COVID-19 DATA GOVERNANCE AND PRIVACY PROTECTION IN NIGERIA: A HUMAN RIGHTS PERSPECTIVE

Lateef A. Adeleke PhD

Department of Public and International Law, College of Law Fountain University, Osogbo, Osun State, Nigeria,
dr.lateefadeleke@gmail.com +2348075139978

Abstract

As the world get rid of the spread of Covid-19, an issue of great concern lies in wait for scholarly engagement. This engagement affects the legal issues surrounding the collection, use and storage of personal data of Nigerians, who were screened, quarantined, isolated, treated and discharged from various isolation centers and health facilities across the nation. Large volumes of personal data concerning Nigerians are held by numerous government agencies. The outbreak of corona virus generated additional volume of data of great value, to both the data subjects and the global data economy. The personal data being generated in the course of Covid -19 treatment constitute the personality of the data subject, the protection of which is a human right issue. To the data merchants, commoditising the personal, medical and genetic data which Covid – 19 generated, is a boom to the data economy. Although, Section 26 (1) of the Nigerian National Health Act, provides that personal data should be treated with confidentiality, however, the problem of commoditising personal data in the global data economy has heightened legal concerns in Nigeria. While the birth of the Nigerian data protection Act 2023, is a timely event, the paper examines its adequacy in protecting data privacy breach. The main argument of this article is that health workers need to comply with data protection principles as they continue to relate with the records of Covid-19 and other patients. The paper adopts doctrinal research method. It's key finding is that, personal data rights, especially in health sector, are prone to breaches, despite the enactment of new law. The paper therefore advocates the amendment of the Nigerian data protection Act 2023, to provide for specific guidelines on the use of health data for research purposes. This will protect the human rights of Nigerian data subjects, because, Dual-Use Research of Concern (DURC) is a modern reality.

Key words: Personal data, Covid-19, Human rights

1. Introduction

Decades ago, data collection was carried out by states, for information gathering about the population and for the purpose of planning the welfare of the people[1]. Today, however, data has taken a central stage in human socio-economic and political endeavour, not only because of the ubiquitous nature of the internet, which serves as its receptacle and means of dissemination, but also for its capacity to reconfigure relationships between states, subjects, and citizens[2]. Data and data collection has thus metamorphosed from strictly a means of ameliorating the conditions of the citizens and diminishing their restlessness, that it was, in the hands of conservative enthusiasts in the 19th century, to a big economic activity in modern time. Hence, vocabularies such as, data mining[3], data merchant[4], commoditisation of data[5], data economy[6], data politics[7], genetic information market[8], among others, have coloured the pages of literatures across relevant disciplines. This is also the reason why personal data has been termed "the new oil" of the information society and new currency of the digital world[9].

Consequent upon the foregoing, data protection has not only become a compelling necessity, but also a human right issue[10]. The central problems around data protection in Nigeria, are

[1] Hacking, Ian. 2015. "Biopower and the Avalanche of Printed Numbers." *In Biopower: Foucault and Beyond*, edited by Vernon W. Cisney and Nicolae Morar, 65–80. Chicago, IL: University of Chicago Press.

[2] For instance, Didier Bigo etal., reported that big data was allegedly manipulated to influence the pattern of vote in the US election and UK referendum. It was alleged that Cambridge Analytica, a company owned by Robert Mercer, a US billionaire, mined the personal data of about 87 million users from Facebook, used same to predict their personality profiles and reeled out advertisement model that suit their psychological profiles. This personal data breach became scary when Cambridge Analytica claimed that its action is legal and hundreds of companies harvest such data. To make matters worse, CEO Mark Zuckerberg owned up that Facebook took no precaution to ensure that the numerous apps it approved adhere to their terms of service. See: Didier etal, (2019) Data Politics, World, Subject, Right. Routledge : New York p. 5

[3] M.R. Bharati, Data Mining Technique and Applications, India Journal of Computer Science and Engineering, (2010) Vol 1 (4) 301-305, S. Arora and J. Birla A Review on Law of Data Mining, Journal of Engineering and Technology (2015) Vol 4 (2) T. Khabaza, Nine Laws of Data Mining (2022) http://creativecommons.org/licenses/by-nc-nd/4.0, and Giorgos V. A Literature Review of "Lawful" Text and Data Mining , Open Research Europe (2024) vol 4, 1-35

[4] Vallemoni R.K, Cononical Payment Data Models for Merchant Acquiring: Merchants, Terminal, Transactions, Fees and Chargebacks, International Journal of Computer Science and Engineering, (2022), Vol. 3, 42-66

[5] D.W Augustin, Personal Data as a Commodity in The Digital Economy, *International Journal of Socia, Politics and Humanities*, (2025) Vol. 8 (1) p 2, D. Alberto and L. Michael, Data as Tradeable Commodity and New Measures for their Protection, The Italian Law Journal, (2015) Vol 1, p. 3

[6] Data Economy: Radical Transformation or Dystopia, *Frontier Technology Quarterly*, (2019) p. 2-6, F. Maryam and V. Laura, Model for Data Economy, National Bureau of Economic Research, Cambridge (2022) p. 4-32, A. Sestino, A. Kahlawi and D. Andrea, Decoding Data Economy: A Literature Review of Its Impact on Business, Society and Digital Transformation, *European Journal of Innovation Management* (2023) Vol. 28, p. 2-26

[7] Didier etal, (2019) Data Politics, World, Subject, Right. Routledge: New York p. 5

[8] R. Daviet, N. Gideon, J. Wind, Genetic Data: Potential Uses and Misuses in Marketing, *Journal of Marketing*, a Journal of the American Marketing Association, (2022) Vol. 86 (1) 7-26

[9] World Economic Forum (WEF), Personal Data: The Emergence of a New Asset Class (Aug. 11, 2014), available at http://www3.weforum.org/docs/WEF ITTCPersonalDataNewAssetReport_2 011 .pdf. accessed 17/3/2026

[10] M. Brkan, The Essence of the Fundamental Rights to Privacy and Data Protection: Finding the Way Through the Maze of the CJEU's Constitutional Reasoning, German Law Journal (2019), 20, pp. 864–883, C. Weiquan, Data

indiscriminate accumulation of personal data, undeserving transparency of data subject, occasioned by various indiscretion to which data subjects are exposed to, in the hands of states and business entities. Even when data is collected, collectors hardly adhere to the purpose of collection. Another legal question is the inadequate safeguard of information legitimately collected. In Nigeria, Large volumes of personal data concerning Nigerians are held by numerous government agencies. These include; the National Population Commission (NPC), National Identity Management Commission (NIMC), Federal Road Safety Commission (FRSC), Independent Electoral Commission (INEC), Nigerian Immigration Service, Health care facilities, Banks and Mobile phone service providers, among others. The protection of this huge data is of great legal concern.

The outbreak of Covid - 19 and the attendant response of the Nigerian health sector, generated additional volume of data which are of great value, to both the data subjects and the global data economy. While data subjects crave for protection of their personal information, the data economy can only thrive when such information is a commodity in the data market. In Nigeria, diagnostic and molecular Laboratories provided invaluable services as Covid – 19 grew in to a Public Health Emergency of International Concern (PHEIC) and an epidemic. This was done through prompt diagnosis, surveillance capacity and epidemiology studies. Yet, there are some biosecurity and legal concerns, chief among which is sample and data Management[11]. In the respected opinion of Abdulrauf[12], Nigeria is a country that is rapidly growing technologically and most services rendered in various sectors are reliant on Information Technology (IT). Therefore, accumulation and use of personal information will be inevitable.

The fear expressed in past literatures[13], about the non-existence of legal frameworks for privacy and data protection in Nigeria has been allayed by the provisions of Nigerian Data Protection Regulation (NDPR) 2019 and the Nigeria Data Protection Act (NDPA) 2023. This contribution examines the compliance of data controller with the general principles of data protection and Data Protection Regulations in Nigeria, regarding the personal data collected in the wake of Covid – 19 in the country. What seems to heighten legal concern is that digitisation has made the generation and dissemination of personal data faster and cheaper than ever. Again, the fortress that separates private sector research from traditional academic endeavour is fast disappearing, just as the

Protection as a Fundamental Right: The European General Data Protection Regulation and Its Exterritorial Application in China, *US-China Law Review,* (2019), Vol.16, No. 3, 97-113

[11] Ibid

[12] L. A. Abdulrauf Do We Need to Bother About Protecting our Personal data? Reflections on Neglecting Data Protection in Nigeria Yonsei Law Journal (2014) Vol.5 No.2 p. 64 -95

[13] A. Kusamotu, *Privacy law and technology in Nigeria: The legal framework will not meet the test of adequacy as mandated by Article 25 of European Union Directive* 95/46, 16(2) INFO. & COMM. TECH. L. 149 (2007). S. Okedara, O. Babalola and I. Chukwukelu, *Digital Rights in Nigeria: Through the Cases*, Digital Rights Lawyers Initiative (DRLI) (2022) 45-95

distinction between researches that benefit humanity and those that serve private interests (especially in Africa) is blurrier than ever[14]. The acceleration of Dual-Use Research of Concern (DURC) has also made research atmosphere to be suspicious. DURC is research intended for good which may also be used to cause harm to humans. This is possible via synthetic viruses and genetic engineering of pathogens[15]. Importantly, there is a paradigm shift from natural resources and physical labour as fundamental sources of wealth, to information and knowledge.[16] Thus, personal data, an important specie of the information taxonomy, has become vulnerable as an intangible asset that wield influence in the corporate boardroom discussion. This paper thus seeks to interrogate the following issues: how adequate is the Nigerian data protection legal framework? Did COVID-19 emergency measures comply with privacy law? How does Nigeria compare to international standards?

2. 0 The meaning of Data

Today, data can be generally described as information transmitted and stored into a computer or any other digital device. Black's law dictionary 11th edition defined data as *"facts or figures, in a form that can be processed, stored, or transmitted by a computer"*[17]. *Etymologically, the word ''data'' has its root in the Latin word ''datum'' which means '' thing given'' it* encompasses a broad swathes of information that can be processed, analyzed, and utilized for various purposes[18]. It serves as the foundation for insights and decision-making[19] across multiple fields, including business, healthcare, and technology[20]. Essentially, data is information prepared for action, designed to be processed, managed, and transferred. It takes many forms, including numbers, text, and multimedia, allowing us to interact with and understand our environment.

2.1 Classification of Data

Broadly speaking, data can be classified based on the following variables: structure, source, nature, and sensitivity. For the scope of this paper, it delves into only the nature and sensitivity of data as means of classification.

---

[14] In 1996, Nigeria had 109,580 cases of meningitis with 11,717 deaths. Pfizer, a U.S. pharmaceutical company, took advantage of the situation to launch a new antibiotic drug, Trovan. Having tested the drug on adults with serious side effects, such as liver problems and cartilage abnormalities, Pfizer decided to test the efficacy of Trovan in pediatric settings. After one year of this unethical experimentation, 11 out of the 200 children used as experimental guinea pigs died, while many were reported to suffer various disabilities including paralysis and liver failure. Jegede A.S. What Led to the Nigerian Boycott of the Polio Vaccination Campaign? PLoS Med. 2007; 4(3):e73. https://doi.org/10.1371/journal.pmed.0040073. LA Adeleke COVID-19 Vaccine and the Legal Conundrum of Informed Consent and Public Health Emergency in Nigeria, GET Journal of Biosecurity & One Health [2022] vol. 1 57- 67

[15] Note 2 supra

[16] T.A. Stewart, Intellectual Capital (Doubleday/Currency, New York, 1997) at 12.

[17] *Black's Law Dictionary* (11th ed Thomson Reuters 2019).

[18] M Chen and others "Big data: A survey." *Mobile Networks and Applications (2014) 19*(2) 171-209.

[19] ibid.

[20] C L Borgman, *Big data, little data, no data: Scholarship in the networked world.* MIT Press (2015) 9

Classification based on nature include; Qualitative data which **is** descriptive and non-numerical, capturing characteristics, opinions, observations, and attributes of a subject. It is widely used in research relating to behavioral analytics. It provides insights into phenomena by exploring concepts[21] Quantitative data on the other hand focuses on measurable entities and statistics[22].

2.2 Classification based on sensitivity

Public data: Public data refers to information that is made available by government agencies, organizations, and institutions for public access and use. This data can encompass a wide range of topics, including census information, economic statistics, health data, environmental reports, and educational records. The transparency and availability of public data promote accountability and informed decision-making among citizens, researchers, and policymakers[23].

2.3 Private or Personal Data

Private or personal data is central to this paper, it refers to information that is not publicly accessible and is often protected due to privacy concerns, confidentiality, or proprietary interests[24]. This type of data can include personal information such as Social Security numbers, financial records, medical history, and sensitive business information. Organizations and individuals have a vested interest in safeguarding private data to prevent unauthorized access, identity theft, or data breaches. The handling of personal data is governed by various legal frameworks and regulations.

Article 1 of the African Union Convention on Cyber Security and Data Protection defines personal data as follows: "Any information relating to an identified or identifiable natural person by which this person can be identified, directly or indirectly in particular by reference to an identification number or to one or more factors specific to his/her physical, physiological, mental, economic, cultural or social identity"[25] The National Information Technology Development Agency (NITDA) Guidelines as contained in the NITDA Act 2007, define personal data as any information relating to an identified or identifiable natural person ('data subject'); information relating to an individual, whether it relates to his or her private, professional or public life. It can be anything from a name, address, a photo, an email address, bank details, posts on social networking websites, medical information, or a computer's IP address. The Guidelines define personal sensitive data as data relating to: (a) religious or other beliefs (b) sexual orientation health (c) race (d) ethnicity (e) political views (f) trade union membership (g) criminal record.

---

[21] **J W Creswell,** *Research Design: Qualitative, Quantitative, and Mixed Methods Approaches* (4th ed. **2014)** *SAGE Publications.*

[22] **S J Tracy,** *Qualitative Research Methods: Collecting Evidence, Crafting Analysis, Communicating Impact* (2nd ed. **2020)**. *Wiley-Blackwell.*

[23] **B Ubaldi,** "Open Government Data: Towards Empirical Analysis of Open Government Data Initiatives." *OECD Working Papers on Public Governance,* **[2013]** *No. 22.*

[24] **S D Warren, & L. D Brandeis,** The Right to Privacy. *Harvard Law Review, (***1890)** *4(5), 193-220.*

[25] Article 1, African Union Convention on Cyber Security and Data Protection (2014)

The Registration of Telephone Subscribers Regulation 2011 provides that personal information refers to: (a) full names (including mother's maiden name) (b) gender (c) date of birth (d) residential address (e) nationality (f) state of origin (g) occupation and such other personal information (h) contact details of subscribers, as specified in the Regulation Specifications. Regulation 1.3 of the Nigerian Data Protection Regulation (NDPR) defines defines sensitive data as follows: (a) religion or belief (b) sexual orientation (c) health (d) race (e) ethnicity (f) political view (g) trade union membership (h) annual record (i) any other sensitive personal information[26] The category of data which is the subject of this paper is private or personal data, which are equally sensitive.

Section 65 of the Nigerian Data Protection Act 2023 defines personal data as:

> any information relating to individual, who can be identified or identifiable, directly or indirectly, by reference to an identifier such as, name, an identification number, location data, an online identifier, or one or more factors specific to the physical, physiological, genetic, psychological, cultural, social or economic identity of that individual

The same section defines sensitive personal data as date relating to individual's (a) genetic and biometric data, for the purpose of uniquely identifying a natural person, (b) race or ethnic origin (c) religious or similar beliefs such as those reflecting conscience or philosophy, (d) health status (e) sex life; (f) political opinions or affiliations; (g) trade union memberships; or (h) other information prescribed by the Commission as sensitive personal data in section 30 (2) of the Act.

3.0 The Notion of Privacy

The concept of privacy is deeply rooted in societal values and legal traditions. The notion of privacy is innate to man, but it has changed in nature and forms in tandem with human civilization and technological development. Today, privacy has grown from mere physical space that it was, to informational privacy in the age of information revolution. In philosophy, privacy has been a subject of enquiry. A significant figure in the discussion of privacy, is privacy as a concept of human dignity, famously emphasized by Immanuel Kant. Kant proposed that individuals possess inherent dignity and should be treated as ends in themselves, not merely as means to an end. Privacy, in this context, serves as a safeguard for personal dignity and autonomy[27]. When people

[26] See: Regulation 1.3 (xxv). Any other sensitive personal information has been categorized to include the following: (a) financial data (b) income data (c) matrimonial information (d) social security numbers like; Bank Verification Number (BVN), National Identification Number (NIN), Personal Identification Number (PIN), and Tax Identification Number (TIN) and (f) genetic and biometric information. See also; Karen McCullagh, 'Data Sensitivity: Proposal for Resolving the Conundrum' (2007) 2 (4) *Journal of International Commercial Law and Technology*, 109 – 201. Catherine Jasserand, Legal Nature of Biometric Data: from Generic Personal Data to Sensitive Data (2016) 2 (3) *Eur. Data Protection Law Revision*, 297

[27] I Kant, *Groundwork of the Metaphysics of Morals* (M. Gregor, Trans.). *Cambridge University Press*, (1998)

can control their personal information and maintain their private lives[28], they uphold their self-respect and agency[29]. This view highlights that infringement on privacy can lead to violations of moral respect and the dignity of individuals, particularly in a world increasingly driven by data and surveillance.

Solove,[30] in an attempt to conceptualize privacy puts the various aspects in which we face privacy issues under six themes. They include; the right to be let alone, limited access to the self, secrecy, control of personal information, personhood, and intimacy. In explaining the right to be let alone, he examined the work of Samuel Warren and Louis Brandeis[31]. This concept, often associated with the notion of personal freedom, underscores the fundamental desire for solitude and autonomy from external intrusion. In his new work, Solove[32] advances a taxonomy of privacy that includes four general categories and sixteen subcategories of activities that can lead to disruptions of private life. The general categories are; information collection (the methods by which data about people is collected), information processing (the storage, use and analysis of personal data), information dissemination (the means by which personal data is transferred or disclosed), and invasions (direct interferences with an individual's life). In protecting privacy, all these issues must be addressed. Contextually, Helen Nissenbaum[33] sees Privacy is one of the most enduring social issues associated with information technologies.

3.1 Theoretical Framework

The central idea of this paper is driven by two theories, the non-intrusion theory of privacy and the Informational Self-determination theory.

Non - Intrusion theory of privacy

The Non-intrusion theory of privacy was propounded by James Moor in 2004[34]. It is a philosophical theory that views privacy from the prism of a right to be free from unwanted intrusion into one's personal space or private affairs. This theory is particularly relevant today, as ''problematisation'' of privacy is an increasingly pressing legal concern. The meaning of this is that, privacy has become a problem that is attracting the attention of legal scholars all over the world. Today, personal data is being accessed, shared and used for various purposes without the data subject's knowledge or explicit consent. This theory aligns with section 37 of the 1999 Constitution of the Federal Republic of Nigeria which provides for right to private and family life.

---

[28] J.H Reiman, *Driving to the Panopticon: A Philosophical Exploration of the Risks to Privacy Posed by the Information Technology Revolution*. *The Monist, (*2004) *86*(3), 347–370.

[29] I Kant, *The Metaphysics of Morals* (M. Gregor, Trans.). *Cambridge University Press, 1996.*

[30] J Solove, Conceptualizing privacy. *George Washington Law Faculty Publications* (2002)

[31] D Warren, & D Louis The Right to Privacy, 4 Harvard Law Review (1980)193

[32] D J Solove,. *On Privacy and Technology*. Oxford University Press (2025).

[33] H. Nissenbaum, Privacy as Contextual Integrity *Washington Law Review* (2004) 101

[34] J Moor, 'The Non-Intrusion Theory of Privacy' *The Journal of Information Technology* (2004) 1

The theory acknowledges that data subjects have the right to control the information about themselves that is accessible to others. The theory also recognises that data subjects have the right to control the context in which their personal information is shared. Importantly, the Non - Intrusion theory of privacy acknowledges that privacy is not an absolute right and it needs to be balanced against other values such as security and public interest. This is in consonance with section 45 of the 1999 Constitution of the Federal Republic of Nigeria which provides for restriction on and derogation from the fundamental rights of the citizens.

4.0 Informational Self-Determination Theory

This theory was authored and articulated by the Federal Constitutional Court of Germany in its landmark Census Decision of December 15, 1983. The court developed this theory as a response to the 1983 population census, ruling that individuals have a fundamental right to decide for themselves when and within what limits their personal data is disclosed and used. This theory was distilled from two major provisions of the German Constitution[35]. These are; Article 2 (1) of the German Basic law, which guaranteed right to personality and Article 1(1) of the German basic law, which guaranteed right to human dignity. These provisions are similar to the provisions of section 37 of the 1999 Constitution of the Federal Republic of Nigeria, which provides for right to private life and section 34 of the same Constitution which provides for right to the dignity of human person. Scholars have since made contribution to the development of the theory.

Helen Nissenbaum's primary contribution is a paradigm shift from viewing privacy as a ''right to control'' or ''secrecy'' to viewing it from another prism, as a matter of Contextual integrity[36]. While the original German theory of informational self-determination focused on an individual's power to decide how their data is used, Nissenbaum argued that this ''control'' model is insufficient in a digital world. Her theory of Contextual integrity suggests that privacy is preserved when information flows remain appropriate to the specific social context in which they occur. The core goal of Nissenbaum's Contextual integrity is appropriateness of information flow. The mechanism is adherence to contextual norm (choice and consent of data subject). Privacy is then breached, when data flow out of its original context without permission.

5.0 Legal Framework for Data Protection as Human Right

The 1948 Universal Declaration of Human Rights (UDHR) stands as the cornerstone of international human rights law, fueling the development of numerous binding international and national legal frameworks. Its influence is evident in countless domestic constitutions, laws, and policies designed to safeguard fundamental rights. The UDHR establishes a fundamental international standard for privacy, explicitly safeguarding both physical and communicative

[35] J. C. Buitelaar, Post-mortem Privacy and Informational Self-determination, Ethics Information Technology (2017) (19) 129–142

[36] H. Nissenbaum, Privacy as Contextual Integrity *Washington Law Review* Vol 79, (2004) 119 - 124

spaces. Specifically, Article 12 of the UDHR aims to ensure legal protections for the rights to privacy and confidentiality as it provides thus:

> No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honour and reputation. Everyone has the right to the protection of the law against such interference or attacks.

The right to privacy is not just a right, it is a fundamental human right, also enshrined in the following international instrument: Articles 14 and 17 of the International Covenant on Civil and Political Rights (ICCPR); Articles 16 and 40 in the Convention on the Rights of the Child (CPR); Article 14 of the International Convention on the Protection of the Rights of All Migrant Workers and Members of Their Families; Article 22 of the Convention on the Rights of Persons with Disabilities; and Article 4 of the African Charter on Human and Peoples' Rights.

The 1999 Constitution of the Federal Republic of Nigeria, which provides for the fundamental rights of its citizens in its chapter IV, upholds the right to privacy as sacrosanct. Section 37 thereof, provides for the guarantee and protection of the privacy of citizens, their homes, correspondence, telephone conversations and telegraphic communications.

The Nigerian Supreme Court in recent time, has expanded the meaning of right to privacy under the Nigerian Constitution, due to the global digital revolution. In *Emerging Market Telecommunication Services v. Godfrey Nya Eneye*, it was held that the respondent breached the applicant's privacy by sending unsolicited messages and advertisements without his consent[37]. *Molehin v. United Bank of Africa (UBA)*[38], represents another significant decision where the Court decided that the rights to privacy of data under the Nigeria Data Protection Regulation (NDPR) is subsumed under the right to privacy as provided by Section 37 of the 1999 Constitution and thus, a fundamental right.

Briefly, the facts of the case are that Miss Molehin provided her UBA savings account to her employer for the payment of her salary, which was denominated in US Dollars. The employer subsequently deposited the salary into the designated account as instructed. However, UBA opened a domiciliary dollar account and paid the money therein instead of the designated account. UBA argued that the action was taken in Miss Molehin's best interest as paying dollar into her naira account would run contrary to certain the Central Bank regulation. The Court held that opening the dollar account without her consent constitute data privacy breach as the action is contrary to Paragraph 2.2 of the NDPR and section 37 of the Nigerian 1999 Constitution.

The above case is similar to *Nworah v UBA*[39] and *Tokunbo Olatokun v Polaris Bank Limited*[40], it is significant, as it shows the readiness of Nigerian courts to expand the frontiers of data privacy

[37] (2018) LPELR-46193
[38] Suit No. FHC/L/CS/2625/2023
[39] Suit No. FHC/L/CS/1484/2021
[40] Suit No: LD/17392MFHR/2024

jurisprudence. It noteworthy, that while the case of *Molehin v UBA* was held based on the NDPR, *Tokunbo Olatokun v Polaris Bank Limited* was decided pursuant to the Nigeria Data Protection Act 2023 (NDPA).

Section 26 (1) (b) of the Nigerian Data Protection Act 2023 provides that personal data must be collected for specified, explicit and legitimate purposes and not to be further processed in a way incompatible with theses purposes. The appropriate medium to communicate such purposes to the data subjects in through the privacy policy of the of the data controller such as the EMID platform for Covid – 19 vaccination. Section 26 (1) (f) of the same Act provides that personal data must be processed in a manner that ensures appropriate security of personal data, including protection against unauthorized and unlawful processing, access, loss, destruction, damage or any form of data breach. In similar vein, the said protection ought to have been made known to the data subject via the EMID privacy policy, which is non-existence. Section 24 (3) of the Act, provides that every data controller owes the data subjects duty of care for the protection of their personal data and must be accountable for any data breach. Section 47 of the Act provides for enforcement of the provisions of the Act while section 49 thereof, provides for legal sanctions, including fines and terms of imprisonment for failure to comply.

As a fundamental right, right to privacy cannot be taken away without the consent of an individual. Hence, section 30 (1) of the Nigerian Data Protection Act 2023 prohibits any data controller or processor to process sensitive personal data of an individual without his or her consent among other conditions. While the UDHR treats privacy rights as fundamental human rights, these rights, are subject to limitations. Article 12(2) permits restrictions only if they pass a three-part test: legality (based on law), legitimate aim (serving a valid purpose), and proportionality (the restriction is no greater than necessary). Section 45 of the 1999 Constitution of the Federal Republic of Nigeria provides for derogation of the fundamental human rights including right to privacy, in defense of public interest and the right of others. In similar vein, Section 3 of the Nigerian Data Protection Act 2023 provides for the limitation in the application of the Act, in defense of national security and public interest. However the said restriction does not affect sections 24, 25, 32 and 40 which relate to the core principles of personal data protection, lawful basis for personal data processing, appointment of data protection officer, and personal data breaches respectively.

The provision for restriction is for the purpose of meeting the just requirements of morality, public order and the general welfare in a democratic society. However, there must be a measure of legal protection against arbitrary interferences by public authorities on personal data. This is very important today, because dual-use research of concern (DURC) has also made research atmosphere to be very suspicious. Especially at a time when personal data has been reduced to a commodity, to drive the growing global data economy.

6.0 Personal Data Generation and Management during Covid -19 Immunization in Nigeria

The efforts of all our regular and special health facilities across the country did not go unnoticed, and prosperity will never forget the commitment and resilience of every category of health worker,

while Covid – 19 ravaged our nation. However, some of the information collected and documented in the course of duty constitute personal data of the patients (data subjects) and need to be protected within the ambit of the law. For instance, Laboratories processed and stored sensitive data during four major phases of (a) arrival of patients in the Laboratory premises and registration of their data, (b) pre-analytical, (c) analytical and (d) post analytical phases. Data accumulated from the foregoing exercise are required to be adequately regulated and protected. Data that escape to the wrong hands, including those of non-state actors, may be manipulated for biosecurity and personal data breach[41].

From the provisions of various Nigerian regulations earlier examined, some of the sensitive personal data collected from data subjects during Covid – 19 intervention are; full name, sexual orientation, health history, phone number, date of birth, e-mail address, residential address and National Identification Number NIN among others. These data are required to be supplied by data subjects in the Electronic Management of Immunization Data (EMID), a registration platform of the Federal Ministry of Health for Covid-19 vaccination. The platform captures personal data and schedules people for Covid – 19 immunization. A cursory look at the EMID shows that it has no privacy policy. This omission is contrary to the provision of Article 2.5 of the Nigeria Data Protection Regulation (NDPR), which requires the publicity and clarity of privacy policy from any medium of personal data collection such as the EMID used by the Federal Ministry of Health to facilitate Covid-19 vaccination.

The said Article provides thus:

> Notwithstanding anything contrary in this Regulation or any instrument for the time being in force, any medium through which Personal Data is being collected or processed shall display a simple and conspicuous privacy policy that the class of Data Subject being targeted can understand[42].

The provision states further that the privacy policy shall in addition to any other relevant information contain the following:

a) what constitutes the Data Subject's consent;
b) description of collectable personal information;
c) purpose of collection of Personal Data;
d) technical methods used to collect and store personal information, cookies, JWT, web tokens etc.;
e) access (if any) of third parties to Personal Data and purpose of access;
f) a highlight of the principles stated in Part 2;
g) available remedies in the event of violation of the privacy policy;
h) the time frame for remedy; and

[41] Note 3 at p.12
[42] Article 2.5 Nigeria Data Protection Regulation 2019

i) provided that no limitation clause shall avail any Data Controller who acts in breach of the principles set out in this Regulation.[43]

Privacy terms and all the above sensitive provisions meant to protect personal data of Nigerians were not provided for in the EMDI platform used by the Federal Ministry of Health to generate data in the course of Covid -19 vaccination. What the EMID contained is Google Privacy Policy which is neither relevant nor applicable. About the application of Google Privacy Policy, the Policy reads:

> This Privacy Policy applies to all the services offered by Google LLC and its affiliates, including YouTube, Android, and services offered on third party sites, such as advertising services. This Privacy Policy doesn't apply to services that have separate privacy policies that do not incorporate this Privacy Policy.[44]

The implication of the foregoing is that, the Privacy Policy applies to only Google services mentioned therein, but does not apply to even other Google services with separate privacy policies. Therefore, the EMID portal not being a Google service but the service of the Federal ministry of Health, which is guided by a separate and distinct legal framework (NDPR), is required to have a separate and distinct Privacy Policy (not Google Privacy Policy) as provided in Article 2.5 paragraph (a) – (i) of the NDPR. It is also worrisome, that the Federal Ministry of Health, one of the authorities responsible for data protection in Nigeria[45] could float an electronic portal for the purpose of collecting personal data of millions of Nigerians without a Privacy Policy.

More so, section 26 (1) of Nigerian Health Act, requires that personal data be treated with confidentiality. Again, Federal Ministry of Health is a data controller within the definition of the NDPR and therefore owes data subjects duty of care as well as other obligations. Article 3.1 (x) defines a data controller as: ''a person who either alone, jointly with other persons or in common with other persons or a statutory body determines the purposes for and the manner in which Personal Data is processed or is to be processed''. Within the context of the foregoing provision, the Federal Ministry of Health is a Data Controller. Consequently, the most compelling duty of a Data Controller is the legal responsibility of complying with obligations under the NDPR.

In similar vein, the EMID portal being used by the Federal Ministry of Health to collect data for the purpose of Covid -19 vaccination does not comply with the provision of Article 3.1 (7) (b) of the NDPR, which provides that the Data Controller shall appoint a Data Protection officer and make the contact details of such officer available to the Data Subjects. Similarly, Section 32 of the

[43] Ibid

[44] See: https://policies.google.com/privacy#about accessed 16/02/2023

[45] Other authorities responsible for data protection in Nigeria National Information Technology Development Agency (NITDA), Nigerian Communications Commission (NCC), National Identity Management Commission (NIMC) Federal Road Safety Commission (FRSC) and Central Bank Of Nigeria (CBN) among others.

Data Protection Act provides that every Data Controller of significance (like the Federal Ministry of Health) should retain an expert as a Data Protection officer, whose duty shall be the prevention of data breach among other things. The community reading of Articles 2.5 (a) – (i), 3.1 (x) and 3.1 (7) (b) shows that the EMID portal does not comply with the relevant provisions of the NDPR. Ultimately the portal contravenes the main objective of the regulation as provided in Article 1.1 (a), which is the safeguard of the rights of natural person to privacy. The portal does not provide for data security required in Article 2.6, as it fails to develop an effective organisational policy for handling Personal Data.

Broadly speaking, the Federal Ministry of Health, through the EMID portal, breached the duty of care imposed on it as a Data Controller by Article 2.1 (2) of the NDPR. The Article provides thus: ''Anyone who is entrusted with Personal Data of a Data Subject or who is in possession of the Personal Data of a Data Subject owes a duty of care to the said Data Subject''. Duty of care simply means the duty a party owes in law, to be careful, so that his conduct will not injure another party or person.[46] It is a duty imposed by law, to exercise reasonable care, so that a party's actions and omissions do not injure other parties or persons[47]. The question of whether the Federal Ministry of Health owes Nigerians who are Data subjects on the EMID portal a duty of care has been determined by Article 2.1 (2) of the NDPR quoted above. In this circumstance, it is foreseeable due to the insecurity of the global cyberspace, that if the Ministry does not exercise due care as prescribed by the NDPR, Data subjects on the EMID portal will be injured.

In specific terms, the non-compliance of the EMID portal, with the combined provisions of Articles 2.5 (a) – (i), 2.6, 3.1 (7) (b) and resultantly 1.1 (a) of the NDPR, shows that the Federal Ministry of Health as a Data Controller is negligent of the duty of care imposed on it by the law. This is because, duty of care is pivoted on the foreseeability that the other party will be exposed to the risk of injury if one party continues particular acts or omissions.[48] The omission of the EMID portal to comply with the provisions of the NDPR has exposed millions of Nigerians to the risk of personal data breach, which is not only a breach of duty of care but also an infringement on their right to privacy. [49]

7. 0 Nigerian Courts on Breach of Privacy

Right to privacy is one of the constitutional rights guaranteed by chapter IV of the 1999 Constitution, which is entitled, 'Fundamental Rights,' spanning from section 33 to section 46. Right to privacy is specifically provided for in section 37 of the Constitution, which include right to personal data privacy. This has been upheld by Nigerian courts in a number of decided cases in

[46] G Kodilinye, and O Aluko The Nigerian Law of Torts, Spectrum Books Limited: Ibadan (1999)

[47] ibid

[48] See: L A Adeleke, Service Providers' Duty of care on the Exposure of Subscribers to Heavy Metals from Silver Coatings on Mobile Phone Recharge Cards in Nigeria, *Crescent University Law Journal* [2017] Vol. 2

[49] In tort, breach of duty of care is categorised as a tort of negligence. The age long consideration of whether a reasonable man in the position of Federal Ministry of Health as a Data Controller, will act the same way in similar circumstances is ever relevant. In assessing the standard of care expected of Data Controller in Nigeria and determine what a reasonable man would do in the circumstances at hand, the law considers the risk factor, which has four elements.

recent time. Section 46 of the Constitution, gives jurisdiction to the High Court of a State in matters relating to the breach of any fundamental right in Chapter IV of the Constitution. The provision runs as follows:

> 46 (1) any person who alleges that any of the provisions of this Chapter has been, is being or likely to be contravened in any State in relation to him, may apply to a High Court in that State for redress.

In consonance with this provision, many cases in respect of personal data privacy have been instituted before the Nigerian courts for determination. Especially with respect to whether personal data protection is a fundamental human right. While some judges who are not in tune with digital rights have declined that personal data privacy is a fundamental right, digital migrants among our judges have held personal data privacy to be a fundamental human right concern. The dictum of Nweze, JSC in *Kalu **v.** State*[50] comes to relevance, where his Lordship stated that issues around fundamental rights should not be subjected to the austerity of tabulated legalism. In fundamental rights cases, it is enough that an applicant's complaint is understood and deserves to be entertained by the court.

On whether the right to privacy extends to protection of personal data, the Court in *Incorporated Trustees of Digital Right Lawyers Initiative v. L.T. Solutions & Multimedia Limited*[51], referred to *Nwali v. Ebonyi State Independent Electoral Commission & Ors*[52] to hold that the court has no power to restrict the phrase "privacy of citizens" to specific situations but must interpret it generally, liberally, and expansively. The court referred to the NDPR as a sector specific regulation made pursuant to section 37 of the 1999 Constitution. It is thus evident, that, the provisions are to be interpreted expansively and liberally to ensure the protection of personal data privacy of citizens. On the strength of foregoing, the court further held as follows:

> In the light of the above, I thus also have no hesitation in holding that the right to privacy extends to protection of a citizen's personal data such [has] been alleged that the Respondent has violated or is threatening to violate as I now go on to consider whether the Respondent has indeed violated the Applicant's right to privacy or threatens to violate it.[53]

The court in *Incorporated Trustees of Digital Rights Lawyers Initiative v. Minister of Industry, Trade and Investment & 2 Ors,*[54] held that failure of the Respondent to provide privacy policy on

---

[50] [2017] 14 NWLR (Pt. 1586) 522, 544–545

[51] Unreported Judgement of the High Court of Ogun State, Abeokuta Judicial Division, Coram Hon. Justice O. Ogunfowora, delivered on the 9th day of November 2020 in Suit No. HCT/262/2020.

[52] [2014] LPELR–23682

[53] Ibid

[54] Unreported Case Suit No. FHC/AWK/CS/116/2020, Delivered by the Federal High Court, Awka

its portal and to appoint a data control officer, constitute a breach of the NDPR. This is similar to what the Federal Ministry of Health did through the EMID portal. The facts are as follows: in 2020, the Nigerian Federal Government, via the Ministry of Industry, Trade and Investment, launched the Micro, Small and Medium Enterprise (MSME) Survival Fund. This initiative involved an online application process hosted at https://www.survivalfund.gov.ng, where personal data, including sensitive information like the Bank Verification Number (BVN), was collected and processed from Nigerian citizens applying for the government funds.

On who is a Data Controller, the Federal High Court Awka per Dimgba J. held:

> I have carefully examined the NDPR particularly Regulations I. l (a), 2.1(d), 2.1(3), 2.3 (b), 2.5, 2.6, and 3.1(7) outlined above and spelling out the obligations of data controllers and duties of data subject, as well as exhibits 3 – 6 which is an electronic document generated from the Applicant's computer on the MSME Survival Fund application portal of the 1st Respondent. First, I quite agree with Applicant that indeed the 1st Respondent is a data controller by virtue of Regulation 1.3 (x) NDPR which defines a data controller as "a person who either alone, jointly with other persons or in common with other person or a statutory body, determines the purpose for and the manner in which persona data is processed or to be processed. (p.18)

On when a Data Controller will be held liable for breach of data privacy of a data subject, the court held:

> The 1st Respondent did not deny the Applicant's case by providing any evidence to show that the obligations set out above as a data controller were complied with. The Applicant furnished the Court with Exh.3 – 6 which are photographs of the MSME Survival Fund Program online portal and in them I see that neither of the obligations required of the 1st Respondent by the NDPR were complied with. (p.20)

> All things considered, I hold that the failure of the Respondents, from taking measures towards protecting the data privacy of the citizens, taking into account the vital information required from the data subject such as the Bank Verification Number, names and addresses, poses a threat to the Applicant's members right to private and family life owing to the fact that the objectives of the NDPR as provided in

Judicial Division on Tuesday 2nd day of November 2021. Coram: Justice N. O. Dimgba

> Regulation 1.1 is to safeguard the rights of natural persons to data privacy. (p.20)

The foregoing decision applies *mutatis mutandis* to the EMID portal created by the Federal Ministry of Health for Covid – 19 intervention, where sensitive data of Nigerians were collected without any privacy policy to safeguard their rights. Just like the Ministry of Industry, Trade and Investment, in the above decision, the Ministry of Health is a data controller within the meaning of section 24 of the NDPA 2023 and ought to process personal data of the data subjects in line with the provisions of the law. Section 26 of the NDPA puts the burden of proofing the consent of data subject on the data controller. The only means of establishing such consent is through the privacy policy, to which data subjects consent. Section 32 of the NDPA further provides for the appointment of a data protection officer, to guide every data controller about the lawful process of personal data. Again, section 28 of the Act provides for data privacy impact assessment, to measure the risk or impact of processing personal data on the data subjects. All these, including the provisions of the NDPR earlier identified were not complied with by the EMID portal. The portal was therefore mounted in gross violation of the data protection laws and regulation of the country.

8.0 Theoretical Discussion

This paper is driven by the theories of non-intrusion of privacy, Informational Self-determination as well as Contextual integrity, as stated earlier. The central argument of this paper is that personal data of Nigerians submitted to the Electronic Management of Immunization Data (EMID), a registration platform of the Federal Ministry of Health for Covid-19 vaccination, ought to be accessed, processed and shared in accordance with the provisions of the Nigerian laws and regulations. The, Non - Intrusion theory of privacy, echoes the above legal concerns in the following ways; (i) data subjects have the right to control the information about themselves that is accessible to others, (ii) data subjects have the right to control the context in which their personal information is shared and (iii) that privacy is not an absolute right as it needs to be balanced against other values such as security and public interest. However, the EMID portal denied data subjects of having control over how their data is treated, when it failed to provide privacy policy guide acceptance or denial of consent. In the case of Informational Self-determination, for data in the custody of a data controller to have Contextual integrity, it must be obtained from the appropriate channel (the data subject). There must be adherence to contextual norm (i.e. choice and consent of data subject). Privacy is breached, when data flow out of its original context without permission of the data subject. For instance, if a data subject does not click 'I agree", the data controller should not transmit such data to a third party. In the case of the EMID portal which is the subject of discussion in this paper, privacy policy was entirely absent, thereby denying the data subjects their informational self-determination, leaving their data with no contextual integrity. The paper holds that, the rights of the data subjects who submitted to the EMID portal could be simply protected with the provision of privacy policy to which their personal data is subjected, and such Nigerians could expressly consent or decline such terms and conditions. However, the EMID portal did not provide such privacy policy. The portal therefore denied Nigerians who submitted their personal

sensitive data to the EMID platform, the right of determination over same. This finding is in consonance with the provisions of law and decisions of the court as discussed in the paper.

9.0 Conclusion and Recommendation

From Lassa fever to Ebola, from Ebola to Covid -19, every regional or international outbreak or epidemic, presents an opportunity to enrich the growing global data economy. Dual - Use Research of Concern (DURC) is another modern reality and bitter a pill to swallow. The foregoing situation calls for adequate personal data protection policy and legal framework to tighten the loose ends. It is noteworthy that the Covid – 19 emergency measure discussed in this paper did not comply with data protection principles as contained in the Nigerian legal framework.

While the enactment of NDPA 2023 is a response to the global trend in data protection, this paper finds that the NDPA needs certain improvements. For instance, it does not provide explicit guidelines on the use of health data in research but applies general personal data processing principles. There is the need to amend the NDPA 2023, to be in tune with global best practices, to provide for a broader ethico - legal framework in the age of DURC in the health sector. For instance, unlike the US Health Impact Portability and Accountability Act (HIPAA), the NDPA does not have an established mechanism for waivers or the use of de-identified health data in research, making it less flexible for researchers handling health data at a large scale, the like of which Covid-19 provides.

In similar vein, section 33 of the Nigerian Health Act 2014 requires researchers to obtain informed consent for health research involving human participants. However unlike the HIPAA of the US, it does not provide for structured exemptions or guidelines for data anonymisation, for the protection of data subject.

From a compliance perspective, this paper acknowledges the regulatory and compliance initiatives undertaken by the Data Protection Commission. Examples of this include the Nigerian Data Protection Commission's fine of N555.8 million against Fidelity Bank for violations of the Nigeria Data Protection Act, 2023, and the Nigeria Data Protection Regulation, 2019[55]. Additionally, the Federal Competition and Consumer Protection Commission in Nigeria, imposed a $220 million fine on Meta Platforms for breaching data privacy laws[56]. The decided cases as cited earlier are other instances. While these actions demonstrate commendable efforts to enforce the provisions of the law, this paper notes a lack of comparable cases within the healthcare sector. Our laws and regulations therefore need to be more comprehensive and responsive in a very important sector like health.

[55] Patrick-Okwoli L. NDPC fines bank N555.8 million over data privacy violations. Business Day. August 21, 2024. https://businessday.ng/news/article/ndpc-fines-fidelity-bank-n555-8-million-over- accessed 14/03/2025

[56] Okamgba J. Nigeria fines Meta $220m for violating consumer, data laws. July 20, 2024. Punch Newspaper. https://punchng.com/nigeria-fines-meta-220m-for-violating-consumer-data-laws/#google_vignette accessed 14/03/2025

A significant strength of the U.S. HIPAA is its explicit requirement for data controllers to conduct routine risk assessments and establish security policies tailored to the sensitivity of electronic personal health information (ePHI). This stands in stark contrast to the Nigerian National Health Act (NHA), which does not contain comparable provisions, leaving data security and management largely to the discretion of individual healthcare institutions. On the whole, the Nigerian national Health Act and the NDPA 2023 need a thorough review, to adequately protect the data subjects and catch up with global best practice