 and 2022, the federal government enforced the mandatory linkage of NINs to all active telecommunications SIM lines and bank accounts (via the Bank Verification Number system). This regulatory integration successfully created the largest centralized biometric identity repository in West Africa.

Yet, as critically examined in subsequent sections, the legal framework governing NIMC provides insufficient statutory protection against arbitrary data sharing, government surveillance, and the systematic exclusion of citizens who encounter structural barriers during biometric enrollment (Eubanks, 2018).

Data Governance and Privacy: NDPR 2019 to the Nigeria Data Protection Act 2023

Prior to 2019, Nigeria lacked a comprehensive legal framework governing data privacy, data subject rights, and the processing of personal information by public and private entities. The regulatory gap was initially addressed when NITDA issued the **Nigeria Data Protection Regulation (NDPR) 2019** under its general administrative powers. While the NDPR established foundational principles regarding data collection, consent, and storage, its status as a subsidiary regulation exposed it to legal challenges regarding its enforceability against sovereign government ministries.

A milestone in Nigeria's digital legal framework occurred with the enactment of the **Nigeria Data Protection Act (NDPA) 2023**, signed into law in June 2023. The NDPA 2023 elevated data privacy to a statutory level, establishing an independent regulatory body: the **Nigeria Data Protection Commission (NDPC)**.

Key Provisions of the NDPA 2023 Relevant to Public Sector AI:

1. **Principles of Data Processing (Section 24):** Mandates that personal data processed by public and private controllers must be collected lawfully, transparently, and for specific, explicit, and legitimate purposes. Data processing must adhere to principles of data minimization, accuracy, storage limitation, and robust security.

2. **Legal Basis for Public Sector Processing (Section 25):** Clarifies that government agencies processing citizen data must establish a valid legal basis, such as statutory mandate, public interest, or explicit consent.
3. **Automated Decision-Making and Profiling (Section 37):** Contains provisions directly addressing automated processing and profiling. Section 37 guarantees data subjects the right **not** to be subject to a decision based solely on automated processing—including profiling—which produces legal effects or significantly affects the individual, unless specific exceptions apply (such as explicit statutory authorization or performance of a public task).
4. **Data Protection Impact Assessments (DPIAs) (Section 33):** Mandates that where data processing—particularly involving emerging, automated technologies—is likely to result in high risks to the rights and freedoms of individuals, the data controller must conduct a comprehensive DPIA prior to processing.

The NDPA 2023 represents a crucial legal safeguard against the arbitrary deployment of algorithmic decision-making tools by government agencies. However, as legal scholars note, the actual institutional independence and regulatory capacity of the NDPC to enforce compliance against powerful sovereign bodies—such as state security agencies, tax authorities, and federal ministries—remains an unresolved structural challenge.

Emerging Policy Landscapes: NDEPS, NCAIR, and the National AI Strategy

Alongside formal statutory enactments, the executive arm of government has articulated a series of high-level policy strategies designed to position Nigeria as a regional leader in digital economy infrastructure and emerging technologies.

National Digital Economy Policy and Strategy (NDEPS 2020–2030)

Formulated by the then-Federal Ministry of Communications and Digital Economy, NDEPS establishes eight executive pillars designed to accelerate digital transformation:

1. Developmental Regulation.
2. Digital Literacy and Skills.
3. Solid Infrastructure.
4. Service Infrastructure.
5. Digital Services Development and Promotion.
6. Soft Infrastructure (Cybersecurity and Data Protection).
7. Digital Society and Emerging Technologies.
8. Indigenous Content Development and Adoption.

Pillar 7 explicitly prioritizes national capacity building in artificial intelligence, robotics, blockchain, and cybersecurity. Under this pillar, the federal government established the **National Centre for Artificial Intelligence and Robotics (NCAIR)** as a specialized research hub under NITDA tasked with promoting applied research, incubating local tech talent, and prototyping AI solutions for public administration and industry.

The National AI Strategy Process (2024 Onward)

Following the reorganization of the ministry into the **Federal Ministry of Communications, Innovation and Digital Economy**, the federal government launched a national initiative to formulate a comprehensive **National Artificial Intelligence Strategy**. Through a co-creation workshop involving local and international AI researchers, data scientists, and policy experts, the ministry outlined key strategic priorities:

- Developing a national Large Language Model (LLM) trained on indigenous Nigerian languages to prevent cultural and linguistic bias in AI systems.
- Constructing computing infrastructure, AI research hubs, and high-performance computing centers.
- Expanding technical capacity through national talent acceleration initiatives, such as the **3 Million Technical Talent (3MTT)** programme.
- Formulating ethical AI guidelines emphasizing fairness, safety, non-discrimination, and human oversight in public sector AI deployment.

Sectoral Legal Frameworks: The Electoral Act 2022 and FOI Act 2011

Electoral Administration and Technology: The Electoral Act 2022

In the domain of electoral governance—which represents the most scrutinised application of technology in Nigerian public administration—the **Electoral Act of 2022** provided landmark legal authorization for technological innovation. Section 47(2) of the Act formally legalized the use of electronic devices for voter accreditation, providing statutory backing for the **Bimodal Voter Accreditation System (BVAS)**.

Furthermore, Sections 60 and 64 empowered the Independent National Electoral Commission (INEC) to prescribe electronic procedures for the real-time transmission of polling unit results to the **INEC Result Viewing (IReV)** portal.

As Aluaigba (2016) demonstrated in his analysis of pre-2022 electoral technology, statutory backing for technological tools is vital for preventing judicial invalidation of technology-driven administrative processes. However, as the judicial disputes following the 2023 general elections showed, ambiguity in statutory drafting regarding whether electronic transmission is legally *mandatory* or merely *discretionary* can severely erode public confidence in technological integrity.

Transparency and Algorithmic Openness: Freedom of Information Act 2011

The **Freedom of Information (FOI) Act of 2011** gives citizens and civil society organizations the legal right to request records, contracts, source codes, data architectures, and operational evaluations from public institutions. In an era of AI governance, the FOI Act serves as an essential, yet underutilized, tool for demanding **algorithmic transparency**. It provides the statutory mechanism through which researchers and citizens can inspect how government algorithms are procured, what training datasets are utilized, and how risk-scoring models make automated administrative decisions.

Critical Evaluation of the Legal and Regulatory Landscape

While Nigeria's legal framework for digital technology and data protection has matured significantly over the past two decades, several structural vulnerabilities persist:

1. **Absence of Statutory Algorithmic Accountability:** Nigerian law contains no explicit requirement forcing government agencies to conduct pre-deployment algorithmic impact assessments, perform open-source code audits, or publish algorithmic logic for public scrutiny before deploying automated decision tools.
2. **Regulatory Overlap and Conflict:** Statutory jurisdiction over digital systems remains fragmented among NITDA, NDPC, NCC, NIMC, and individual line ministries, leading to duplicated regulatory efforts, conflicting guidelines, and regulatory arbitrage by private technology vendors.
3. **Enforcement Gaps Against the State:** While the NDPA 2023 grants strong rights on paper, the NDPC lacks financial independence and operational enforcement power to

penalize powerful sovereign bodies (such as security agencies or financial ministries) when they violate citizen data privacy rights.

4. **Procurement Opacity:** Public procurement laws governing technology acquisition remain largely conventional, lacking specialized protocols for evaluating machine learning software, training dataset representations, intellectual property ownership of source code, and long-term vendor lock-in risks.

As summarized in Table 3, the existing legal framework provides a foundational, yet structurally incomplete, architecture for regulating public sector AI in Nigeria.

Table 3: Comparative Mapping of Nigeria's Legal Framework and AI Governance Requirements

Legal / Policy Instrument	Core Statutory Purpose	Primary Governance Strengths	Key AI-Specific Regulatory Deficits
NITDA Act 2007	Establishes NITDA; mandates national IT standardisation and e-government coordination.	Provides broad regulatory mandate over public sector IT procurement and digital architecture.	Lacks explicit statutory provisions governing machine learning algorithms, automated profiling, or AI ethical standards.
NIMC Act 2007	Establishes national identity database and mandatory NIN usage.	Constructs centralized biometric identity infrastructure required for integrated public service delivery.	Weak statutory safeguards against arbitrary database linkage, state surveillance, and technological exclusion of marginalized groups.
Cybercrimes Act 2015	Criminalizes unauthorized access, identity theft, and cyberattacks on Critical National Information Infrastructure.	Establishes criminal penalties for hacking public sector databases and compromising national digital networks.	Focuses strictly on external cyber threats; fails to regulate internal algorithmic misuse or data corruption by state actors.
Nigeria Data Protection Act (NDPA) 2023	Provides statutory framework for data privacy; establishes independent NDPC.	Enacts data minimization, mandatory DPIAs, and data subject rights regarding automated decision-making (Section 37).	Regulatory enforcement capacity against sovereign state institutions remains untested; lacks dedicated algorithmic audit guidelines.
NDEPS (2020–2030)	Ten-year national strategy for digital economy expansion and emerging technology adoption.	Prioritizes capacity building, local content creation, and AI research hubs via NCAIR.	Executive policy document; lacks statutory enforceability in court and binding force on state governments.
Electoral Act 2022	Regulates electoral administration;	Modernizes election management; provides	Statutory ambiguities regarding mandatory

	authorizes electronic accreditation (BVAS) and results transmission (IReV).	explicit legal recognition for electronic voter verification tools.	vs. discretionary electronic transmission created severe judicial uncertainty.
FOI Act 2011	Guarantees public right of access to government information and administrative records.	Enables civil society to demand disclosure of technology procurement contracts and public sector datasets.	Public agencies routinely resist FOI requests regarding proprietary software source code, citing commercial confidentiality exceptions.

HISTORICAL EVOLUTION AND PHASES OF PUBLIC SECTOR DIGITALISATION IN NIGERIA (1999–2026)

The evolution of digital and automated technology across the Nigerian public sector since the re-emergence of civilian democratic rule in May 1999 exhibits a distinct structural trajectory. Rather than representing a linear, planned progression toward artificial intelligence, technological integration in Nigerian governance has proceeded through four successive, overlapping historical phases. Each phase has been characterized by specific political imperatives, technological architectures, regulatory priorities, and structural limitations. Analyzing these developmental phases is essential because the data infrastructure, administrative habits, procurement patterns, and institutional resistance generated during earlier phases constitute the operational foundation upon which current AI-adjacent and automated public sector systems operate.

Phase 1: Foundational Infrastructure and Telecommunications Liberalisation (1999–2006)

The primary objective of the first phase was establishing basic telecommunications connectivity and formulating initial national information technology policies. When the civilian administration assumed office in 1999, the national telecommunications landscape was severely underdeveloped, managed by the state monopoly Nigerian Telecommunications Limited (NITEL), which provided fewer than 400,000 fixed landlines for a population exceeding 120 million. Key administrative and policy milestones of this phase included:

- The formulation and adoption of the **National Information Technology Policy (2001)**.
- The establishment of the **National Information Technology Development Agency (NITDA)** in 2001.
- The historical auction of Global System for Mobile Communications (GSM) spectrum licenses by the Nigerian Communications Commission (NCC) under the **Nigerian Communications Act 2003**.

The liberalisation of telecommunications catalyzed a dramatic expansion of mobile cellular connectivity, expanding telephone subscriber lines from under 500,000 in 2001 to over 30 million by 2006. Within the public service, early e-government initiatives were primarily limited to basic informational websites, static web portals, and preliminary computerisation of central administrative offices within federal ministries in Abuja.

However, back-office administrative workflows across federal, state, and local government bureaucracies remained almost entirely paper-based. Record-keeping was decentralized, highly vulnerable to loss or physical damage, and lacked standardized data

formats. Consequently, while Phase 1 successfully created the external telecommunications connectivity backbone, it generated virtually no structured, machine-readable digital data within state institutions.

Phase 2: Core Systems Building and Biometric Database Creation (2007–2014)

The second phase represented a strategic transition from static basic e-government toward constructing centralized administrative enterprise platforms and biometric identity registers across public finance, civil service personnel management, and electoral administration. Driven by the imperative to curb fiscal leakages and improve administrative visibility, the federal government initiated large-scale technology procurement projects:

1. Integrated Payroll and Personnel Information System (IPPIS)

Conceptualized to construct a verified central database of all federal public servants, IPPIS introduced mandatory biometric enrolment (fingerprints and facial capture) linked to direct bank payment channels. Its primary structural goal was eliminating "ghost workers"—non-existent or fraudulent identities listed on government payrolls by corrupt administrative handlers to siphon state funds.

2. Treasury Single Account (TSA) and GIFMIS

The government designed the TSA framework alongside the Government Integrated Financial Management Information System (GIFMIS) to consolidate thousands of fragmented commercial bank accounts operated by Ministries, Departments, and Agencies (MDAs) into a unified account structure at the Central Bank of Nigeria (CBN). This brought real-time visibility to public revenues and expenditure flows.

3. Biometric Verification and Identification Databases

The enactment of the **NIMC Act 2007** formally established the legal foundation for the National Identification Number (NIN). Concurrently, the Central Bank of Nigeria, in collaboration with the Bankers' Committee, launched the **Bank Verification Number (BVN)** system in 2014, creating a centralized biometric identity database for all commercial bank account holders.

4. Electoral Technology Innovations

Following the deeply flawed 2007 general elections, the Independent National Electoral Commission (INEC) executed a complete overhaul of the national voter register ahead of the 2011 elections. INEC deployed Direct Data Capture (DDC) machines to compile Africa’s largest biometric voter register, incorporating ten-fingerprint capture and digital photography to eliminate multiple registrations.

Phase 2 established the foundational digital registers and biometric datasets of the Nigerian state. However, these platforms functioned as isolated, departmental silos; cross-agency system interoperability remained non-existent, and data quality was frequently compromised by poor entry validation, duplicate records, and lack of continuous updates.

Phase 3: Executive Consolidation, Treasury Integration, and Enforcement (2015–2022)

The third phase was characterized by an aggressive executive push to enforce mandatory compliance with pre-existing digital platforms, scale centralized identity requirements, expand digital tax administration, and legally codify electoral technology.

1) **Mandatory Enrolment and Inter-Database Linkages**

Under federal executive directives, compliance with IPPIS was made strictly mandatory for all federal MDAs, military and paramilitary services, and tertiary institutions. Simultaneously, the federal government enforced the mandatory linkage of NINs to all

active telecommunications SIM cards, driving national NIN registrations from under 10 million in 2015 to over 95 million by late 2022.

2) **Automated Electoral Verification and Result Transmission**

INEC scaled electoral technology by introducing the **Smart Card Reader (SCR)** in the 2015 and 2019 general elections, culminating in the deployment of the **Bimodal Voter Accreditation System (BVAS)** and the **INEC Result Viewing (IReV)** portal for off-cycle elections and the 2023 general elections. BVAS combined fingerprint and facial biometric verification algorithms to authenticate voters at polling units, while IReV enabled the real-time upload of scanned polling unit result sheets (Form EC8A) directly to a public cloud portal.

3) **Institutionalization of Emerging Technology Policy**

The executive re-designation of the ministry as the Federal Ministry of Communications and Digital Economy led to the formulation of the **National Digital Economy Policy and Strategy (NDEPS 2020–2030)** and the establishment of the **National Centre for Artificial Intelligence and Robotics (NCAIR)** in 2020. This marked the formal transition from viewing IT merely as administrative office tooling to recognizing artificial intelligence, data analytics, and robotics as strategic drivers of national development.

Despite significant operational expansions, Phase 3 exposed major institutional and infrastructural friction. The rigid enforcement of IPPIS across federal universities triggered prolonged industrial action by the Academic Staff Union of Universities (ASUU). ASUU argued that the generic rule-based architecture of IPPIS was fundamentally incompatible with university autonomy, academic sabbaticals, and flexible research appointments—a textbook example of Heeks's design–reality gap.

Phase 4: Explicit AI Policy Formation, Data Governance, and Deep Tech (2023–2026)

The current phase marks the explicit prioritization of artificial intelligence as a distinct pillar of national public administration, supported by statutory data protection legislation and strategic talent initiatives.

Key features defining Phase 4 include:

- **Statutory Data Protection Architecture:** The enactment of the **Nigeria Data Protection Act (NDPA) 2023** established a statutory framework governing automated decision-making, profiling, data subject rights, and mandatory Data Protection Impact Assessments (DPIAs) for high-risk public sector AI systems.
- **National AI Co-Creation and Indigenous Strategy:** The Federal Ministry of Communications, Innovation and Digital Economy launched an ambitious national AI strategy process. A central objective is constructing an indigenous Large Language Model (LLM) trained on major Nigerian languages (Yoruba, Hausa, Igbo, Nigerian Pidgin) to ensure public sector AI applications do not embed linguistic or cultural biases inherent in Western datasets.
- **Talent Acceleration Programs:** The **3 Million Technical Talent (3MTT)** initiative was launched to systematically address acute civil service and industrial skill deficits by training technical talent across software engineering, data science, AI development, and cloud computing.
- **Sectoral AI Pilot Implementations:** Government agencies have initiated targeted AI pilots. The Federal Inland Revenue Service (FIRS) introduced automated machine-learning risk-scoring platforms to detect tax evasion and anomaly matching across bank transaction records. The Federal Ministry of Agriculture deployed satellite-based

machine learning tools for crop yield estimation and subsidy targeting. Simultaneously, state security agencies expanded computer-vision video surveillance systems across major urban centers.

Table 4: Comprehensive Historical Synthesis of Public Sector Digitalisation Phases in Nigeria (1999–2026)

Phase / Era	Key Policy & Legal Drivers	Core Technologies & Platforms Deployed	Primary Administrative Goals	Major Operational Constraints & Failure Points
Phase 1: Foundation (1999–2006)	National IT Policy 2001; NITDA Act 2007; Communications Act 2003.	GSM cellular networks; basic web portals; standalone desktop computerisation.	Establish telecommunications market; establish IT regulatory agency; build basic digital presence.	Complete absence of digital databases; paper-based workflows; erratic power; negligible digital skills in civil service.
Phase 2: Systems Building (2007–2014)	NIMC Act 2007; CBN BVN directives; Electoral Act amendments; Freedom of Information Act 2011.	IPPIS; TSA; GIFMIS; BVN; NIMC biometrics; Direct Data Capture (DDC) voter registers.	Eliminate ghost workers; centralize public treasury; create national biometric registers; curb payroll fraud.	Departmental database silos; poor data entry validation; user resistance; lack of cross-agency system interoperability.
Phase 3: Executive Enforcement (2015–2022)	NDEPS 2020–2030; Mandatory NIN-SIM linkage directives; NDPR 2019; Electoral Act 2022.	Enforced IPPIS; mandatory NIN-SIM database integration; Smart Card Readers; BVAS; IReV portal.	Executive enforcement of treasury control; automated electoral accreditation; centralized identity linkage.	Design–reality gaps (e.g., ASUU IPPIS dispute); network coverage failures; long queues and exclusion in NIN enrolment; political friction.
Phase 4: Explicit AI Policy (2023–2026)	NDPA 2023; National AI Strategy Framework; 3MTT Programme executive mandates.	Indigenous LLMs; FIRS ML tax auditing; satellite agro-analytics; urban computer-vision surveillance; NDPC privacy portal.	Strategic deployment of AI; building local computing/LLM capacity; statutory data privacy enforcement; technical talent acceleration.	Severe high-performance compute deficits; civil service skill gaps; opaque technology procurement; fragile public trust in automated state platforms.

CRITICAL IMPACT ANALYSIS OF AI AND DIGITAL SYSTEMS ON PUBLIC SERVICE DELIVERY IN NIGERIA

Evaluating the actual impact of AI and AI-adjacent automated technologies on Nigerian public service delivery requires moving beyond administrative declarations to conduct a critical empirical assessment grounded in the theoretical framework synthesized in Section 3. Drawing on the **Technology–Organisation–Environment (TOE)** framework, Heeks's **Design–Reality Gap** model, and the **Public Values Management (PVM)** paradigm, this section analyzes six crucial administrative impact dimensions.

Operational Efficiency versus Institutional Leakage

A primary normative argument for deploying automated platforms like IPPIS, TSA, and ML-based tax audit tools is their capacity to optimize operational efficiency, eliminate human discretion, and halt revenue leakage.

Empirical evidence demonstrates genuine, quantifiable gains in specific administrative metrics:

- **Payroll Fraud Suppression:** The federal government reported that integrating federal MDAs into the biometric IPPIS platform successfully detected and removed over 70,000 "ghost workers" from the federal payroll between 2010 and 2022, yielding billions of Naira in monthly personnel costs saved.
- **Treasury Visibility:** The consolidation of over 17,000 commercial bank accounts into the Central Bank via the Treasury Single Account (TSA) provided real-time visibility over federal cash reserves, eliminating commercial bank interest charges on government funds while curbing secret account operations by revenue-generating agencies.
- **Tax Audit Automation:** Machine learning algorithms deployed by the Federal Inland Revenue Service (FIRS) for cross-matching corporate bank transaction records against tax returns identified thousands of unregistered corporate taxpayers, expanding the formal tax base.

However, evaluated through the TOE framework and Heeks's Design–Reality Gap model, these operational efficiency gains remain partial, fragmented, and vulnerable to systemic circumvention.

First, technological automation at the central level has not eliminated underlying institutional corruption; instead, it has frequently exposed the limits of technology in weak institutional environments. As Obi (2022) observes, while IPPIS prevented lower-level civil servants from inserting ghost workers directly onto local payrolls, corrupt senior administrators devised workarounds, including:

- Inserting real biometric profiles of non-existent employees via corrupt system administrators.
- Demanding kickbacks from legitimate staff during manual data clearance procedures.
- Operating off-budget, unintegrated personnel recruitment schemes.

Second, severe technological context deficits—including unstable electricity supply, inadequate broadband connectivity in rural offices, and database downtime—frequently paralyze automated processing. When GIFMIS or IPPIS servers experience downtime or connectivity failure, processing civil service salaries, contractor payments, and operational funds is delayed for weeks.

Consequently, efficiency gains achieved at the macro-systemic level are neutralized at the micro-level by operational paralysis, creating severe hardship for front-line civil servants and service recipients.

Digital Identity Infrastructure, Equity, and Structural Exclusion

In a data-driven administration, a citizen's ability to access state services—such as obtaining a driver's license, registering a business, receiving social safety net transfers, or purchasing a mobile SIM card—is strictly conditioned on possessing a verified digital identity (NIN) linked to a biometric database.

While centralized identity registration under NIMC has scaled rapidly, evaluating its impact through the **Public Values Management (PVM)** framework reveals profound duty-oriented equity failures. The design of NIMC's biometric enrolment systems embeds implicit assumptions of an urbanized, connected, and literate population—a clear design–reality gap when deployed across rural Nigeria.

Primary structural mechanisms of exclusion include:

1. **Biometric Failure-to-Enrol (FTE):** Standard optical fingerprint scanners routinely fail to capture high-quality biometric templates from manual laborers, elderly citizens, and agricultural workers whose friction ridges are worn down by manual labor.
2. **Geographic and Infrastructural Exclusion:** Enrolment centers are heavily concentrated in urban centers and state capitals. Rural citizens in remote communities face substantial travel costs, long queues, and frequent server downtime at local enrolment centers.
3. **Extortion and Informal Gatekeeping:** Despite official policies declaring NIN registration free, severe hardware shortages and network delays enable local registration agents to demand illegal cash payments from poor applicants to expedite enrolment.

When statutory mandates make the presentation of a NIN strictly mandatory for accessing basic services, citizens who are structurally excluded from enrolment are effectively denied their fundamental constitutional rights. As Eubanks (2018) cautions, automated identity frameworks introduced into unequal societies can function as automated tools of social exclusion, punishing the poor for structural deficiencies beyond their control.

Algorithmic Bias, Cultural Misalignment, and "Colonial AI"

A critical issue in deploying artificial intelligence in the Global South is the reliance on imported software architectures, pre-trained machine learning models, and algorithmic designs originating in Western or Asian contexts. Scholars such as Birhane (2020) and Mohamed et al. (2020) conceptualize this phenomenon as **"Algorithmic Colonisation"** or **"Decolonial AI"** challenges.

In Nigeria—a multi-ethnic, multi-lingual state with over 250 distinct ethnic groups and complex informal socio-economic structures—importing off-the-shelf AI systems introduces severe representational and operational biases:

1. Facial Analysis and Biometric Errors

As demonstrated by Buolamwini and Gebru (2018), commercial computer vision and facial recognition algorithms display significantly higher error rates when processing individuals with darker skin tones, particularly dark-skinned women. When Nigerian law enforcement or border control agencies deploy imported computer vision tools for automated surveillance or identity verification, the probability of false positives, false arrests, and misidentifications is statistically magnified.

2. Linguistic and Cultural Exclusion in Natural Language Processing (NLP)

Citizen-facing conversational AI agents and automated government helplines configured primarily in standard global English fail to serve millions of Nigerian citizens who speak only local languages (such as Hausa, Igbo, Yoruba, Kanuri, Ibibio) or Nigerian Pidgin.

This linguistic mismatch prevents unlettered citizens from interacting with automated public portals, deepening the digital divide.

3. Misalignment with Informal Economic Realities

Machine learning risk-scoring algorithms designed in Western contexts evaluate creditworthiness, tax liability, and social welfare eligibility based on formal bank records, fixed residential addresses, and continuous digital transaction trails.

In Nigeria, where over 60% of economic activity occurs within the informal sector, applying rigid algorithmic credit or tax scoring models automatically classifies millions of legitimate informal traders and micro-entrepreneurs as "high-risk" or "fraudulent" simply because their economic activities do not generate conventional digital traces. These structural mismatches demonstrate that without local contextual adaptation, indigenous dataset training, and rigorous algorithmic bias audits, deploying AI in Nigerian public service delivery will exacerbate socio-economic inequalities.

Migration of Bureaucratic Discretion and Rent-Seeking

Proponents of administrative automation frequently assert that replacing human civil servants with automated algorithms eliminates corrupt discretion and petty bribery at service counters. However, analyzing technological deployment through Bullock's (2019) framework on administrative discretion and Heeks's Design–Reality Gap model reveals a more complex reality: **automation does not eliminate administrative discretion; it migrates discretion upstream.**

In the traditional Nigerian bureaucracy, discretion was exercised at the front desk by lower-level civil servants who could delay paper files, demand bribes for signatures, or alter manual records. With the introduction of centralized digital platforms like IPPIS, GIFMIS, and automated portal services, lower-level front-desk discretion has indeed been curtailed.

However, discretion and rent-seeking have migrated to three higher, less transparent administrative nodes:

1. **Technology Procurement and Vendor Capture:** The procurement of complex software, biometric hardware, and AI platforms has become a lucrative locus of high-level administrative rent-seeking. Bureaucrats and political actors collaborate with favored private IT vendors to inflate contract values, secure kickbacks, and construct proprietary software architectures that create long-term vendor lock-in.
2. **Database Administration and System Engineering:** Discretion now resides with system administrators, database engineers, and software vendors who control backend access. Civil servants seeking to bypass automated checks or resolve system flags pay bribes to database administrators to manually override algorithmic blocks, clear flags, or alter master database records.
3. **Algorithmic Parameter Configuration:** The power to set risk thresholds, audit parameters, and automated filtering criteria resides with elite technical committees and software designers. Because these parameter choices are executed behind closed doors and hidden within proprietary code, decisions regarding who gets audited or prioritized for public contracts become less visible and harder to challenge than traditional paper-based decisions.

Thus, technological automation in weak institutional environments transforms petty, visible front-desk bribery into sophisticated, opaque, tech-mediated rent extraction at the system level.

Data Governance, Privacy Safeguards, and State Surveillance

The deployment of AI systems in public administration requires aggregating massive volumes of personal, financial, biometric, and geospatial citizen data. Evaluated under the **Nigeria Data Protection Act (NDPA) 2023** and Bannister and Connolly's duty-oriented public values, Nigeria's existing public sector data governance practices reveal severe vulnerabilities.

First, despite the enactment of the NDPA 2023, inter-agency data sharing across the Nigerian public sector routinely occurs without explicit statutory authorization or mandatory **Data Protection Impact Assessments (DPIAs)**. For example, linking NIMC's biometric database with telecommunications SIM registries, commercial banking BVN networks, tax databases, and security agency monitoring frameworks was executed via executive directives with limited public consultation or independent privacy oversight.

Second, the centralisation of national biometric databases creates immense cybersecurity targets. Public sector databases—including NIMC, IPPIS, and tax portals—operate under persistent threats of data breaches, insider unauthorized access, and illicit data sales on black markets. Investigations by investigative journalists and privacy advocates have repeatedly revealed instances where unauthorized third-party commercial platforms obtained access to NIMC identity verification portals, selling citizens' NIN data online for negligible fees.

Third, expanding AI-driven computer-vision surveillance networks across major cities (such as Abuja and Lagos) under the guise of public safety raises deep constitutional concerns regarding state surveillance, political intimidation, and civil liberty erosion. Without independent judicial warrant frameworks, automated facial recognition systems deployed by state security agencies risk being weaponized against political dissidents, investigative journalists, and peaceful protesters.

Electoral Technology, Process Integrity, and Citizen Trust

The application of digital and automated technologies in electoral administration provides the ultimate empirical test of technology's capacity to build public trust and reinforce institutional legitimacy in Nigeria. As Aluaigba (2016) demonstrated, the credibility of an electoral system depends far less on the technological sophistication of the tools deployed than on the overall transparency, verifiability, and administrative integrity of the operating institution.

The introduction of the **Bimodal Voter Accreditation System (BVAS)** and the **INEC Result Viewing (IReV)** portal ahead of the 2023 general elections was hailed by civil society and international observers as a revolutionary step toward eliminating electoral fraud. The technological logic was sound: BVAS would prevent impersonation and multiple voting through real-time biometric authentication, while IReV would eliminate manual result manipulation by uploading scanned polling unit result sheets (Form EC8A) directly to a public cloud portal before manual collation could occur.

However, the operational execution during the February 2023 presidential election exposed a catastrophic design–reality gap:

- While BVAS performed relatively well for voter accreditation, the real-time upload of presidential election results to the IReV portal suffered severe delays and technical outages, whereas national assembly result uploads proceeded with fewer interruptions.
- INEC cited technical glitches, database management system (DBMS) errors, and cloud security throttling as reasons for the upload failures.

- Public perception was severely damaged. Opposition parties and citizens alleged that technical glitches were engineered to permit manual result collation manipulation at regional collation centers.

The electoral outcome reinforced a primary theoretical proposition of this paper: **technology cannot serve as a structural substitute for institutional integrity.** When technical failures occur within an environment characterized by low historical trust in state institutions, citizens do not attribute the failure to benign technical glitches. Instead, they interpret it as deliberate, technology-facilitated manipulation.

Rather than enhancing institutional legitimacy, the opaque deployment of technology during the 2023 elections deepened public cynicism, triggering prolonged judicial disputes and demonstrating that automated technology deployed without operational transparency destroys citizen trust.

ACTIONABLE RECOMMENDATIONS AND STRATEGIC IMPLEMENTATION ROADMAP

To transition Nigeria from passive, uncoordinated, and high-risk technology procurement toward responsible, accountable, and citizen-centered AI implementation in public service delivery, state actors must execute deliberate institutional, legal, and operational reforms. Grounded in the Technology–Organisation–Environment (TOE) framework, Heeks's Design–Reality Gap model, and Public Values Management (PVM), this section presents a comprehensive, structured roadmap across five key implementation pillars.

Pillar 1: Legal Oversight and Mandatory Algorithmic Accountability

1) **Enact Statutory Algorithmic Accountability Legislation:** The National Assembly should amend the NITDA Act 2007 or enact a dedicated **Public Sector Algorithmic Accountability Act**. This legislation must mandate that every federal and state MDA execute and publicly publish a comprehensive **Algorithmic Impact Assessment (AIA)** prior to deploying any automated decision-making tool, profiling software, or machine learning model that impacts citizen rights, benefit entitlements, tax obligations, or civil liberties.
2) **Empower the Nigeria Data Protection Commission (NDPC):** The NDPC must be granted full statutory independence, financial autonomy, and specialized technical capacity to strictly enforce the **Nigeria Data Protection Act (NDPA) 2023** across all sovereign state entities. The NDPC should establish a specialized **Algorithmic Audit Directorate** equipped to conduct independent source-code audits, training dataset review, and algorithmic bias testing on state AI platforms.
3) **Establish Legal Recourse and Algorithmic Due Process:** Statutory mechanisms must guarantee citizens explicit rights to:

- Receive a clear, human-understandable explanation of decisions generated by automated or AI-assisted public systems (the "right to explanation").
- Directly contest automated decisions before a designated human administrative review officer.
- Obtain rapid administrative and judicial redress when automated systems fail, err, or unlawfully deny entitlements.

Pillar 2: Interoperable Data Governance and Exclusion Mitigation

1) **Construct Open Data Architecture and Standards:** Under NITDA and NDPC leadership, the federal government must establish unified national data interoperability standards

(a **National Government Data Exchange Platform**) to eliminate departmental database silos across NIMC, FIRS, IPPIS, and line ministries while enforcing zero-trust encryption protocols.

2) **Eliminate Digital Identity Exclusion:** NIMC and partner registration agencies must eliminate structural barriers to National Identification Number (NIN) enrolment by:

- Deploying alternative, multimodal biometric capture systems (such as iris scanning and facial recognition) to accommodate manual laborers, farmers, and elderly citizens whose fingerprints are degraded.
- Expanding mobile enrolment units to hard-to-reach rural, riverine, and conflict-affected communities.
- Prohibiting the immediate denial of essential public services (such as healthcare, primary education, and basic banking) solely on the grounds of lacking a NIN, establishing transitional paper-based and assisted manual verification channels.

3) **Establish Localized Indigenous AI Datasets:** The Federal Ministry of Communications, Innovation and Digital Economy should accelerate the development of high-quality, ethically curated datasets representing all major Nigerian languages, dialects, and informal socio-economic activities. Training local Large Language Models (LLMs) on these indigenous datasets will prevent algorithmic bias and linguistic exclusion in public sector AI tools.

Pillar 3: Institutional Civil Service Capacity and Talent Development

1) **Establish Public Sector AI Leadership Cadres:** Every federal and state ministry should establish the statutory office of **Chief Data and AI Officer (CDAIO)**. CDAIOs must possess dual expertise in public administration and computational data science, serving as internal guardians of algorithmic ethics, system integrity, and data quality.

2) **Institutionalize Systemic AI Literacy:** The Public Service Institute of Nigeria (PSIN) and the Administrative Staff College of Nigeria (ASCON) must integrate mandatory modules on data literacy, algorithmic governance, digital ethics, and cybersecurity into civil service promotion examinations and executive leadership training.

3) **Absorb Technical Talent via 3MTT Pathways:** The federal government should construct formal civil service recruitment pathways for top graduates of the **3 Million Technical Talent (3MTT)** initiative, creating specialized, competitively compensated technical cadres within the civil service to reduce chronic dependence on expensive external contractors.

Pillar 4: Open Technology Procurement and Vendor Lock-In Prevention

1) **Implement Open Contracting and Source Code Audits:** The Bureau of Public Procurement (BPP), in collaboration with NITDA, should establish specialized procurement guidelines for government software and AI architecture. Technology procurement must mandate open-contracting standards, transparent bidding, published contract costs, and mandatory technical performance evaluations.

2) **Prevent Proprietary Vendor Lock-In:** Public sector IT contracts must explicitly reserve full intellectual property (IP) rights, source code access, master database ownership, and algorithmic transfer rights for the procuring government agency. Contracts that trap government institutions in proprietary vendor lock-in or grant private contractors exclusive control over citizen data must be legally prohibited.

3) **Institute Independent Technical Review Committees:** Prior to awarding major public technology contracts, procurement panels must submit software designs to independent technical review committees comprising local university researchers, civil society tech advocates, and software engineering professional bodies.

Pillar 5: Human-in-the-Loop Safeguards and Inclusive Multi-Channel Design

1) **Mandate Human-in-the-Loop (HITL) Architecture:** Fully automated decision-making must be strictly prohibited in high-stakes public service domains, including criminal justice, social welfare targeting, university admissions, and major civil service disciplinary proceedings. All public sector AI tools in these domains must operate strictly as **decision-support tools**, retaining human civil servants as final, legally responsible decision-makers.
2) **Maintain Assisted and Offline Service Channels:** To prevent the disenfranchisement of digitally illiterate, low-income, or rural citizens, public service delivery must adhere to a mandatory **multi-channel service design principle**. Physical service counters, paper-based application options, and community-assisted digital desks must be maintained alongside automated online portals.
3) **Execute Real-Time Process Transparency in Electoral Technology:** Building on lessons from the 2023 elections, electoral technology systems operated by INEC must embed complete operational transparency. System audit logs, cloud server uptime indicators, and automated error reports must be published in real-time to independent technical observers and political party representatives during live election cycles.

Table 5: Strategic Implementation Roadmap for Public Sector AI Adoption in Nigeria

Implementation Horizon	Primary Policy / Strategic Objective	Actionable Tasks & Key Deliverables	Primary Responsible Lead Agencies	Success Indicators
Short-Term (1–12 Months)	Regulatory Enforcement & Immediate Audit	• Conduct mandatory Data Protection Audits across NIMC, IPPIS, FIRS, and INEC. • Issue binding NDPC guidelines on public sector automated profiling. • Establish CDAIO offices across core federal ministries.	NDPC, NITDA, BPP, Federal Ministries	Published DPIAs; established CDAIO offices; zero unauthorized third-party NIN database access.
Medium-Term (13–36 Months)	Legislative Reform & Capacity Scaling	• Enact Public Sector Algorithmic Accountability Act. • Roll out localized indigenous LLM for public service chatbots. • Integrate 3MTT technical graduates into civil service software cadres. • Establish alternative biometric capture across NIMC centres.	National Assembly, FMONE, NIMC, PSIN, ASCON	Statutory AIA requirement; reduction in NIN biometric enrolment failure rates; operational local language AI portals.

Long-Term (37–60 Months)	Systemic Interoperability & Open Governance	• Deploy National Government Data Exchange Platform for zero-trust cross-MDA sharing. • Execute independent algorithmic bias audits across all operational AI tools. • Achieve full open-contracting compliance for state IT procurement.	NITDA, NDPC, BPP, State Executive Councils	Interoperable MDA data flows; zero proprietary vendor lock-in; high citizen trust metrics in digital services.

CONCLUSION AND FUTURE RESEARCH AGENDA

Concluding Synthesis

The adoption of artificial intelligence and automated digital technologies within the machinery of the state represents one of the most consequential administrative transformations in contemporary African governance. As Nigeria seeks to modernize its public bureaucracy, optimize tax revenue collection, eliminate payroll fraud, secure national identity, and strengthen democratic electoral administration, the strategic appeal of AI-driven public administration is undeniable.

However, as the theoretical and empirical analysis in this paper demonstrates, **technology is not a neutral, self-executing shortcut to institutional integrity.** Grounded in the Technology–Organisation–Environment (TOE) framework, Heeks's Design–Reality Gap model, and the Public Values Management (PVM) paradigm, this study establishes that the primary determinant of public service delivery quality in Nigeria is not the acquisition of advanced computational algorithms, but the institutional, legal, data governance, and ethical frameworks within which those technologies are deployed. Where public sector technology is introduced into weak institutional settings characterized by severe infrastructural deficits, administrative skill gaps, opaque procurement practices, and low public trust, high-tech tools do not eliminate bureaucratic dysfunction. Instead, they risk:

- Automating and accelerating existing administrative pathologies.
- Migrating corrupt discretion upstream to private software vendors and system administrators.
- Structurally excluding vulnerable citizens who lack digital identity documentation or connectivity.
- Eroding state legitimacy when opaque automated platforms fail during critical administrative processes.

Conversely, the minimal efficiency gains recorded across specific finance and identity systems prove that effective, responsible AI adoption in Nigeria is achievable. Realizing this potential requires moving beyond technological fetishism toward institutional consolidation. Nigeria must prioritize statutory algorithmic accountability, establish robust data privacy safeguards under the NDPA 2023, build technical capacity within the civil service, enforce open technology procurement, and maintain human-in-the-loop safeguards that defend citizen rights. Technology must serve as an instrument for deepening democratic public values, equity, and citizen trust, rather than an instrument of autocratic efficiency or opaque rent-seeking.

Future Research Agenda

To build upon the qualitative, policy-level analysis presented in this paper, public administration and digital governance scholars should pursue five primary empirical research avenues:

1. **Sectoral Micro-Empirical Field Surveys:** Scholars should conduct rigorous micro-level field evaluations—utilizing citizen surveys, user-experience testing, and semi-structured interviews with front-line civil servants—to measure the actual user-level impact of specific AI pilots in primary healthcare triage, agricultural subsidy targeting, and automated tax auditing across specific Nigerian states.
2. **Sub-National Comparative Analysis:** Future studies should execute comparative analyses contrasting highly digitalized state bureaucracies (such as Lagos or Kaduna) with financially constrained, rural state governments to evaluate how variations in sub-national technological, organizational, and environmental contexts condition AI adoption outcomes.
3. **Quantitative Algorithmic Auditing and Bias Testing:** Technical and legal researchers should collaborate to execute quantitative audits of computer vision, facial recognition, and automated risk-scoring models deployed by Nigerian security and revenue agencies to measure error rate disparities across dark skin tones, genders, and informal economic profiles.
4. **Political Economy of Technology Procurement:** In-depth political economy research is required to map the networks linking political actors, civil service elite procurement committees, and international private software vendors, documenting the dynamics of vendor lock-in, contract inflation, and technology-mediated rent extraction in West Africa.
5. **Longitudinal Citizen Trust Metrics:** Scholars should construct longitudinal survey frameworks measuring shifts in citizen trust, state legitimacy, and perceived administrative fairness following the introduction of automated and AI-assisted public service portals over successive electoral and administrative cycles.

References

- Aluaigba, M. T. (2016). Democracy deferred: The effects of electoral malpractice on Nigeria's path to democratic consolidation. *Journal of African Elections*, *15*(2), 136–158. https://doi.org/10.20940/JAE/2016/v15i2a7
- Bannister, F., & Connolly, R. (2014). ICT, public values and transformative government: A framework and programme for research. *Government Information Quarterly*, *31*(1), 119–128. https://doi.org/10.1016/j.giq.2013.06.002
- Birhane, A. (2020). Algorithmic colonization of Africa. *SCRIPTed: A Journal of Law, Technology and Society*, *17*(2), 389–409. https://doi.org/10.2966/script.170220.389
- Bullock, J. B. (2019). Artificial intelligence, discretion, and bureaucracy. *The American Review of Public Administration*, *49*(7), 751–761. https://doi.org/10.1177/0275074019856123
- Buolamwini, J., & Gebru, T. (2018). Gender shades: Intersectional accuracy disparities in commercial gender classification. *Proceedings of Machine Learning Research*, *81*, 1–15. http://proceedings.mlr.press/v81/buolamwini18a.html

- *Constitution of the Federal Republic of Nigeria 1999 (as amended)*. Federal Republic of Nigeria.
- *Cybercrimes (Prohibition, Prevention, etc.) Act 2015*. Federal Republic of Nigeria Official Gazette, No. 67, Vol. 102.
- Dunleavy, P., Margetts, H., Bastow, S., & Tinkler, J. (2006). New public management is dead—Long live digital-era governance. *Journal of Public Administration Research and Theory*, *16*(3), 467–494. https://doi.org/10.1093/jopart/mui057
- *Electoral Act 2022*. Federal Republic of Nigeria Official Gazette, No. 35, Vol. 109.
- Eubanks, V. (2018). *Automating inequality: How high-tech tools profile, police, and punish the poor*. St. Martin's Press.
- Federal Ministry of Communications and Digital Economy. (2020). *National digital economy policy and strategy (2020–2030)*. Federal Republic of Nigeria.
- Floridi, L., Cowls, J., Beltrametti, M., Chatila, R., Chazerand, P., Dignum, V., Luetge, C., Madelin, R., Pagallo, U., Rossi, F., Schafer, B., Valcke, P., & Vayena, E. (2018). AI4People—An ethical framework for a good AI society: Opportunities, risks, principles, and recommendations. *Minds and Machines*, *28*(4), 689–707. https://doi.org/10.1007/s11023-018-9482-5
- *Freedom of Information Act 2011*. Federal Republic of Nigeria Official Gazette, No. 58, Vol. 98.
- Heeks, R. (2002). Information systems and developing countries: Failure, success, and local improvisations. *The Information Society*, *18*(2), 101–112. https://doi.org/10.1080/01972240290075039
- Heeks, R. (2006). *Implementing and managing eGovernment: An international text*. Sage Publications.
- Jobin, A., Ienca, M., & Vayena, E. (2019). The global landscape of AI ethics guidelines. *Nature Machine Intelligence*, *1*(9), 389–399. https://doi.org/10.1038/s42256-019-0088-2
- Linz, J. J., & Stepan, A. (1996). *Problems of democratic transition and consolidation: Southern Europe, South America, and post-communist Europe*. Johns Hopkins University Press.
- Mergel, I., Edelmann, N., & Haug, N. (2019). Defining digital transformation: Results from expert interviews. *Government Information Quarterly*, *36*(4), Article 101385. https://doi.org/10.1016/j.giq.2019.06.002
- Mohamed, S., Png, M.-T., & Isaac, W. (2020). Decolonial AI: Decolonial theory as sociotechnical foresight in artificial intelligence. *Philosophy & Technology*, *33*(4), 659–684. https://doi.org/10.1007/s13347-020-00405-8
- *National Identity Management Commission Act 2007*. Federal Republic of Nigeria Official Gazette, No. 59, Vol. 94.
- *National Information Technology Development Agency Act 2007*. Federal Republic of Nigeria Official Gazette, No. 106, Vol. 94.

- *Nigeria Data Protection Act 2023*. Federal Republic of Nigeria Official Gazette, No. 102, Vol. 110.
- *Nigerian Communications Act 2003*. Federal Republic of Nigeria Official Gazette, No. 51, Vol. 90.
- Obi, C. (2022). Public sector reforms, administrative integrity, and technological automation in West Africa. *African Journal of Public Administration and Management*, *28*(1), 45–68.
- Obi, C. (2023). Regulatory fragmentation and data governance in Nigeria's digital economy. *Journal of Modern African Governance*, *41*(3), 201–224.
- Pasquale, F. (2015). *The black box society: The secret algorithms that control money and information*. Harvard University Press. https://doi.org/10.4159/harvard.9780674736061
- Rogers, E. M. (2003). *Diffusion of innovations* (5th ed.). The Free Press.
- Sun, T. Q., & Medaglia, R. (2019). Mapping the challenges of artificial intelligence in the public sector: Evidence from public healthcare. *Government Information Quarterly*, *36*(2), 368–383. https://doi.org/10.1016/j.giq.2018.09.008
- Tornatzky, L. G., & Fleischer, M. (1990). *The processes of technological innovation*. Lexington Books.
- Wirtz, B. W., Weyerer, J. C., & Geyer, C. (2019). Artificial intelligence and the public sector—Applications and challenges. *International Journal of Public Administration*, *42*(7), 596–615. https://doi.org/10.1080/01900692.2018.1498103
- Zuiderwijk, A., Chen, Y.-C., & Salem, F. (2021). Implications of the use of artificial intelligence in public governance: A systematic literature review and a research agenda. *Government Information Quarterly*, *38*(3), Article 101577. https://doi.org/10.1016/j.giq.2021.101577