ISSN 2747-2671 (online)

PINISI
JOURNAL OF ART, HUMANITY & SOCIAL STUDIES
Vol. 3 No. 6, 2023

Data in Motion: Cross Border Data Transfer and Cloud Data Security

Stephen Adi Odey
Department of Sociology, University of Calabar, Cross River State, Nigeria.
*Penulis Koresponden: adiodey@unical.edu.ng

ABSTRACT

Industry 4.0, otherwise known as the 4th Industrial Revolution, is gradually taking shape in the affairs of man globally. Therefore, the issue of data privacy and protection has garnered attention. The development of cloud-based technologies and the globalisation of data storage have become very vital for studies. It is expedient that tech entrepreneurs and global users alike appreciate the provisions of the law vis-à-vis cross-border data transfer and cloud data security. Laws are not deadwoods never to rise again; rather, laws have lives, and this informs the ever-dynamic nature of law to fit in with the chages of society. After all, society cannot move on while we remain still. There have been changes in several data protection laws across the world, and it is well settled that ignorance of the law is not an excuse. It is important that tech entrepreneurs and users gain a fair knowledge of the subject matter in order to prevent them from managing and transferring data contrary to the law. Therefore, this article shall begin by exposing the importance of cross-border data transfer and cloud data security in light of their significance in the 21st century. The meaning of data and the general regulatory framework of data in Nigeria shall also be examined, as shall the significance of cross-border data transfer considering socio-economic relations and advancements in the world. Cross-border data transfer under the 2019 and 2023 Nigeria Data Protection Act shall also be examined. At the end, in light of the new Act, it would be submitted that the transition of authority to the Commission for issuing adequacy decisions signifies a centralised and expert-driven approach to safeguarding personal data during cross-border transfers.

Keywords: Data Privacy; Data protection; Cross border transfer; cloud computing; Regulatory framework; Personal data.

1. INTRODUCTION

The 21st century, often referred to as the "information age," has revolutionised the quick and effortless distribution of personal information or data, thanks to its most significant creation—the internet (Kline¸ 2015). As new technologies continue to emerge, safeguarding one's privacy is increasingly crucial. The rise of information technology has established an environment where personal and organizational data can be readily obtained by unauthorized individuals if proper safeguards are not put in proper perspective. Moreover, the undeniable reality that people's lives are now intertwined with constant information exchange and data flow signifies that data protection is growing in significance and occupying a central position within political and institutional frameworks. This has brought about the enactment of data privacy and protection laws across different countries around the world. The protection of personal data has increasingly been seen as a fundamental aspect of the right to privacy, also known as 'the right to be left alone'. As early as 1988, the UN Human Rights Committee, the treaty body charged with monitoring the implementation of the International Covenant on Political and Civil Rights (ICCPR), recognized the need for data protection laws to safeguard the fundamental right to privacy recognized by Article 17 of the ICCPR (Alston & Crawford, 2000).

Cross-border data flows have also now become an integral component of international trade, revolutionising the global commerce landscape. Data has assumed an unprecedented role as a crucial input in trade, not only within the realms of the information technology sector but also in traditional industries. This transformative shift has necessitated a substantial expansion in global internet bandwidth, signalling an expanding reliance on data-driven trade practices.

The escalation in global internet bandwidth is staggering, exemplifying the rapid evolution of data usage. In a span of merely two decades, global internet bandwidth escalated from a modest 56 Gbps in 1999 to an impressive 393 Tbps in 2018, indicating an astounding compound annual growth rate (CAGR) of 59.1 percent. This growth trajectory underscores the urgency with which industries are adapting to the data-intensive trade environment. Notably, Africa experienced an extraordinary surge in international internet bandwidth between 2014 and 2018, with a compounded annual growth rate of 45 percent (Orji, 2018). A parallel trend was observed in India, which witnessed a substantial increase of 62.7 percent per year in its international internet bandwidth during the same period.

However, this rapid expansion in data flows, while catalysing growth and socio-economic transformation, has introduced a host of intricate policy challenges. The multifaceted nature of these challenges encompasses domains such as anti-trust practices, inequality, privacy concerns, data security, and surveillance. The onus lies on private businesses to ensure the security and integrity of the personal data they amass and exploit for their commercial endeavors. These businesses' capability, ethical stance, and commitment to safeguarding user data have become central points of debate. Furthermore, governmental policy decisions have triggered contentious discussions, particularly in the context of data sovereignty and citizens' privacy.

The surge in cross-border data flows has undeniably reshaped the landscape of international trade, propelling economies into a new era of data-driven commerce. However, this transformation comes with a set of intricate challenges that span privacy, security, policy-making, and regulatory frameworks. Striking a harmonious balance between data-driven innovation and the preservation of individual rights and national interests remains a critical endeavour in navigating the evolving nexus of cross-border data flows and international trade.

On June 12, 2023, President Bola Ahmed Tinubu signed the Nigerian Data Protection Act (NDPA) into law, signifying a momentous achievement in the nation's journey to harmonise technological advancement and the safeguarding of individuals' privacy rights (Tom¸ et al., 2023). The NDPA introduces a comprehensive framework that delineates the duties and responsibilities of entities in managing personal data with transparency, security, and adherence to lawful protocols. A particular domain of substantial significance for Nigerian tech entrepreneurs revolves around the clause concerning the transfer of data across borders and the security of cloud-based data. Given the prevalent dependence of local tech enterprises on foreign cloud technologies and the storage of data through service providers situated beyond the confines of Africa, it becomes crucial to discern the implications of the NDPA on these practices.

Nigeria, as a prominent player in the digital economy, faces the challenges and opportunities associated with the cross-border transfer of personal data. With a growing number of businesses and individuals engaging in international data flow, it has become imperative to examine the legal and regulatory framework governing this practice. This article provides an overview of the cross-border transfer of personal data in Nigeria, aiming to highlight key considerations, regulatory mechanisms, and emerging trends in this domain. The author delves into the fundamental components of the Act that pertain to these spheres, taking into account the challenges confronted by domestic tech companies that engage with overseas cloud technologies and entrust their data to service providers located outside the African region.

2. THE MEANING OF PERSONAL DATA

Personal data is the new oil of the internet and the new currency of the digital world'. From the definition, we can deduce how important 'personal data' is in data privacy and processing, which should be carefully planned, managed, and regulated by trained experts.

Under GDPR Article 4(1), which provides a definition of personal data, this is stated below: Personal data' means any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier, or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural, or social identity of that natural person (Finck & Pallas, 2020). It is evidently clear that personal data implies all possible information that relates to natural persons who can be identified. The overriding scope of personal data also extends to 'public and non-sensitive information as well as pseudonymous identifiers; others include 'tracking cookies', IP addresses, and similar data.

The GDPR's definition of 'personal data' pertains to 'online identifiers' and 'location data' as examples of identifiers. 'Personal data is broad, flexible, and adaptable to technological contexts.' It is against this backdrop that the right to personal data protection is a fundamental provision guaranteed by Article 8 of the EU Charter (Charter of Fundamental Rights of the European Union).

There is a clear uncertainty created because the nature of this right is 'non-absolute'. Indeed, the uncertainty of personal data is an imperative concept and principle of data protection. By virtue of Article 2(1), the GDPR "applies to the processing of personal data wholly or partly by automated means and to the processing other than by automated means of personal data that forms part of a filing system or is intended to form part of a filing system" (Bulgakova & Bulgakova, 2016, p. 113).

3. GENERAL REGULATORY FRAMEWORK OF DATA IN NIGERIA

Several laws in Nigeria contain ancillary provisions seeking to protect data privacy. The most comprehensive instrument is the subsidiary legislation mandated in pursuance of the National Information Technology Development Agency Act, 2007 (NITDA Act'). The Act empowers the agency to, amongst others, develop guidelines and regulations for electronic governance and the activities of data in both the private and public sectors (Babalola, 2022).

Pursuant to the above, the agency developed and issued the 2013 Guidelines for Data Protection. Subsequently, the Nigeria Data Protection Regulation 2019 ('NITDA Regulation') was made to regulate data in Nigeria. The Regulation is unique for its specificity and focus on data protection, as opposed to other legislation that just makes data protection ancillary. It should be noted that NITDA is the apex regulator for data privacy and protection in Nigeria; however, this is without prejudice to other regulators listed in specific legislation providing for the same protection. The following are relevant laws impacting data protection and data privacy in Nigeria:

3.1 NITDA REGULATION

The NITDA Act empowers the agency to issue guidelines for electronic administration and navigation. The regulation is made pursuant to these powers. The regulation is appraised for its specificity and directions (Oni, et al., 2016).

3.2 THE 1999 CONSTITUTION OF THE FEDERAL REPUBLIC OF NIGERIA AS ALTERED

It is said that the Constitution is the find *et origo* of all laws in any country undergoing constitutionality; all laws must bow and take their breath therefrom. Therefore, Nigeria's data privacy and protection regime can be gleaned from the right to privacy guaranteed under Section 37 of the Constitution (Elgujja¸2020). The section protects the rights of citizens to their privacy and the privacy of their homes, correspondence, telephone conversations, and telegraphic communication. Thus, there is an extension of the constitutionally guaranteed right to privacy.

3.3 FREEDOM OF INFORMATION ACT 2011 (FOIA)

The purpose of the Act is to make records and information held by government agencies more freely accessible to the public. Happily, and important to this paper, it makes provisions for exceptions. One such exception is with respect to personal records, information, and matters related thereto (Martins¸et al., 2020). Section 14 provides for the limitation of government agencies from disclosing the personal information of citizens unless the individual's consent is obtained or the information is publicly available.

3.4 CYBERCRIMES (PROHIBITION, PREVENTION, etc.) ACT 2015 (CPPA)

The CPPA is established for the prohibition, prevention, detection, prosecution, and punishment of cybercrimes in Nigeria. The Act imposes obligations on mobile networks, computers, and communications service providers to store and retain subscriber information for a period of two years. Services providers are expected to accord premium to an individual's right to privacy as enshrined in the Constitution and to take steps towards safeguarding the confidentiality of data and its processes.

3.5 THE CENTRAL BANK OF NIGERIA CONSUMER PROTECTION FRAMEWORK 2016 (CPF)

In furtherance of the CBN's mandate to promote a stable financial system, it establishes the CPF to engender public confidence in the financial system. The CPF is made pursuant to the CBN Act 2007 and the Banks and Other Financial Institutions Act 2007 (BOFIA). Section 3.1(e) of the CPF states that consumer information must be protected from unauthorised access and disclosure (Jolayemi & Fatomilola, 2020). Disclosure is only possible upon obtaining the written consent of customers before any

3.6 THE CREDIT REPORTING ACT 2017 (CRPA)

The CRPA is an Act of the National Assembly made to improve access to credit information and standard risk management in credit transactions. The framework includes credit reporting, licencing, and credit bureaus (McVea¸ 2010). Section 9 provides that data subjects maintained by credit bureaus shall be entitled to the privacy, confidentiality, and protection of their credit information, subject to exceptions under subsections 2 to 6 of the same section.

3.7 THE CHILD RIGHTS ACT

The Child Rights Act was adopted in 2003, domesticating the United Nations Convention on the Rights of the Child, which is a human rights treaty designed to guarantee the civil, socio-economic, political, health, and cultural rights of children (Enemo, 2021). The legislation provided for and protected the rights of a child, who is a person under 18 years old. Section 3 of Part II incorporates the provisions of Chapter IV of the Constitution by reference. Section 8 covers a child's rights to private and family life.

3.8 THE NIGERIA COMMUNICATIONS COMMISSION (REGISTRATION OF TELEPHONE SUBSCRIBERS) REGULATIONS 2011 (NCC REGULATIONS)

The NCC is empowered, pursuant to Section 70 of the 2003 Act, to make and publish regulations concerning multiple subjects, including but not limited to permits, written authorizations, and licences, with attendant penalties and offences (Babajide & Odumesi, 2016). Pursuant to this, the NCC issues the Regulations, which apply to telecommunications companies. Regulation 9 of the Regulation furthers the right provided in Section 37 of the 1999 Constitution, and subject to any guidelines issued by the NCC or a licensee, any subscriber whose personal information is stored in the Central Database is entitled to request updates, to have the data kept confidential, and not to have subscriber information duplicated except as prescribed by the Regulation or an Act of the National Assembly. There are other relevant provisions in the regulation.

4. THE SIGNIFICANCE OF CROSS-ORDER TRANSFER OF PERSONAL DATA

In the ever-evolving global landscape driven by technology, the significance of cross-border data transfer has risen to prominence, shaping the way businesses operate, governments interact, and individuals connect. This dynamic process, involving the movement of data across international borders, is not just a technicality; it has become a fundamental enabler of progress, innovation, and cooperation on a global scale.

The digital technology revolution has become a cornerstone of the global economy's operation. Its impact goes beyond merely altering the functioning of traditional industries; it has brought about a profound transformation in the interactions between economies, businesses, governments, and institutions. This contemporary equivalent of the Silk Route is characterised by the presence of undersea fibre-optic cables and satellite links that serve as conduits for transmitting electronic information. The transfer of data across borders has democratised access to various services. Educational platforms, telemedicine, and financial services can now reach underserved regions and remote communities, bridging gaps and improving the quality of life. Cross-border data flow empowers individuals with opportunities that were previously inaccessible due to geographic barriers. This development has given rise to global delivery models, allowing workers to engage in foreign labor markets without being hindered by immigration barriers. What was once considered non-tradable has evolved, with services now constituting a substantial portion of the global economic landscape.

The World Trade Organisation (WTO) predicts a notable shift in the trade landscape, with services projected to play an increasingly significant role. According to their estimations, the proportion of services in total trade will witness an escalation from 21 percent to 25 percent by the year 2030. This transformation underscores the growing impact of services on global economic activity, illustrating the evolving nature of trade patterns in response to the rise of digital technology. The influence of digital technologies reaches beyond the realm of trade in services; it extends its impact to various sectors of the economy. This phenomenon is exemplified by the evolution of goods consumption, where products like books, music, and movies are now commonly consumed in digital formats, aptly termed "digital goods." The process of digitization has prompted a substantial shift in the trading landscape for these goods.

One of the transformative aspects of digitalization is its ability to negate geographical constraints and significantly reduce trade-related costs. Studies indicate that international trade costs have experienced a notable

decrease of 15 percent between 1996 and 2014. This reduction in trade costs has the potential to catalyse an annual increase of 1.8 percent to 2 percent in overall trade until 2030, cumulatively contributing to a growth rate of 31 percent to 34 percent over a span of 15 years (Steinfeld, 2006). As we have seen, cross-border data transfer lies at the heart of international trade and commerce. Businesses, regardless of their size or industry, rely on the seamless exchange of information to collaborate with partners, suppliers, and customers across different regions. In the digital age, a manufacturer in Asia can communicate directly with retailers in Europe, facilitating supply chain efficiency and reducing lead times. E-commerce platforms can instantly reach customers on a global scale, enabling businesses to tap into new markets with ease.

In conclusion, cross-border data transfer stands as a pillar of the modern digital society, shaping economies, societies, and cultures across the world. Its significance extends beyond business transactions and technical intricacies, encompassing the very fabric of how we interact, innovate, and evolve as a global community. As we navigate the complexities of data governance, we must strive to unlock the full potential of cross-border data transfer while upholding values of privacy, security, and cooperation. As technology continues to advance, the significance of cross-border data transfer is poised to grow even further. Emerging technologies such as 5G, edge computing, and the Internet of Things (IoT) will amplify the need for seamless data exchange. As we navigate this landscape, finding ways to address challenges while harnessing the immense potential of global data connectivity will be pivotal.

5. CROSS-BORDER DATA TRANSFER UNDER THE NIGERIA DATA PROTECTION ACT (NDPR) 2019

Before the newly enacted Nigerian Data Protection Act of 2023 came into force, the data protection sphere was largely protected by the Nigerian Data Protection Regulation of 2019 (hereinafter referred to as the NDPR 2019) (Ere-Mendie, 2023).

Under the NDPR 2019, the regulation of cross-border transfers of personal data was governed by two permissible methods:

1. **Adequacy Decision by NITDA under the supervision of the Attorney General of the Federation:**

This approach involved obtaining an adequacy decision from the National Information and Technology Development Agency (NITDA) under the supervision of the Attorney General of the Federation (AGF). This process required a thorough assessment by the AGF, including a review of the foreign country's data protection framework. Moreover, the AGF was tasked with evaluating general and sector-specific legislation about public security, national security, defense, and criminal law. Based on these evaluations, the AGF would decide on the adequacy of data protection measures in the foreign country.

1. **Alternative Conditions for Transfer:**

In cases where an adequacy decision was not attainable, the NDPR outlined several conditions that allowed for cross-border transfers of personal data:

1. **Explicit Consent:** The transfer could occur if the data subject explicitly consented to the proposed data transfer. Before giving consent, the data subject needed to be informed about the potential risks associated with such transfers.
2. **Contractual Performance:** Transfer was permitted if it was necessary for the performance of a contract or the implementation of pre-contractual measures at the data subject's request.
3. **Contractual Conclusion in the Data Subject's Interest:** Transfers were acceptable if they were necessary for the conclusion or execution of a contract that benefited the data subject and was established between the controller and another natural or legal person.
4. **Public Interest:** Transfers could be justified if they served important reasons of public interest.
5. **Legal Claims:** Transfer was permissible when necessary for the establishment, exercise, or defence of legal claims.
6. **Protection of Vital Interests:** Data transfers were allowed to safeguard the vital interests of the data subject or other individuals, particularly if the data subject was unable to provide consent due to physical or legal incapacity. However, this provision was subject to the condition that the data subject was informed through explicit warnings about the specific data protection principles that might be compromised in the event of transfer to a third country.

In all instances, the NDPR emphasised the importance of transparency and clear communication with data subjects regarding the implications of cross-border data transfers. The regulation strived to strike a balance between enabling necessary data transfers and safeguarding the privacy and rights of data subjects (Ere-Mendie, 2023).

6. CROSS-BORDER DATA TRANSFER UNDER THE NIGERIA DATA PROTECTION ACT (NDPR) 2023

Where personal data is to be transferred or shared with a country outside Nigeria, the law has made ample provisions for the procedure to legally do so. The recently enacted Nigeria Data Protection Act 2023 (NDPA) introduces a distinctive approach compared to its predecessor. Unlike the previous requirement of obtaining an adequacy decision from the NITDA or the AGF, the NDPA streamlines the process for cross-border data transfers (Adaji, 2023). This new legislation outlines that

such transfers can occur when the recipient of personal data adheres to a law, binding corporate rules, contractual clauses, code of conduct, or certification mechanism that ensures adequate protection aligned with the NDPA's provisions.

In contrast to the earlier framework, the responsibility for determining the sufficiency of protection now rests solely with the Nigeria Data Protection Commission (the Commission). This signifies a shift from the role previously held by the AGF, implying that the Commission will now be responsible for issuing adequacy decisions.

In compliance with the Act, data controllers and processors are mandated to uphold certain obligations. This includes the imperative of maintaining comprehensive records that substantiate the grounds for conducting cross-border transfers of personal data and the assessment of the adequacy of protection. The Act empowers the Commission to establish rules that require organisations to notify the Commission about the measures they have in place to ensure data security and explain their adequacy. Additionally, the Commission has the authority to identify specific categories of personal data that have additional restrictions on cross-border transfers, considering the nature of the data and the risks to data subjects.

7. THE ADEQUACY OF PROTECTION UNDER THE NDPA 2023

The concept of "adequacy of protection" is a pivotal aspect of this provision. It is defined within Section 42 of the Act as one that upholds principles substantially similar to those outlined in the Data Protection Act (Makulilo, 2013). When evaluating the adequacy of protection, several critical factors are taken into account. These factors collectively contribute to the comprehensive evaluation process and assist in determining whether the data protection measures in place meet the required standards. These factors include enforceable data subject rights, access to administrative or judicial redress, the existence of data protection laws, competent supervisory authorities, and international commitments.

However, when a satisfactory level of protection is absent, cross-border data transfers are permissible only under certain conditions outlined in Section 43 of the NDPA. These conditions include obtaining and maintaining the consent of the data subject, transfers necessary for contractual performance or initiation, transfers in the data subject's interest, transfers for public interest reasons, transfers for legal claims, and transfers to protect vital interests when the data subject is unable to provide consent. They largely resemble the provisions highlighted in the NDPR earlier. Notably, there is a new addition to the conditions: allowing cross-border transfers if they are solely for the benefit of a data subject, and obtaining the data subject's consent for the transfer is impractical. Additionally, if obtaining consent is feasible and the data subject is likely to provide consent, the transfer can be conducted under this circumstance.

The NDPA's approach reflects a more streamlined and comprehensive framework for cross-border data transfers, focusing on ensuring data protection while facilitating necessary international data flows. The transition of authority to the Commission for issuing adequacy decisions signifies a centralised and expert-driven approach to safeguarding personal data during cross-border transfers.

8. RECOMMENDATIONS

It has been discovered that local tech companies in Nigeria face various challenges when utilising foreign cloud-based technologies and storing data with service providers located outside of Africa. These challenges may now include ensuring compliance with the Nigerian Data Protection Act (NDPA) and international best practices, maintaining data security and privacy, and managing potential jurisdictional conflicts (Osherenko, 2006). By way of recommendation, the following should be considered:

1. **Data Localization and Jurisdiction:** One of the challenges that may be faced by local tech companies is the potential conflict between the requirement to store personal data within Nigeria (data localization) and utilising foreign cloud service providers with data centres located outside Africa. To solve this challenge, companies can explore hybrid cloud solutions that combine local data centres with foreign cloud providers. This approach allows for the storage of sensitive personal data within Nigeria while leveraging the scalability and efficiency of global cloud infrastructure. By carefully selecting cloud service providers that have a strong commitment to data privacy and security, companies can ensure compliance with the NDPA and international best practices.

2. **Data Transfer Mechanisms and Adequate Protection: T**he NDPA requires data controllers and processors to ensure that personal data transferred outside Nigeria receives an adequate level of protection. Local tech companies must assess the data protection measures implemented by their foreign cloud service providers and ensure compliance with international standards. Implementing measures such as robust encryption, access controls, regular security audits, and contractual agreements with service providers can enhance data security and privacy. It is important to conduct due diligence when selecting cloud service providers, considering factors such as their data protection policies, certifications, and adherence to global data protection frameworks like the EU's General Data Protection Regulation (GDPR).

9. CONCLUSION

In an era defined by globalization and intricate digital interconnections, the significance of cross-border data transfers cannot be overstated. These transfers serve as critical facilitators of economic expansion and technological innovation. Yet, within this landscape of data movement, an essential equilibrium must be achieved—a balance between the fluid exchange of information and the imperative to safeguard individual privacy rights. As the world transforms and evolves through technological leaps, there is an inherent necessity to continually adapt and refine Nigeria's data protection framework. This adaptability ensures that the nation remains attuned to technological advancements and the shifting global standards that govern data flows.

The pursuit of equilibrium lies at the heart of this endeavor. It is a pursuit that recognises the value of both open data circulation and the inviolable right to privacy. The synergy of these ideals holds the key to a sustainable and harmonious digital landscape. By adapting and evolving its data protection framework, Nigeria positions itself to effectively navigate the intricate landscape of cross-border data transfers, where challenges and opportunities coexist. As the Nigerian data protection framework evolves, it reflects the nation's commitment to keeping pace with technological innovations. By embracing this commitment, Nigeria reaffirms its role in the global community—a nation that proactively seeks to foster a progressive and protective environment for digital interactions. The continuous evolution of the data protection framework is more than a legislative necessity; it symbolises a commitment to fostering a resilient and adaptable digital ecosystem.

Through this journey of evolution, Nigeria holds the potential to achieve multifaceted outcomes. The protection of its citizens' privacy rights is not a standalone goal but a foundation upon which various pillars of progress stand. By nurturing a robust and transparent environment for cross-border data transfers, Nigeria achieves more than the safeguarding of individual rights; it constructs a fertile ground for data-driven innovation to flourish. Such innovation is the catalyst for economic growth, development, and international collaboration—an arena where Nigeria can stand as a significant contributor and collaborator.

In conclusion, the dynamic nature of the digital era mandates a proactive and holistic approach to cross-border data transfers. Nigeria's efforts to strike a harmonious balance between data flow and privacy rights illuminate a path of conscientious progress. By adapting its data protection framework, Nigeria not only safeguards its citizens but also establishes a framework for data innovation that can reshape its socio-economic landscape and enhance its standing on the global stage.

REFERENCES

Act, C. (2015). Cybercrimes (Prohibition, Prevention, Etc) ACT, 2015. *Centre For Laws Of The Federation Of Nigeria*.

Adaji, A. E. (2023). Reconciling the ideals of open science with data privacy in the context of health research in Nigeria: A legal analysis.

Alston, P., & Crawford, J. (Eds.). (2000). *The future of UN human rights treaty monitoring*. Cambridge University Press.

Babajide, A. O., & Odumesi, J. O. (2016). An exploratory study of internet control and surveillance. *Computing Information Systems, Development Informatics & Allied Research Journal*, *7*(4).

Babalola, O. (2022). Nigeria's data protection legal and institutional model: an overview. *International Data Privacy Law*, *12*(1), 44-52.

Bulgakova, D., & Bulgakova, V. (2016). The compliance of facial processing in France with the article 9 paragraph 2 (a)(g) of (EU) General data protection regulation. *Regulation*, *119*, 1.

Elgujja, A. A. (2020). A synopsis on data protection under the Nigerian laws: has the universality of right to privacy trickled down to Nigeria?. *OSF Preprints*.

Enemo, I. P. (2021). Challenges Still Facing the Domestication and Implementation of Key Provisions of Nigeria's Child Rights Act of 2003. *Nordic Journal of Human Rights*, *39*(3), 358-372.

Ere-Mendie, A. J. (2023). Nigerian Data Policies. *The Mediation of Sustainability: Development Goals, Social Movements, and Public Dissent*, 161.

Finck, M., & Pallas, F. (2020). They who must not be identified—distinguishing personal from non-personal data under the GDPR. *International Data Privacy Law*, *10*(1), 11-36.

Jolayemi, L. B., & Fatomilola, O. (2020). Causal Relationship between Industrial Action and Economic Growth in Nigeria. *Open Access Library Journal*, *7*(5), 1-14.

Kline, R. R. (2015). *The cybernetics moment: Or why we call our age the information age*. JHU Press.

Makulilo, A. B. (2013). Data Protection Regimes in Africa: too far from the European 'adequacy'standard?. *International data privacy law*, *3*(1), 42-50.

Martins, O. P., Luke, A. I., Chima, O. A., Chinaza, U., & Williams, E. E. (2020). Journalists perception of the freedom of information act (FOIA) in Nigeria: A study of journalists in imo state. *Media & Communication Currents*, *4*(2), 108-128.

McVea, H. (2010). Credit rating agencies, the subprime mortgage debacle and global governance: the eu strikes back. *International & Comparative Law Quarterly*, *59*(3), 701-730.

Oni, A., Okunoye, A., & Mbarika, V. (2016). Evaluation of E-Government Implementation: The Case of State Government Websites in Nigeria. *Electronic Journal of e-Government*, *14*(1), pp48-59.

Orji, U. J. (2018). *Telecommunications Law and Regulation in Nigeria*. Cambridge Scholars Publishing.

Osherenko, G. (2006). New discourses on ocean governance: understanding property rights and the public trust. *J. Envtl. L. & Litig.*, *21*, 317.

Steinfeld, H. (2006). *Livestock's long shadow: environmental issues and options*. Food & Agriculture Org..

Tom, J., Adigwe, W., Anebo, N., & Bukola, O. (2023). Automated Model for Data Protection Regulation Compliance Monitoring and Enforcement. *International Journal of Computing, Intelligence and Security Research*, *2*(1), 47-57.

***philosophy*, *19*, 206-219.**

Searle, J. R. (2004). *Mind: A brief introduction*. oxford university press.

Searle, J. R. (2008). *Philosophy in a new century: Selected essays*. Cambridge University Press.

Sorem, E. (2010). Searle, materialism, and the mind-body problem. *Perspectives: International Postgraduate Journal of Philosophy*, *3*(1), 30-54.

Stroll, A., & Popkin, R. H. (2012). *Philosophy made simple*. Routledge.

Taylor, J. R., & Cooren, F. (1997). What makes communication 'organizational'?: How the many voices of a collectivity become the one voice of an organization. *Journal of pragmatics*, *27*(4), 409-438.

Tollefsen, D., & Dale, R. (2012). Naturalizing joint action: A process-based approach. *Philosophical Psychology*, *25*(3), 385-407.

Underhill, E. (2018). *Mysticism: A study in the nature and development of man's spiritual consciousness*. Routledge.