Digital Sovereignty and the Politics of Data Control in Nigeria's Digital Economy

Ofon UWEM[1]
Department of Development Communication
Faculty of Communication and Media Studies
University of Uyo, Nigeria
uwemoffon1@gmail.com

Abasifreke IDIONG[2]
Department of Journalism
Faculty of Communication and Media Studies
University of Uyo, Nigeria
abasifrekeidiong@uniuyo.edu.ng

DOI: 10.61090/aksujomas.11602

ABSTRACT
The rapid growth of Nigeria's digital economy has intensified debates on digital sovereignty, particularly regarding the ownership, governance, and control of citizens' data within a digital ecosystem dominated by global technological platforms. As digital platforms increasingly shape economic transactions, communication, and information exchange, concerns have emerged regarding influence of foreign technological firms in the collection, processing, commodification and commercialisation of user data. Although regulatory frameworks, such as the Nigeria Data Protection Commission (NDPC) have been introduced to strengthen data governance and policy compliance, public awareness and understanding of these policies remain limited. This raises important questions about Nigeria's capacity to protect citizens' data rights and assert regulatory authority within the global digital environment. Guided by the political economy of communication, this study examines public perceptions of data ownership, awareness of data protection policies, and attitudes toward government regulation of digital platforms. The survey research design was adopted using a structured questionnaire administered to 400 digital media users across selected urban centers in Nigeria. Descriptive statistical analysis was used to assess patterns of awareness and perceptions of data governance. Findings indicate that while citizens acknowledge the importance of protecting national data resources, awareness of existing data protection frameworks remains relatively low. Mitigating this concern requires improved public awareness, accountability, capacity building and stronger regulatory paradigms.

Keywords: *Digital, sovereignty, economy, commodification, protection.*

1. INTRODUCTION

The rapid expansion of the digital economy has fundamentally transformed global socio-economic interactions, redefining how individuals, institutions, and governments communicate, transact, and access information. In Nigeria, this transformation has been particularly significant, driven by increased internet penetration, mobile connectivity, and the widespread adoption of digital platforms. These platforms now play a central role in financial services, commerce, governance, education, and social engagement, making data a critical

resource in the digital age. As digital interactions continue to grow, vast amounts of personal and institutional data are generated daily. This data has become a valuable economic asset, often described as the "new oil" of the digital economy. However, unlike traditional resources, data is largely intangible and can be collected, processed, and transferred across borders with minimal physical constraints. This has raised important concerns about ownership, control, and governance, particularly in countries like Nigeria where much of the digital infrastructure is operated by foreign technology companies.

Digital sovereignty has therefore emerged as a key issue in contemporary policy and academic discourse. It 'refers to the ability of a nation-state to control data generated within its territory and to regulate digital platforms operating within its jurisdiction. In Nigeria, the dominance of global technology firms in areas such as social media, cloud services, and digital advertising has intensified debates about the extent to which the country can assert control over its digital resources (Atairet & Ibnaga, 2021; Ibanga & Akpan, 2024). These firms often collect and process user data outside national borders, limiting the effectiveness of local regulatory frameworks. In response to these challenges, the Nigerian government has taken steps to strengthen data governance. One of the most notable initiatives is the introduction of the Nigeria Data Protection Regulation (NDPR) in 2019, which aims to safeguard personal data, ensure privacy, and promote accountability among data controllers and processors. More recently, the Nigeria Data Protection Act (NDPA) has further reinforced the legal framework for data protection. These policies are designed to align Nigeria with global standards such as the European Union's General Data Protection Regulation (GDPR).

Despite these regulatory efforts, significant gaps remain in public awareness and understanding of data protection policies. Many Nigerians are unaware of their rights regarding personal data or lack the knowledge needed to navigate digital platforms safely (Akpan & Uford, 2024). This lack of awareness undermines the effectiveness of existing regulations and limits citizens' ability to hold organizations accountable for data misuse. Furthermore, the political economy of communication provides a useful framework for understanding these dynamics. It highlights how power and control over communication systems are often concentrated in the hands of a few dominant actors, particularly multinational corporations. In the Nigerian context, this concentration of power raises concerns about digital dependency, economic exploitation, and the erosion of national sovereignty.

The intersection of global digital capitalism and local regulatory efforts creates a complex environment in which issues of data ownership, governance, and control are continuously negotiated. As Nigeria seeks to position itself within the global digital economy, it must address these challenges to ensure that its citizens' data is protected and that the benefits of digitalization are equitably distributed. This study therefore examines public perceptions of data ownership, awareness of data protection policies, and attitudes toward government regulation of digital platforms. By doing so, it contributes to ongoing debates about digital sovereignty and provides empirical evidence to inform policy and practice in Nigeria's digital economy.

Statement of the Problem

The increasing integration of digital technologies into everyday life in Nigeria has brought significant benefits, including improved access to information, financial inclusion, and economic opportunities. It has also raised critical concerns about the governance and control of personal data. A major issue is the dominance of foreign technology companies in Nigeria's digital ecosystem, which has led to questions about data ownership, privacy, and national security. Although regulatory frameworks such as the Nigeria Data Protection Regulation (NDPR) and the Nigeria Data Protection Act (NDPA) have been introduced to address these

concerns, their impact has been limited by low levels of public awareness and weak enforcement mechanisms. Many digital users are not fully informed about their data rights, nor do they understand how their data is collected, processed, and utilized by digital platforms. This lack of awareness reduces ability to make informed decisions and demand accountability from data handlers.

There is uncertainty regarding the Nigerian government's capacity to effectively regulate global technology companies whose operations often transcend national boundaries. This creates a gap between policy intentions and practical outcomes, undermining efforts to achieve digital sovereignty. Without adequate public awareness and strong institutional frameworks, the risk of data exploitation, privacy violations, and economic disadvantage remains high. The problem this study addresses is the disconnect between the growing importance of data protection in Nigeria's digital economy and the limited awareness, understanding, and trust among citizens regarding data governance and regulatory mechanisms.

Objectives of the Study

The main objective of this study is to examine digital sovereignty and the politics of data control in Nigeria's digital economy. The specific objectives are to:

1. Assess the level of public awareness of data protection policies in Nigeria.
2. Examine perceptions of data ownership among digital platform users.
3. Evaluate the extent to which users understand their data rights and privacy.
4. Analyze public attitudes toward government regulation of digital platforms.
5. Identify major concerns related to privacy, security, and foreign control of digital data.

Significance of the Study

This study is significant as it contributes to the growing discourse on digital sovereignty and data governance within Nigeria's expanding digital economy by providing empirical insights into public awareness, perceptions of data ownership, and attitudes toward regulation. As data increasingly functions as a strategic economic resource, understanding how citizens perceive its control and protection is essential for developing effective policies. The study offers valuable information for policymakers and regulatory bodies by identifying gaps in awareness of data protection frameworks such as the Nigeria Data Protection Regulation (NDPR), thereby informing the design of targeted public education and enforcement strategies. It also contributes to academic literature in communication and digital studies by situating Nigeria within broader global debates on digital capitalism and the political economy of data. Furthermore, the findings are relevant to digital platform users, as they highlight key concerns about privacy, data misuse, and foreign dominance in the digital space, thereby encouraging more informed engagement with digital technologies and strengthening advocacy for data rights and accountability.

2. LIERATURE REVIEW

Theoretical Framework

This study is anchored in the political economy of communication theory, which provides a critical framework for analyzing the relationship between power, ownership, and control in media and communication systems. The political economy of communication theory emerged from Marxist political economy in the 19th century but was formally developed within communication studies in the 1970s, particularly through the works of Dallas Smythe (1977) and Herbert Schiller (1976), and later systematized by Vincent Mosco (1996). The theory posits that communication structures are shaped by economic and political interests, often resulting in the concentration of power among dominant actors such as multinational corporations (Mosco, 2009; Fuchs, 2017). In the context of the digital economy, this perspective is

particularly relevant as global technology companies control major digital platforms and infrastructures, enabling them to collect, process, and monetize vast amounts of user data across national boundaries (Srnicek, 2017). This concentration of control raises concerns about digital dependency and the erosion of national sovereignty, especially in developing countries like Nigeria, where regulatory capacity may be limited. The concept of digital capitalism further reinforces this dynamic by highlighting how user data is commodified and integrated into profit-driven models of accumulation (Zuboff, 2019; Couldry & Mejias, 2019). Through this lens, digital sovereignty becomes a contested space where the state seeks to assert control over data flows while negotiating with powerful corporate entities. The theory also underscores the role of the state in implementing regulatory frameworks to protect citizens' data rights and ensure equitable participation in the digital economy. By applying the political economy of communication, this study examines how structural power relations influence public perceptions of data ownership, awareness of protection policies, and attitudes toward regulation in Nigeria's digital landscape.

Digital Sovereignty, Economics and the Politics of Data Control

The effectiveness of digital sovereignty is an indisputable factor in the space of digital governance, cyber security, technology autonomy, data protection and national control over digital infrastructure. According to Hummel, Braun, Tretter, and Dabrock (2021) data sovereignty, digital sovereignty and cyber sovereignty are used differently their systematic review of published literatures found considerable variation in how sovereignty is understood, particularly regarding the factors involved the value and context in which sovereignty is expressed or seek to protect. A central component of digital sovereignty is data control. The rapid growth of digital technology has contributed to the collection, storage, processing, dissemination or exchanging of personal, commercial and government-controlled information in lager quantity. Hummel et al (2021) affirmed that data sovereignty is the ability to retain control over the data by relevant actors while maintaining values such as privacy, autonomy, and security. This implies that data sovereignty is beyond ownership of data, it requires power control, access and decision on increasing movement of data across national bounderies. Therefore, controlling the path through which data moves becomes imperative, paramount and structural Chagnon, Thiry-Atighehchi, and Chalhoub, (2025) identified security, privacy, autonomy and control over data transmission as important consideration in achieving digital sovereignty. Implying path validation and internet routing are the technical dimension in addition to political and legal dimension of digital sovereignty.

Digital sovereignty requires formal regulatory authority and practical technology dependence. Jansen, Kadenko, Broeders, van Eeten, Borgolte, and Fiebig, T. (2023). Study revealed that digital sovereignty is beyond the adoption of digital policies. Depending on foreign infrastructures foreign owned software, cloud services or network providers is a serious performance concern in terms of data sovereignty irrespective of strong legislation for data protect and cyber security. In developing nations, the distinction between legal authority and technology reality is important in establishing digital sovereignty. This is because digital transformation involves technologies, infrastructure, software, services developed and controlled outside the country. Hummel et al (2021) suggested that digital sovereignty is beyond technology dependence to retain meaningful control over digital resources. Jansen et al (2023) maintained that technologically advanced government still depend on the infrastructure and services that extend beyond their nation's jurisdiction. From the foregoing digital sovereignty is a multidimensional concept involving control, autonomy, security and governance of digital resources and infrastructures. These studies suggest that digital sovereignty is not function of technological isolation. Rather, it involves the ability to govern

and manage critical digital dependencies while protecting data, upholding data security, privacy and institutional autonomy.

Digital economy denotes the economic activities that are increasingly enabled by digital technology, digital platforms, data and electronics networks. It encompasses online businesses and the transformation of traditional sectors such as banking, agriculture, manufacturing, education, healthcare, transportation and public administration through digital technologies. The Organisation for Economic Co-operation and Development (OECD, 2020) explains that digitalisation is transforming economic and social activities by changing how businesses produce goods and services, interact with consumers, and organise economic processes.

Similarly, the World Bank (2016) identifies digital technologies as an important driver of economic opportunity, innovation, access to information and service delivery. This is because digital technologies allow businesses to reach customers beyond geographical boundaries, reduce transaction costs and develop new products and services. According to the World Bank (2016), digital technologies can generate economic benefits by improving inclusion, efficiency and innovation. However, these benefits are not automatic. They depend on complementary factors such as effective institutions, digital skills, reliable infrastructure, competition and appropriate regulatory frameworks.

The International Labour Organization (ILO, 2021) maintained that digital labour platforms have created new opportunities for income generation and employment but have also raised concerns regarding working conditions, income security and social protection. This demonstrates that the economic impact of digitalisation is not limited to job creation. Policymakers must also consider the quality, security and sustainability of emerging forms of digital employment. The OECD (2020) observes that digital technologies can increase business productivity and facilitate innovation by allowing firms to reorganise production, improve communication and develop new business models. For small and medium-sized enterprises, however, the ability to benefit from digitalisation depends on access to affordable connectivity, finance, digital skills and appropriate technological resources. The relationship between the digital economy and inclusive economic growth is complex. Digital technologies can expand opportunities for people and businesses, but unequal access can also deepen existing socioeconomic inequalities.

The World Bank (2016) emphasises that digital technologies produce stronger development outcomes when supported by effective institutions, human capital and a favourable business environment. Cybersecurity, digital infrastructure, affordable connectivity, supportive institutions and digital skills are the actors that determine the promotion of innovation, entrepreneurship, employment, financial inclusion, productivity and market access. Digital revolution policies need to address the technological access and people's capacity to utilise technology productively. In a developing country like Nigeria, strengthening the foundations of digital economy is important in promoting digital transformation that contributes to economic based participation rather than creating new forms of exclusion.

In Nigeria, as the government, businesses and citizens keep depending on digital technology, the need for data utilization has become an important governance, administrative and economic resource, that has deepen the politics of data control and collection, processing, storage, utilization, sharing and protection of data seems to increase the battle on authority over data governance, accountability and digital transformation. According to Babalola (2022) the rapid expansion of technology into Nigeria’s economy and social activities created the need

for a more expansion of technology into Nigeria's digital ecosystem with a comprehensive for data protection and legal sovereignty. Before the enactment of the Nigeria Data Protection Act (NDPA) 2023, the Nigeria Data Protection Regulation (NDPR) 2019**,** established by the National Information Technology Development Agency (NITDA), attempted to institutionalise the legal framework for personal-data protection. Babalola (2022) describes the NDPR as Nigeria's first comprehensive, although subsidiary, data-protection legislation.

The enactment of the Nigeria Data Protection Act 2023 significantly changed this institutional landscape. The Act projected Nigeria Data Protection Commission (NDPC) as the principal institution responsible for overseeing data protection and privacy in Nigeria. According to the NDPC, the Act was signed into law on 12 June 2023 and seeks to safeguard data-privacy rights, regulate personal-data processing and strengthen the legal foundations of Nigeria's digital economy. Regulatory agencies are also involved in the politics of data control. The transition to the NDPC represents an institutional shift toward a dedicated data-protection authority. Babalola (2022) identified concerns surrounding the institutional and enforcement framework under the earlier NDPR regime, particularly because NITDA issued and administered the regulation within its broader technology-development mandate.

Data control also has implications for political and electoral governance. Electoral institutions possess large datasets containing citizens' personal information. In April 2026, the NDPC announced a joint working group with the Independent National Electoral Commission (INEC) to strengthen data protection within Nigeria's electoral system. The Commission stated that INEC holds personal data relating to approximately 94 million Nigerians and identified political parties, civil-society organisations, third parties and vendors as relevant actors in electoral data processing.

This development illustrates how data protection has become connected to electoral administration and political institutions. It also highlights the importance of clearly defining responsibilities among data controllers, processors, political organisations and technology vendors. This understanding establishes an important connection between data control and digital sovereignty. For Nigeria to remain relevant in the global digital economy, cross border data flow becomes imperative to the politics of data control. The aim is not to prevent data flow from Nigeria to other countries, but to international data flow are legal, secured, transparent, and subject to expert scrutiny mechanism.

3. METHODOLOGY

This study adopted a quantitative survey research design to systematically examine public perceptions of digital sovereignty and data control in Nigeria's digital economy. The survey approach was considered appropriate because it allows for the collection of standardised data from a relatively large number of respondents, enabling the researcher to identify patterns, trends, and relationships among variables such as awareness, perception, and attitudes. By using a structured questionnaire, the study ensured consistency in responses and minimized researcher bias during data analysis and discussion of findings.

The population of the study comprised all digital media users in Nigeria who engage with online platforms for communication, transactions, and information exchange. According to DataReportal (2026) Nigeria currently has about 143 million internet users. This includes individuals using social media platforms, smart devices penetration, online banking services, e-commerce websites, and other internet-enabled applications. The population is diverse, cutting across different age groups, educational levels, and occupational categories. Given the

widespread use of digital technologies in Nigeria, the population is considered large and heterogeneous, making it necessary to select a representative sample for the study.

The study was, however, conducted across selected urban centers in Nigeria, where digital platform usage is relatively high due to better access to internet services, mobile connectivity, and technological infrastructure. Urban areas were chosen because they host a large concentration of digital media users who actively engage in online activities such as social media interaction, digital banking, e-commerce, and content consumption. These locations provide a relevant context for examining issues of data ownership, awareness of data protection policies, and attitudes toward digital regulation. The urban focus also reflects the uneven distribution of digital access between urban and rural areas in Nigeria. From the population, a representative sample was drawn using the Taro Yamane's formula. Respondents were purposively selected, with data collected using a structured questionnaire administered through an online survey. Data collected were analyzed using descriptive statistical techniques, including frequencies, percentages, and mean scores.

4. DATA ANALYSIS AND INTERPRETATION

Table 1: Analysis of Demographic Data

Items	Category	Frequency	Percentage (%)
Sex	Female	242	69.50%
	Male	158	39.50%
	Total	**400**	**100%**
Age	18–24	142	35.50%
	25–34	103	25.80%
	35–44	88	22.00%
	45–54	55	13.80%
	55 and above	12	3.00%
	Total	**400**	**100%**
Education	Bachelor's Degree	184	46.00%
	Diploma	96	24.00%
	Secondary School	74	18.50%
	Postgraduate Degree	46	11.50%
	Total	**400**	**100%**
Occupation	Student	184	46.00%
	Self-employed	82	20.50%
	Private Employee	62	15.50%
	Public Employee	48	12.00%
	Unemployed	24	6.00%
	Total	**400**	**100%**

The findings on sex segregation in table one reveals that 69.50% of respondents were female this indicates that both male and female sex participated in the survey. Table two indicates the responses on age bracket, out of which respondent who are 18 – 24 years were

the majority this was followed by the ages of 25 – 34 who accounted 35.5% of the respondents. The table shows that the higher the age the lesser the engagement on internet. In terms of educational background of the respondents, the table above revealed that 46.0% of the respondents were gradutes with Bachelor's Degree, while respondents with Diploma Degree were 24.0% this implies that majority of respondents are literate. The occupational engagement of respondents revealed that students were the majority of respondents with a46.0% response rate followed by seflf employed who made 20.5% of respondents 12.0% of respondents were employed by private or public sector, while 6.0% of respondents were unemployed. This implied that majority of respondents were youths, educated and economically engaged. All the respondents were Nigerians who lived across the six geopolitical zones.

Table 2: Analysis of Awareness of data protection in Nigeria

Items	Category	Frequency	Percentage (%)
Awareness of data protection in Nigeria	Yes	208	52.0%
	No	192	48.0%
	Total	**400**	**100%**
Awareness of specific data protection regulation in Nigeria	NDPA	164	41.0%
	NDPR	84	21.0%
	Not Sure	152	38.0%
	Total	**400**	**100%**

Regarding awareness of data protection in Nigeria, the above table revealed that 52.0% 0f the respondents are aware while 48.0% are not aware of data protection in Nigeria. This indicates significant proportion in the population who lacks knowledge of data protection in Nigeria. To justify this finding the study revealed that 38.0% of respondents maintained that they are not aware of any data protection regulations in Nigeria, 48.0% indicated that they are aware of Nigeria Data Protection Act and 21.0% were aware of Nigeria Data Protection Regulation. This implies that majority of respondent are aware of the data protection regulations and acts in Nigeria but a significant level of the population are not aware of data protection.

Table 3: Analysis of Government Control on Nigerians' Data

Items	Category	Frequency	Percentage (%)
Perceived control over personal data	Technology Companies	188	47.00%
	Government	118	29.50%
	Individuals	58	14.50%
	Don't know	36	9.00%
	Total	**400**	**100%**
Perception that foreign technology companies have too much	Strongly agree	104	26.0%
	Agree	112	28.0%
	Neutral	82	20.5%
	Disagree	54	13.5%
	Strongly disagree	48	12.0%

control over Nigerians' data	**Total**	**400**	**100%**
Trust in Nigeria government to protect personal Data	Yes	120	30.0%
	No	188	47.0%
	Maybe	92	23.0%
	Total	**400**	**100%**

Table 3 revealed that 47.0% of respondents believed that technology companies have control over personal data as 29.5% of respondents indicated that government of Nigeria has control over data and 14.5 are of the opinion that an individual has control over personal data. In addition, 54.0% of respondent are of the opinion that foreign technology companies have too much control over Nigerians' data. 15.5% of respondents totally disagree while 20.5% were not sure about foreign control over their data. Further analysis revealed that 30.0% of Nigerians trust that Nigerian government can protect their data while 47.0% of the respondents do not trust Nigerian government to protect their data as 23.0% were totally uncertain

Table 4: Analysis of Support for Data Localisation Policy in Nigeria

Items	Category	Frequency	Percentage (%)
Support for Data Localisation Policy in Nigeria	Yes	232	58.00%
	No	92	23.00%
	Maybe	76	19.00%
	Total	**400**	**100%**
Concern about personal data online	Data breaches	248	62.0%
	Unauthorised sharing	224	56.0%
	Identity theft	196	49.0%
	Commercial exploitation	182	45.5%
	Surveillance	158	39.5%
	Data breaches	248	I 62.0%
Stronger data protection laws will improve Nigeria's digital economy	Yes	184	46.00%
	May be	128	32.00%
	No	88	22.00%
	Total	**400**	**100%**

The above findings show that 58.0% of respondents are in support of policies that will ensure all data generated in Nigeria are stored in Nigeria. This idea was opposed by 23.0% respondents who indicated that they do not support localisatio and 19.0% of respondent where indecisive. Further analysis revealed a significant increase in concern about online data, 62.0% of respondents indicated that it might result in data breach, unauthorised sharing of online data was indicated by 56.0% of respondent. Strong anxiety about identity theft was expressed by 49.0% 0f respondents, followed by commercial exploitation and surveillance as indicated by 45.5% and 39.5% respectively. Regarding the perception on whether stronger data protection laws will improve Nigeria's digital economy 46.0% of respondents supported the view, 32.0% were not, and 22.0% opposed the view. The increasing positive perception is an indication that data governance influences digital economic development of Nigeria.

Table 5: Analysis of government's top priority on data protection and digital economy

Priority Area	Frequency	Percentage (%)
Monitoring tech companies	150	37.50%
Strengthening laws	140	35.00%
Encouraging local tech development	80	20.00%
Public awareness	30	7.50%
Total	**400**	**100%**

The analysis on government's top priorities concerning data protection and digital economy revealed that regulatory control and developmental initiatives can improve digital sovereignty and Nigeria's digital economy. This was significant among 37.5% of respondents who indicated that government should prioritise monitoring of tech companies, followed by 35.0% who upheld that laws should be strengthened, while 20.0% of respondent indicated that encouraging local tech development should be a priority and 7.5% emphasized public awareness should prioriise to promote data protection and Nigeria's digital economy.

Discussion of Findings

The findings of this study are thematically discussed in line with the objectives of the study. On the subject of user awareness of data protection policies in Nigeria, for instance, findings revealed that majority of Nigerian internet users were not aware of any such policy in place, indicating a widening chasm in digital literacy among the Nigeria populace. The fact that the Nigerian Data Protection Act (NDPA) in its new form has been in existence since June 2023, when it was signed into law, yet a significant percentage of the population is still to come to its knowledge brings into focus arguments as to whether there have been deliberate efforts on the part of relevant government agencies to educate the public on the propriety of such a critical legislation, especially given its legal framework for the protection of personal information – or it is politics as usual.

This finding, situated within the broader context of Nigeria's rapidly expanding digital economy, where data has become a critical economic resource, supports the earlier findings by Ugbedeojo (2025) who reported limited education and widespread lack of awareness, and the PDPPA (2026) whose study indicated that "less than 20% of Nigerians are aware of our data protection law", further blaming the low rating on low public literacy. As established in this study, there is no gainsaying the fact that increased internet penetration, mobile connectivity, and widespread digital platform usage have transformed socio-economic interactions in Nigeria. However, public awareness of critical data protection provisions remains low, with many unsure or unaware of these frameworks. This supports earlier research findings in developing countries which show that data protection laws often exist without sufficient public understanding or civic education (Duncan, 2020; Greenleaf, 2021). The implication is that regulatory effectiveness is weakened when citizens lack awareness of their rights, thereby limiting accountability mechanisms in digital governance.

This raises concerns about public perception of data ownership and control, especially given the dominance of foreign technology companies. Empirically, the study found that most respondents perceive technology companies as having the greatest control over personal data,

while very few believe individuals retain control. This supports the theoretical argument of the political economy of communication, which posits that digital infrastructures are dominated by powerful corporate actors who shape data flows and access (Mosco, 2009; Fuchs, 2017).

The finding that respondents overwhelmingly believe foreign technology companies have excessive control over Nigerian internet users' data is instructive, as it aligns with the concept of digital capitalism, which describes how global platforms commodify user data for economic gain (Zuboff, 2019; Couldry & Mejias, 2019). The empirical evidence suggests that Nigerians are increasingly aware of this imbalance, reflecting concerns about digital sovereignty as outlined in the theoretical framework. The perception that data is largely controlled externally indicates a growing recognition of Nigeria's dependency on foreign digital infrastructures, which limits national control over data governance.

The significant lack of trust in the Nigerian government's ability to protect personal data in the findings connects directly to thrust of this paper and contemporary data policy scholarship globally, which have highlights variously highlighted the weak enforcement of data protection regulations by agencies such as the NDPR and NDPA. Despite these legal frameworks in place, respondents expressed skepticism about government's effectiveness in regulating data practices. This suggests a gap between policy formulation and implementation, reinforcing the problem of weak institutional capacity and limited public confidence in regulatory bodies. From a political economy perspective, this reflects the uneven distribution of power between the state, corporations, and citizens in the digital ecosystem.

Concerns about privacy, data breaches, identity theft, unauthorized data sharing, and surveillance reflect lived experiences and perceived risks associated with digital platforms. This aligns with global empirical studies which show that users in emerging digital economies are increasingly vulnerable to cybercrime and data exploitation due to weak enforcement systems (Kshetri, 2017). The prominence of these concerns in the Nigerian context highlights the urgency of strengthening cyber security infrastructure and improving regulatory oversight. It is thought that greater media literacy, data localization policies and stronger data protection laws would improve Nigeria's digital economy. This reflects a desire for greater national control over data, consistent with the tenets of digital sovereignty outlined in the political economy of communication. Empirical dynamics of data economics and technological development in countries such as India and Brazil have shown shown that data localization policies are often supported as mechanisms for enhancing national security and digital independence (Belli, 2018; Aaronson, 2020).

5. Concluding remarks

Conclusion

The findings of this study reveal a clear perception among respondents that control over personal data in Nigeria is largely dominated by technology companies, with comparatively limited confidence in individuals and government institutions. There is also a strong sense of concern regarding data protection, as issues such as data breaches, identity theft, unauthorized sharing, surveillance, and commercial exploitation consistently emerged as major fears. Trust in the Nigerian government to adequately protect citizens' data appears low, with many respondents' expressing uncertainty or outright distrust, which reflects broader concerns about institutional capacity and enforcement effectiveness within the country's digital governance framework.

At the same time, the study shows strong public support for regulatory reforms, particularly policies that strengthen data protection laws and require data generated within

Nigeria to be stored locally. This indicates an awareness of the importance of digital sovereignty and a desire for greater national control over data governance. Respondents also emphasized the need for improved cybersecurity systems, increased public awareness, professional capacity building, and stricter enforcement mechanisms. Overall, the evidence suggests that while Nigerians are highly aware of the risks associated with digital data, there remains a significant gap between policy existence and effective implementation, highlighting the need for stronger institutional frameworks and sustained public engagement to build trust and improve data governance outcomes in the country.

Recommendations

1. The Nigerian government should strengthen the implementation of data protection laws (NDPA/NDPR) through consistent monitoring, penalties, and compliance checks for both local and foreign tech companies.
2. Increase nationwide public awareness on data rights and digital safety using schools, media campaigns, and community-based sensitization programs.
3. Government, academic institutions and the private sectors should invest in local digital infrastructure**,** including secure national data centers to reduce dependence on foreign technology companies and improve data sovereignty.
4. Nigerian government should develop cybersecurity capacity by training and certifying more professionals in data protection, cybersecurity, and digital risk management.
5. Regulatory institutions should improve regulatory oversight of technology companies through stronger institutional coordination, routine audits, and transparent monitoring' systems.
6. The government, in collaboration with academic institutions and the private sector should encourage local tech innovation and development to strengthen Nigeria's self-reliance in managing and securing digital data.

REFERENCES

Adeyemi, A. (2021). Data governance and digital economy in Nigeria. *Journal of African Media Studies*, 13 (2), 145–160. https://doi.org/10.1386/jams_00047_1.

African Union. (2020). *Digital transformation strategy for Africa (2020–2030).* Addis Ababa: African Union Commission. https://au.int/en/documents/20200518/digital-transformation-strategy-africa-2020-2030.

Akpan, S. J., & Uford, I. C. (2024). Effect of fuel subsidy removal on purchase of consumer goods in Nigeria: A literature review. *International Journal of Economics, Business and Social Science Research*, *2*(4), 30-38.

Atairet, A. C., & Ibanga, S. E. (2021). Nigerian Legislature and Administration of Constituency Projects in Nigeria:(2015–2020). *KIU Interdisciplinary Journal of Humanities and Social Sciences*, *2*(1), 165-180.

Babalola, O. (2022). Nigeria's data protection legal and institutional model: An overview. *International Data Privacy Law, 12*(1), 44–52. https://doi.org/10.1093/idpl/ipab023.

Benkler, Y. (2006). *The wealth of networks: How social production transforms markets and freedom.* Yale University Press. https://yalebooks.yale.edu/book/9780300125771/the-wealth-of-networks/

Castells, M. (2010). *The rise of the network society* (2nd ed.). Wiley-Blackwell. https://www.wiley.com/en-us/The+Rise+of+the+Network+Society%2C+2nd+Edition-p-9781405196864

Chagnon, D., Thiry-Atighehchi, K., & Chalhoub, G. (2025). A survey on path validation: Towards digital sovereignty. *Computer Networks, 256*, 110905. https://doi.org/10.1016/j.comnet.2024.110905

Couldry, N., & Mejias, U. A. (2019). *The costs of connection: How data is colonizing human life and appropriating it for capitalism*. Stanford University Press. https://doi.org/10.1515/9781503609754

Couldry, N., & Mejias, U. A. (2019). The costs of connection: How data is colonizing human life and appropriating it for capitalism. Stanford University Press. https://doi.org/10.1515/9781503609754

DataReportal (2026). *Global digital insights.* Global Review Report.

Fuchs, C. (2017). *Social media: A critical introduction* (2nd ed.). Sage Publications. https://uk.sagepub.com/en-gb/afr/social-media/book244189

Fuchs, C. (2017). Social media: A critical introduction (2nd ed.). Sage Publications. https://uk.sagepub.com/en-gb/afr/social-media/book244189.

Hummel, P., Braun, M., Tretter, M., & Dabrock, P. (2021). Data sovereignty: A review. *Big Data & Society, 8*(1), 1–17. https://doi.org/10.1177/2053951720982012

Ibanga, S., & Akpan, A. (2024). Road infrastructure and socio-economic development in Akwa Ibom State, Nigeria. *ADUN Journal of Arts, Management and Social Sciences*, *1*(2), 351-367.

International Labour Organization. (2021). *World employment and social outlook 2021: The role of digital labour platforms in transforming the world of work*. International Labour Office.

Jansen, B., Kadenko, N., Broeders, D., van Eeten, M., Borgolte, K., & Fiebig, T. (2023). Pushing boundaries: An empirical view on the digital sovereignty of six governments in the midst of geopolitical tensions. *Government Information Quarterly, 40*(4), 101862. https://doi.org/10.1016/j.giq.2023.101862

Kwet, M. (2019). Digital colonialism: US empire and the new imperialism in the Global South. *Race & Class,* 60 (4), 3–26. https://doi.org/10.1177/0306396818823172

Mosco, V. (1996*). The political economy of communication*. Sage Publications. https://uk.sagepub.com/en-gb/afr/the-political-economy-of-communication/book204784

Mosco, V. (2009). *The political economy of communication* (2nd ed.). Sage Publications. https://uk.sagepub.com/en-gb/afr/the-political-economy-of-communication/book233446

National Information Technology Development Agency. (2020). *Guidelines for the management of personal data by public institutions in Nigeria*. NITDA Public Institution Data Guidelines

Nigerian Communications Commission. (2020). *Nigeria Data Protection Regulation (NDPR).* Abuja: NCC. https://nitda.gov.ng/wp-content/uploads/2020/01/Nigeria-Data-Protection-Regulation.pdf

Nigerian Data Protection Bureau. (2023). *Nigeria Data Protection Act (NDPA).* Abuja: NDPB. https://ndpb.gov.ng/Files/Nigeria_Data_Protection_Act_2023.pdf

Nigeria Data Protection Commission. (2023). *Nigeria Data Protection Act, 2023*. Nigeria Data Protection Act 2023 – NDPC

Nigeria Data Protection Commission. (2024). *Nigeria Data Protection Commission annual report 2023*. NDPC Annual Report 2023

Nissenbaum, H. (2010). *Privacy in context: Technology, policy, and the integrity of social life.* Stanford University Press. https://www.sup.org/books/title/?id=8868

OECD. (2019). *Enhancing access to and sharing of data: Reconciling risks and benefits for data reuse across societies*. Paris: OECD Publishing. https://doi.org/10.1787/276aaca8-en

Ojebode, A. (2019). Political economy of communication in Africa. *African Communication Research,* 12 (1), 23–40. https://www.africancommunicationresearch.org

Organisation for Economic Co-operation and Development. (2020). *OECD digital economy outlook 2020*. OECD Publishing. https://doi.org/10.1787/bb167041-en

PDPA (2026). *Less than 20% of Nigerians know their data protection law.* LinkedIn.

Schiller, H. I. (1976). *Communication and cultural domination.* M.E. Sharpe. https://archive.org/details/communicationcul00schi

Smythe, D. W. (1977). Communications: Blindspot of western marxism. *Canadian Journal of Political* and Social Theory, 1(3), 1–27. https://journals.sfu.ca/cjps/index.php/cjps/article/view/36

Srnicek, N. (2017). *Platform capitalism*. Polity Press. https://politybooks.com/bookdetail/?isbn=9781509504862

Srnicek, N. (2017). *Platform capitalism.* Polity Press. https://politybooks.com/bookdetail/?isbn=9781509504862

Ugbedeojo, S.V. (2025). Data protection and compliance in Nigeria: Challenges and opportunities. SSRN.

UNCTAD. (2021). *Digital economy report 2021: Cross-border data flows and development*. United Nations. https://unctad.org/system/files/official-document/der2021_en.pdf

World Bank. (2021). *Digital economy for Africa initiative*. Washington, DC: World Bank. https://www.worldbank.org/en/programs/all-africa-digital-transformation

World Bank. (2016). *World development report 2016: Digital dividends*. World Bank. https://doi.org/10.1596/978-1-4648-0671-1

World Bank. (2022). *The Global Findex Database 2021: Financial inclusion, digital payments, and resilience in the age of COVID-19*. World Bank. https://doi.org/10.1596/978-1-4648-1897-4

Zuboff, S. (2019). *The age of surveillance capitalism*. Public Affairs. https://www.publicaffairsbooks.com/titles/shoshana-zuboff/the-age-of-surveillance-capitalism/9781610395694/

Zuboff, S. (2019). *The age of surveillance capitalism. Public Affairs.* ttps://www.publicaffairsbooks.com/titles/shoshana-zuboff/the-age-of-surveillance-capitalism/9781610395694/