



GoogleAnalytics



GoogleScholars



KBLSP Journal

Open Research Europe

THE CONCEPT OF ‘PERSONAL DATA’ IN THE NIGERIAN DATA PRIVACY LAWS

•Olugbemi O. Jaiyebo

•MPhil/Doctoral Candidate, College of Law of Igbinedion University School of Post Graduate Studies and Research Okada. <ojaiyebo@gmail.com>

••Doctoral Advisor and Head, Department of Public & International Law-Igbinedion University College of Law Okada. <anya.kingsley@iuokada.edu.ng>**••Professor Anya Kingsley Anya**<<https://orcid.org/0009-0004-5549-1852>>**10.5281/zenodo.21306854**

Abstract

The UNCTAD in 2018 ranked Nigeria as the largest e-commerce market in Africa, in terms of number of shoppers and accruing revenue, against the observation of the World Bank Group that ‘digital financial services’ potentials remained untapped despite the large share of unbanked population. Against this background, the Nigerian government developed series of policies and strategies to harness the anticipated potentials of the Nigeria digital environment by providing personal data into various databases. This official approach triggered the need for a balancing of the equities of ‘data owners’ and ‘data collectors.’ Against this backdrop, the authors argued that dominant liberal response to the increasing discrepancy in digital power should and ought to provide a veritable plank for greater government regulation and oversight. Flowing therefore, the paper considered questions of ‘ownership and control of personal data in Nigeria,’ against the backdrop of lack of transparency in data collection, trade in personal data and power inequality in the digital economy. The authors evaluated the concept of personal data and the consequences for breach of the privacy of personal data in ‘twelve data privacy related legislative instruments in Nigeria,’ and concluded that the examination of the constitution and twelve data privacy related laws is tilted in growth in stages and that these two instruments that deal specifically with data protection are subsidiary legislations which pre-dated the specialized legislation. The authors maintained the need for a systematic alliance between legal and technical experts, in order to have effective regulations devoid of digital exploitation.

Keywords: Privacy laws, legislation, personal data, data owners, databases.

©Terms & Conditions of access and use can be found at <https://www.kblsp.org.ng/index.php/kblsj>

1. Introduction

The internet and smartphones have contributed significantly to making data more valuable, available and abundant. Fifty-three million smartphones were connected in

Nigeria in 2018.¹ In 2021, there were one hundred and eight million internet subscribers with a monthly data consumption of eighty million gigabytes² resulting in a digital data generation increase by over 200 per cent between 2019 and 2022.³ The more our houses, cars, watches and phones are connected to the internet the more data that can be generated. The collection, use, storage, access, security and transfer of personal data is indispensable in a digital economy.⁴ The provision of personal data, sometimes very personal information into government and commercial databases trigger the need for a balancing of the interests of owners of the data with the responsibility to be imposed on collectors, processors and custodians of the data, whether they be private or public entities. The National Digital Economy Policy and Strategy, launched in November 2019, emphasizes the implementation of e-Governance as a means of improving governance and deepening democracy. These information systems have become critical information infrastructure which must be safeguarded, regulated and protected against breaches.⁵

The digital economy is a global phenomenon that has inherent power imbalances against the global south, and manifesting in form of lack of transparency in data collection, trade of personal data between third parties and data aggregators, lack of sensitivity to the contexts in which the data are situated, data leaks and power inequality are some of the factors that undergird the need for tools that allow citizens take intelligent control over the collection and usage of their data. Individuals' personal data is an embodiment of their personality which is under threat from the advances in technology, which ultimately deserving of legal protection for their 'virtual personas.'⁶ For instance, a significant portion of the data collected by government agencies in Nigeria are contracted to private entities, including foreign corporations, for processing and management.

Nigeria's effort is relatively new following the data privacy regulation with its first data protection-specific subsidiary legislation enacted in 2019. The increasing number of data

¹ <https://technext24.com/2021/08/26/nigerias-data-usage-hits-205880-terabytes-representing-202-rise-in-3-years/>

² <https://technext24.com/2021/03/02/nigerians-consume-over-80-million-gigabytes-of-data-per-month-despite-paying-more/>

³ Observation made by the Nigerian Minister of Communications and Digital Economy. <https://dailytrust.com/nigeria-records-200-rise-in-data-generation/>

⁴ Preamble to the Nigeria Data Protection Regulation 2019

⁵ Preamble to the Nigeria Data protection regulations 2019

⁶ Lukman A Abdulrauf & Charles M Fombad, 'Personal Data Protection in Nigeria: Reflections on Opportunities, Options and Challenges to Legal Reforms' (2016) 38(2) Liverpool Law Review 1 @ 4

protection legislations in the world is either a testament to the importance of data protection globally or a desire by many countries to qualify for trade with the EU by meeting its adequacy requirement.⁷

The objectives of the Nigerian Data Protection Regulation are to:

- a) Safeguard the rights of natural persons to data privacy;
- b) Foster safe conduct for transactions involving the exchange of Personal Data; and
- c) Prevent manipulation of Personal Data.⁸

The NDPR applies to natural persons residing in Nigeria or residing outside Nigeria who are citizens of Nigeria and covers all transactions intended for the processing of personal data notwithstanding the means by which the data processing is being conducted or intended to be conducted in respect of natural persons in Nigeria.

The NDPR is Nigeria's pioneer legislation that is dedicated exclusively to the regulation of personal data. The NDPR is modelled after the European Union GDPR. In some quarters the General Data Protection Regulation⁹ and the Nigeria Data Protection Regulation are both applauded as aiming to guarantee strong protection for individuals regarding their personal data and apply to businesses that collect, use, or share personal data, whether the information is obtained online or offline.¹⁰ The definition of personal data, the special categories of personal data and the specification of online identifiers in the EU regulation are very similar to the definitions of personal data, sensitive personal data in the Nigerian Regulation.

Data collection, processing and storage in contemporary Nigeria are driven both by security and commercial motives. There are three categorizations of privacy. Issues of privacy, the protection of personal data and the grave consequences of leaving personal data processing unregulated have been of great concern to the Nigerian government. The legislature in responding to the demands and challenges of digitalization has enacted several laws providing guidelines for the collection, management and storage of personal

⁷ Adekemi Omotubora and Subhajt Basu, 'Next Generation Privacy' (2020) 29(2) Information & Communications Technology Law 151 @ 155 Available at: <https://doi.org/10.1080/13600834.2020.1732055>

⁸ [Hereafter, the NDPR] cf. to the European Union General Data Protection Regulation (GDPR)

⁹ Regulation (EU) 2016/679

¹⁰ Comparing privacy laws. See GDPR v. Nigeria Data Protection Regulation. One Trust Data Guidance

data in Nigeria. Regulatory authorities and the courts are engaging questions on the nature of personal data and the legality of processing data in diverse circumstances.

2. Nature, Scope and Relevance of Personal Data

It is true in 2023 as it was in 1890 that recent inventions and business methods call attention to the next step which must be taken for the protection of the person, and for securing to the individual the right "to be let alone."¹¹ The digitization of our economy and society, in particular the roll-out of the Internet of Things (IoT) and the datafication of business processes, leads to an incredibly fast and ever-increasing mass of data. The need for digital identity lies at the root of citizenship and service-delivery in a digital economy.¹² Data is the new gold. Governments at all levels are the biggest processors of personal data of Nigerians and in Nigeria.¹³ The Independent National Electoral Commission, Nigerian Immigration Service, National Identity Management Commission, Federal Road Safety Corps, the Police and other bodies routinely collect or oversee the collection of biometric and other data. Children's data can now be collected from the moment of their birth. The sheer volume of digital information that is generated during the first 18 years of life and the multiple and advancing technological means for processing children's data all raise serious questions about how children's right to privacy can best be preserved and protected.¹⁴

The NDPR defines sensitive personal data as 'data relating to religious or other beliefs, sexual orientation, health, race, ethnicity, political views, trades union membership, criminal records or any other sensitive personal information.

Significantly, definitions of information, personal information and confidential information adumbrated above, fall within the umbrella of personal data and sensitive personal data under the NDPR. The NDPR provides a general definition for personal data and every person and entity processing data (Data Controller) in Nigeria or processing

¹¹ Samuel D. Warren & Louis D. Brandeis The Right to Privacy Harvard Law Review, Vol. 4, No. 5 (Dec. 15, 1890), p. 193 @ 195 Available at: <https://www.jstor.org/stable/1321160>

¹² National Digital Economy Policy and Strategy (2020-2030) Federal Ministry of Communications and Digital Economy Abuja. P. 33

¹³ See Paragraph 1.2 of the Guidelines for the Management of Personal Data by Public Institutions in Nigeria, NITDA 2020

¹⁴ Children's online privacy and freedom of expression: Industry toolkit. New York. UNICEF (2018)

data emanating from Nigeria must give attention to the sector specific definitions of personal data. The presence of Digital Lending Regulations and the Credit Reporting Act, apparently portends the harmonization and integration of data privacy related laws into the primary legislation. It is gratifying that retention of a digital lending license can be predicated on compliance with the primary data privacy and protection law. The NDPR definition of personal data was largely modelled after the European Union GDPR.

The privacy of citizens, their homes, correspondence, telephone conversations and telegraphic communications is guaranteed and protected by section 37 of the Constitution. "Privacy of citizens" in section 37 of the 1999 Constitution has been interpreted generally, liberally, and expansively to include privacy of citizens' body, life, person, thought, belief, conscience, feelings, views, decisions (including his plans and choices), desires, health, relationships, character, material possessions and family life activities. The courts in Nigeria are conscious of the four types of harm caused by privacy invasion. It has held that the right to privacy implies a right to protect one's thought conscience or religious belief and practice from coercive and unjustified intrusion; and, one's body from unauthorized invasion. The sum total of the rights of privacy and of freedom of thought, conscience or religion which an individual has, put in a nutshell, is that an individual should be left alone to choose a course for his life, unless a clear and compelling overriding state interest justifies the contrary. The right of privacy implies the exclusion of the public eye from prying into an individual's affair...the right to protect one's image and personality and the right to have unfettered access to control one's zones of exclusivity, space, and confidential information.

In order to secure protection within the context of the internet and technologies, the focus has to be on data. The protection of privacy guaranteed under the constitution is applicable to data. The Terrorism Act defines "data" as information generated, sent, received or stored that can be retrieved by electronic, magnetic, optical or any similar means. Data, under the Nigeria Data Protection Regulation means characters, symbols and binary on which operations are performed by a computer, which may be stored or transmitted in the form of electronic signals, stored in any format or any device. Data possess vital capacities because they are about human life itself, have implications for human life opportunities and livelihoods, can have recursive effects on human lives and generate economic value. For instance, in the Incorporated Trustees of Digital Rights

Lawyers Initiative & Ors v National Identity Management Commission case, privacy was interpreted as the right to be free from public attention or the right not to have others intrude into one's private space uninvited or without one's approval. It means to be able to stay away or apart from others without observation or intrusion. It also includes the protection of personal information from others. This right to privacy is not limited to his home but extends to anything that is private and personal to him including communication and personal data.

The protection of data in Nigeria is primarily constitutional and secondarily legislative. When privacy questions arise on the collection, processing and storage of data, section 37 of the Constitution can be invoked. Data not stored in digital format will still be protected by the constitution. The data protection laws of Nigeria relate to digital information. There would be other dealings with personal data that are not privacy based.

The definition of personal data is an element of primordial significance as it determines whether an entity processing data is subject to the various obligations that the Regulation imposes on data controllers. The definition of personal data is far from merely being of theoretical interest. Rather, the contours of the concepts of personal and non-personal data are of central practical significance to almost anyone processing data.

The telecommunications sector is one of the primary conduits for transmission of data in the Nigeria digital economy. In the exercise of its powers to manage or maintain an integrated public number database or an integrated electronic address database, the Nigerian Communications Commission, of necessity, has to access, process and publish personal information. The NCC Act does not make any mention of personal data. It however provides protection against the unreasonable disclosure of personal information about any individual (including a deceased individual) whenever the Commission conducts a public or private inquiry or issues a report on an inquiry.

In furtherance of the Nigeria Digital Economy Policy and Strategies, every telephone number had to be enrolled in the SIM card and transmitted to the National Identity Number (NIN) database. In 2011, the Nigerian Communications Commission (Registration of Telephone Subscribers) Regulation was issued to facilitate the process. Registration of subscribers, of necessity involved the handling of personal information by the licensees. The Regulation subjected the entire registration process to the Constitution,

including the occasions which might warrant handing information to security agencies. The Regulations were emphatic that the information was to be held in strict confidentiality, access to the database was restricted and licensees were prohibited from retaining, duplicating, dealing in or making copies of any Subscriber Information. Release of personal information of a subscriber to any third party could only be with the prior written consent of the subscriber while transfer of subscriber information outside Nigeria had to be done with the prior written consent of the Commission. Licensees shall utilize personal information only for purposes designated by specific laws. In the Nigerian Communications Commission (Registration of Telephone Subscribers) Regulations, “personal information” refers to the full names (including mother’s maiden name), gender, date of birth, residential address, nationality, state of origin, occupation and such other personal information and contact details of subscribers specified in the Registration Specifications.

For purposes of the National Identity database, there is a distinction made between personal information and identification information. Personal information consist of the full names, other names, date of birth, place of birth, gender, address of principal place of residence, address of any other place of residence in Nigeria. Identification information consists of photograph of head and shoulder, signature, fingerprints, and other biometric information about the individual. Both personal and identification information constitute registered information under the NIMC Act. The NIMC Act does not define personal data but it defines registered information to mean in relation to nay registered individual, the information and data, including biometric information entered into the database in respect of the individual.

In the banking sector, the CBN Consumer Protection Framework classifies contact details, account number and balance, statement of accounts and any other information known to the financial institution as confidential information. Information relating to race, ethnicity, colour, religion or political affiliation is to be excluded from data formats, Credit Reports or any other reports or feedback issued by a Credit Bureau to credit information users. The Credit Reporting Act does not define personal data but defines credit information to mean information bearing on a person’s credit worthiness, credit standing or capacity and to the history and profile of such person with regard to credit

assets and any financial obligations, including such person's demographic data and such other information that may aid credit decision making.

"Information" in the Freedom of Information Act, includes all records, documents and information stored in whatever form including written, electronic, visual image, sound, audio recording and "personal information" means any official information held about an identifiable person, but does not include information that bears on the public duties of public employees and officials. With respect to medical records, all information concerning a user, including information relating to one's health status, treatment or stay in a health establishment is confidential. Among the requirements for approval as a Digital lender is the declaration of compliance and commitment to continue to comply with all provisions of law with respect to third-party privacy rights and personal data including data unrelated to principles of lending as provided for the Nigeria Data Protection Regulations, 2019. It is interesting to note that the license of a Credit Bureau can be revoked on the ground that it breached the provisions of a law which deals with data protection, computer misuse or electronic transactions. Section 205 (2) (3) of the Child Rights Act provide that no justice administration information that may lead to the identification of a child offender shall be published and records of a child offender shall be kept strictly confidential and closed to third parties.

The Nigeria Data Protection Regulations and Guidelines for the Management of Personal Data by Public Institutions in Nigeria were subsidiary legislation made specifically for the protection of privacy and other matters related to personal data in Nigeria. In the NDPR, "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; It can be anything from a name, address, a photo, an email address, bank details, posts on social networking websites, medical information, and other unique identifier such as but not limited to MAC address, IP address, IMEI number, IMSI number, SIM, Personal Identifiable Information (PII) and others. While "Personal Identifiable Information (PII)" means information that can be used on its own or with other information to identify, contact, or locate a single person, or to identify an

individual in a context while “sensitive personal data” means data relating to religious or other beliefs, sexual orientation, health, race, ethnicity, political views, trades union membership, criminal records or any other sensitive personal information.

3. The Concepts of ‘Privacy,’ ‘Data Protection’ and ‘Big Data’

It would be wrong to assume that the concepts of “data protection” and “privacy” are completely synonymous. Indeed, the jurisprudence of the European Court of Human Rights and the Court of Justice of the European Union shows that despite substantial overlaps there are also important differences.¹⁵ It should be noted that Nigerian data privacy and protection laws are not rooted in either of the doctrinal disputations. The objectives of the Nigeria Data Protection Regulation¹⁶ are a mixture of data privacy and data protection goals.

The nomenclature, “data protection,” deriving from the German term “*Datenschutz*,” has gained broad popularity in Europe and, to a lesser extent, elsewhere. Its use is being increasingly supplemented by the term “data privacy” which better communicates the central interests at stake and provides a bridge for synthesizing North American and European policy discussions.¹⁷ Data protection involves protection of assets concerning individuals, companies and governments and keeping them out of harm’s way. While data privacy relates to what is done with data that is already in one’s possession. Data protection focuses on the act of safeguarding data already procured regardless of either they are proprietary or not. The concept of privacy tends to precede the question of protection.¹⁸ “Data protection” is typically reserved for a set of norms that serve a broader range of interests than simply privacy protection. To the extent that those norms do engage with privacy protection, they focus only on the informational rather than spatial or physical dimensions of privacy.¹⁹ Protection law specifically regulates all or most stages in the processing of certain kinds of data. It accordingly addresses the way in

¹⁵ Juliane Kokott and Christoph Sobotta, The distinction between privacy and data protection in the jurisprudence of the CJEU and the ECtHR International Data Privacy Law, 2013, Vol. 3, No. 4 p. 222

¹⁶ a) Safeguard the rights of natural persons to data privacy; b) foster safe conduct for transactions involving the exchange of Personal Data; c) prevent manipulation of Personal Data.

¹⁷ Lee A. Bygrave, Privacy and Data Protection in an International Perspective, Stockholm Institute for Scandinavian Law & Lee A Bygrave 2010 p. 168

¹⁸ Uche Val Obi, et al An overview of data privacy and data protection law in Nigeria. The Gravitas Review of Business & Property Law 2019 Volume 10 Issue 4 Page 1 @3

¹⁹ Lee A. Bygrave, op. cit. @ p. 168

which data is gathered, registered, stored, exploited, and disseminated. Putting it differently data protection is a sub-set of the broader privacy concept.²⁰ In contrast to (dignitary) privacy, the protection of personal data is a modern and active right, putting in place a system of checks and balances to protect individuals whenever their personal data are processed.²¹

4. Ownership of data and incidents of ownership under the Nigerian law

Industrial creations confirm that data has now become a new kind of property—an asset that is created, manufactured, processed, stored, transferred, licensed, sold, and stolen. Yet, on a global basis, there is no legal regulatory framework or model that provides guidance on how transactions using data as an asset are to be constructed.²² On the other hand this demand has been described as one of the most facile and legalistic approaches to safeguarding privacy that has been offered to date.²³ Litman however concedes that if this premise is accepted, the natural corollary is that a data subject has the right to control information about him-self and is eligible for the full range of legal protection that attaches to property ownership.²⁴ Once ownership is well- defined, then the attendant rights can be more precisely expressed—rights to access, license, transfer, modify, combine, edit, and delete data naturally flow from the control that ownership vests.²⁵ Data is tangible asset capable of being stolen. It can be traded and moved around for profit. The growing profile of personal data as a commodity and the need for enhancing Trans Border Data Flows was one of the initial motivations for the law on data protection and stimulated the adoption of international data protection instruments, especially the Organization for Economic Cooperation and Development Guidelines and the EU Directive.²⁶

²⁰ Alex B. Makulilo “A Person Is a Person through Other Persons”—A Critical Analysis of Privacy and Culture in Africa. *Beijing Law Review*, 2016, 7, 192 @ 196 Published Online September 2016 in SciRes. <http://www.scirp.org/journal/blr> <http://dx.doi.org/10.4236/blr.2016.73020>

²¹ Adekemi Omotubora and Subhajit Basu, op. cit. @ 157

²² Jeffrey Ritter & Anna Mayer, 'Regulating Data as Property: A New Construct for Moving Forward' (2017-2018) 16 *Duke L & Tech Rev* 220 @ 222

²³ Jessica Litman, 'Information Privacy/Information Property' (2000) 52 *Stan L Rev* 1283 @ 1288

²⁴ Ibid.

²⁵ Jeffrey Ritter & Anna Mayer, op. cit.

²⁶ Lukman A Abdulrauf and Charles M Fombad, 'Personal Data Protection in Nigeria: Reflections on Opportunities, Options and Challenges to Legal Reforms' (2016) 38(2) *Liverpool Law Review* 1 @ 7

Commodification of personal data for the advantage of the data subject is certainly not good for big business. It is therefore not surprising that attempts to make institute data as assets have been unsuccessful. The right to privacy lies within the realm of self-ownership. It is the moral liberty of doing what an individual deems fit to be done with his/her individualism and keeping others outside the sphere of his/her self-ownership.²⁷

In Nigeria, all information contained in the National Identity database is the property of the Federal Government of Nigeria and are treated as classified matter under the provision of the Official Secret Act.²⁸ The central database containing all registered subscribers' information in Nigeria is maintained by the Nigeria Communications Commission and is the property of the Government of the Federal Republic of Nigeria.²⁹ These databases would readily fall within the context of critical national information infrastructure under the Cybercrimes Act.³⁰ A critical examination of Nigerian data privacy laws however reveal that certain incidents of ownership of personal data are reposed in the data subject.

The law vests the data subject with degrees of control over the data in possession of the Government that are suggestive of ownership rights. When a Data Subject has consented to the collection and processing of Personal Data for a specific, legitimate and lawful purpose, a further processing may be done only for archiving, scientific research, historical research or statistical purposes for public interest.³¹ In furtherance of the rights guaranteed by section 37 of the Constitution of the Federal Republic of Nigeria, 1999 and subject to any guidelines issued by the Commission including terms and conditions that may from time to time be issued either by the Commission or a licensee, any subscriber whose personal information is stored in the Central Database or a licensee's database, shall be entitled to view the said information and to request updates and amendments thereto.³²

²⁷ Olomojobi, Yinka, Right to Privacy in Nigeria (October 31, 2017). Available at SSRN: <https://ssrn.com/abstract=3062603> or <http://dx.doi.org/10.2139/ssrn.3062603>

²⁸ Section 3 (2) (2) of the Registration of Persons and Contents of the National Identity Database Regulations, 2017

²⁹ Sections 4 & 5 of the Nigerian Communications Commission (Registration of Telephone Subscribers) Regulations, 2011

³⁰ [Hereafter, the Prohibition, Prevention, Etc. Act 2015]. See particularly section 3.

³¹ Article 2 (1) (a) (i) of the Regulation

³² Article 9 (1) of the Nigerian Communications Commission (Registration of Telephone Subscribers) Regulations, 2011

It would appear that in Nigeria ownership of entrusted persona data is shared between the Federal government and the data subject. Ownership of data collected by consent resides in the data subject. It has been suggested that ownership of data should be recognized at the moment of creation and should attach to data through automated systems exercising control. Once ownership is attached through digital systems, the rights, privileges, controls, and constraints by which the subject data can be used may be expressed and enforced through electronic contracting mechanisms that are already in place across vast sections of the global marketplace.³³

Any person or entity carrying out or purporting to carry out data processing shall not transfer any personal data to any person.³⁴ This is the general rule on transfer of data in Nigeria. In the event of a transfer, there shall be a written contract between the third party and the Data Controller governing the data processing by the third party and compelling compliance by the third party with the Regulation.³⁵ Each party³⁶ to the data processing transfer agreement shall take reasonable measures to ensure the other party does not have a record³⁷ of violating the rights of data subjects and is accountable to NITDA or a regulatory authority for data protection within or outside³⁸ Nigeria.³⁹

Telecommunication Licensees shall not release personal information of a telephone subscriber to any third party without obtaining the prior written consent of the subscriber. Telephone subscriber information shall not be released to a licensee, Security Agency or any other person, where such release of Subscriber Information would constitute a breach of the Constitution or any other Act of the National Assembly, for the time being in force

³³ Jeffrey Ritter & Anna Mayer, 'Regulating Data as Property: A New Construct for Moving Forward' (2017-2018) 16 Duke L & Tech Rev 220 @ 227

³⁴ Article 2(1)(a)(ii) of the Regulation

³⁵ Paragraph 2.7 of the Regulation

³⁶ "A party" shall include directors, shareholders, servants and privies of the contracting party. See Article 2.4 © of the Regulation

³⁷ Record shall include report of public records and reports in credible news media. See Article 2.4 © of the Regulation.

³⁸ NITDA and the Attorney General of the Federation are to supervise transfer of personal data to foreign countries and international organizations. Where no decision is made by either supervisory agent, the transfer could still occur in one of six instances. See Article 2.11 and 2.12 of the Regulation.

³⁹ Paragraph 2.4 of the Regulation

in Nigeria or where such release of subscriber information would constitute a threat to national security.⁴⁰

The tenor of Nigerian legislation is very strict on non-transferability of personal data. The rules are quite explicit: collection of personal data must be for specific purposes and the holder of the data will be allowed to step outside the confines of those specificities with the consent of the data subject. A holistic reading of data privacy laws would suggest that the data subject retains and exercise some incidents of ownership over her personal data after it has been stored in the national database.

The corollary to the principle of non-transferability is the right of portability. Every data subject has a right to data portability.⁴¹ Paragraph 3.1 (14) of the NDPR provides that the Data Subject shall have the right to receive the Personal Data concerning him or her, which he or she has provided to a controller, in a structured, commonly used and machine-readable format, and have the right to transmit those data to another controller without hindrance from the controller to which the Personal Data have been provided, where: (a) the processing is based on consent, or (b) on a contract, and (c) the processing is carried out by automated means. The right of portability is an incident of ownership.

The questions on and implications of ownership of data is not as pronounced in government databases as it when personal data becomes an instrument of profit-making in the control of corporations. One of the major attractions of technology companies to Nigeria is the potential of its e-commerce market. In 2018 the e-commerce spending in Nigeria was estimated at USD 12 billion and was projected to increase to USD 75 billion in revenues by 2025. This digital commerce was provided, among others, by 87 Nigerian platforms, employing 2.9 million people in the country.⁴²

Article 2 (1) (b) of the Regulation provides that Personal Data shall be adequate, accurate and without prejudice to the dignity of human person. The right to privacy is guaranteed in order to protect human dignity. Human dignity is a multi-faceted concept. At its core, however, is the understanding that a human being has intrinsic or inherent worthiness,

⁴⁰ See section 10 (2)(3) of the Nigerian Communications Commission (Registration of Telephone Subscribers) Regulations, 2011

⁴¹ This right shall not apply to processing necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the Controller. See Paragraph 3.1 (15) of the Regulation

⁴² NIGERIA Digital Economy Diagnostic Report. The World Bank Group Washington DC 2019 p. 14

and therefore, is worthy to be treated with a certain measure of respect and concern by the society and other human beings.⁴³ The laws have endeavoured to empower individuals to restrict the access of others to one's personal information. The courts in Nigeria share the perspective when it held that the sum total of the right of privacy and of freedom of thought, conscience or religion which an individual has, is that an individual should be left alone to choose a course for his life, unless a clear and compelling overriding state interest justifies the contrary.⁴⁴

However, with the increasing use of technology for daily living, the individual sends lots of information, some knowingly and most unknowingly, into the custody of government, corporations and other persons. The first of the four needs identified by Westin is 'identity formation.' Many of these data traces are collected, accessed and exploited by other actors and agencies, often without people's knowledge or consent. In some cases, however, people can view and use the data thus produced about them. They may choose to actively collect digitized information about themselves using devices and software specifically designed for this purpose, such as self-tracking apps, platforms and wearable devices. People can also sometimes review data about themselves collected by other actors, such as social media metrics, employee dashboards, educational outcomes, medical records and so on. These technologies work to capture and materialize immanent dimensions of human embodiment, creating human data assemblages.⁴⁵

5. Duties imposed on persons handling Personal Data in Nigeria⁴⁶

⁴³ Alfred Mavedzenge The Right to Privacy v National Security in Africa: Towards a Legislative Framework which Guarantees Proportionality in Communications Surveillance. *African Journal of Legal Studies*, Volume 12(3), 2020, Pp 360 @375. Available at: https://brill.com/view/journals/ajls/12/3-4/article-p360_7.xml

⁴⁴ Paul Galinje JCA (as he then was) in Tega Esabunor (Suing by his next friend Mrs. Rita Esabunor) v. Dr. Tunde Faweya & Ors. [2008] 12 NWLR (Pt. 1102) 794 @ 810, quoting Ayoola JSC in *Medical and Dental Practitioners Disciplinary Tribunal v. Okonkwo* (2001) 7 NWLR (Pt.711) 206

⁴⁵ Deborah Lupton How do data come to matter? Living and becoming with personal data. *Big Data & Society* July–December 2018: 1–11 Available at: DOI: 10.1177/2053951718786314 journals.sagepub.com/home/bds

⁴⁶ Duty as a matter of fact, implies the obligation imposed on and not necessarily the sanction aspect. However, the sanction aspect of duty is reflected in most of the legislations appertaining to privacy and protection of data.

Every person handling personal data in Nigeria, whether by trust or by being in possession, owes a duty of care to the data subject.⁴⁷ Whether a Data Controller comes into possession of personal data by consent of the data subject, by way of a contract related to the data subject, by operation of law or for the protection of vital interest of the data subject, there is a duty of care owed to the data subject. The concept of the duty of care is also specifically mentioned in the banking sector dealings with personal data. The CBN Consumer Protection Framework requires that as a duty of care, financial institutions are obliged to safeguard the privacy of their customers' data and shall not reveal consumers/customers information to a third party except in very specific circumstances.⁴⁸ Every one handling personal data in Nigeria has a legal obligation to adhere to a standard of reasonable care to avoid acts that could reasonably cause foreseeable harm to data subjects.

Article 2 (2) of the Regulation provides that 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. It can be argued, along the lines of the Supreme Court decision in *Medical and Dental Practitioners Disciplinary Tribunal v. Okonkwo*⁴⁹ that this section states the duty of persons handling personal data. It does not by itself create an offence but creates a duty where it would have been doubtful whether or not one existed in criminal law. It establishes liability for consequences of the breach of that duty. It makes negligence the basis of criminal liability for offences against the person where the need to establish intention, knowledge and such mental elements as basis of liability would have been required. It does not dispense with the need to allege in a charge the causal connection between an alleged breach of duty of reasonable skill and care and its consequence, nor does it dispense with the need to charge a specific offence. Under Article 2.2 of the NDPR the processing of personal data shall be lawful in any one of five circumstances:

- a) Where consent has been given for the specific purpose;

⁴⁷ Article 2 (2) of the NDPR

⁴⁸ a) With the express permission of the customer; b) As required by the CBN and other regulatory bodies; c) Where there is a court order; d) In pursuance of public duty/interest. See Paragraph 2 of the CBN Consumer Protection Framework 2016

⁴⁹ (2001) 7 NWLR (Pt.711) 206 @ 237

- b) Processing is necessary for the performance of a contract to which the Data Subject is party or in order to take steps at the request of the Data Subject prior to entering into a contract;
- c) Processing is necessary for compliance with a legal obligation to which the Controller is subject;
- d) Processing is necessary in order to protect the vital interests of the Data Subject or of another natural person, and
- e) Processing is necessary for the performance of a task carried out in the public interest or in exercise of official public mandate vested in the controller.

The express consent of the data subject is required in only the first of the five circumstances under which data can be lawfully processed in Nigeria. In the second instance, consent of the data subject can be regarded as implied. In scenarios (c) to (e), the consent of the data subject is not relevant. The access, processing and storage of the personal data flow from the operation of law, vital interest of a natural person or of public interest. The persons handling personal data in these categories should be regarded as having been entrusted with personal data of a data subject. A tortious 'breach of trust' approach is less likely to legitimize wholesale commercial exploitation of personal information. It would permit courts to give effect to subtle distinctions between consensual and invasive disclosure. Moreover, it has some symbolic value as a statement of societal expectations.⁵⁰ Where for example under the NIMC Act, there is a prohibition against duplication and sharing of personal data with third parties, an official having access duplicates the personal data and shares with a third party for gain. Such officer can be tried under the offence section of NIMC Act but can also be charged with committing the offence of criminal breach of trust.

5.1 Consequences of infringement of right to personal data

A. Constitutional

Data protection is becoming a standalone right. In addition to Article 7 of the Charter of Fundamental Rights of the European Union which upholds the right to privacy, Article 8 specifically provides for the protection of personal data.⁵¹ More countries such as Brazil

⁵⁰ Jessica Litman, 'Information Privacy/Information Property' (2000) 52 Stan L Rev 1283 @ 1312

⁵¹ 1. Everyone has the right to the protection of personal data concerning him or her.

2. Such data must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law. Everyone has the right of access to data which has been collected concerning him or her, and the right to have it rectified.

3. Compliance with these rules shall be subject to control by an independent authority.

and Columbia have the right to the protection of personal information entrenched in the constitution. In Nigeria, three types of constitutional actions can be maintained to enforce the right to data privacy: first, the right to privacy with respect to personal data is protected under section 37 of the Constitution. Where a data subject alleges that there has been a breach of her right to privacy, remedies could be sought through section 46 of the Constitution and Fundamental Rights (Enforcement Procedure) Rules, 2009.⁵² Second, a data subject can request the court to issue a writ of habeas data with respect to personal data. There is abundant wisdom to be drawn from Latin America on the law and policy of habeas data. This concept derives from due-process doctrine based on the writ of habeas corpus.⁵³ Third, data is an asset that is capable of being taken. When it is improperly taken from the data subject, there can be redress for the wrongful taking under section 44 of the Constitution. Despite the general popularity of notions of information control and information self-determination, these have usually not been viewed in terms of a person “owning” information about him-/herself, such that he/she should be entitled to, e.g., royalties for the use of that information by others. Concomitantly, property rights doctrines have rarely been championed as providing a desirable basis for data protection rules.⁵⁴

B. Civil sanctions

The liability for infringement on personal data rights is civil and criminal. Any person who is found to be in breach of the data privacy rights of any Data Subject shall be liable, in addition to any other criminal liability, a) in the case of a Data Controller dealing with more than 10,000 Data Subjects, payment of the fine of 2% of Annual Gross Revenue of the preceding year or payment of the sum of 10 million Naira, whichever is greater; b) in the case of a Data Controller dealing with less than 10,000 Data Subjects, payment of the fine of 1% of the Annual Gross Revenue of the preceding year or payment of the

⁵² Section 46 (2) of the Constitution provides: Subject to the provisions of this Constitution, a High Court shall have original jurisdiction to hear and determine any application made to it...may make such orders, issue such writs and give such directions as it may consider appropriate for the purpose of enforcement or securing the enforcing within that State of any right to which the person who makes the application may be entitled under this Chapter.

⁵³ See Lee A. Bygrave, Privacy and Data Protection in an International Perspective, Stockholm Institute for Scandinavian Law & Lee A Bygrave 2010 p. 169

⁵⁴ Lee A. Bygrave, Privacy and Data Protection in an International Perspective, Stockholm Institute for Scandinavian Law & Lee A Bygrave 2010 pp. 170/171

sum of 2 million Naira, whichever is greater.⁵⁵ The civil penalties prescribed in the NDPR are miniscule when compared with the European GDPR⁵⁶ it was modelled after. Unlike the GDPR, the NDPR does not explicitly outline what NITDA must consider when applying an administrative sanction.⁵⁷ The European Union GDPR presents as a regulation that will be readily enforced with judicial remedies made available in the regulation. The NDPR leans more towards its Administrative Redress Panel.⁵⁸

The Central Bank of Nigeria Consumer Protection Regulations require financial institutions to ensure data protection and privacy of consumers.⁵⁹ Institutions shall protect the privacy and confidentiality of consumer information and assets against unauthorized access, and be accountable for acts or omissions in respect thereof. The Regulation emphasizes consent of the consumer in all dealings with personal data. It imposes a penalty of N2,000,000.00 per complaint against the institution for non-acknowledgment of complaints from customer or non-issuance of tracking numbers.⁶⁰

In addition to the civil sanctions imposed by legislation, a data subject has a cause of action in negligence against a data controller that mishandles personal data by virtue of the duty of care imposed in Article 2.2 of NDPR.

C. Criminal sanctions

Any person who intentionally and without authorization or in excess of authority, intercepts by technical means, transmissions of non-public computer data, content data or traffic data, commits an offence and shall be liable on conviction to imprisonment for a term of not less than two years or to a fine of not less than N5,000,000.00 or to both fine and imprisonment.⁶¹ An unauthorized modification of computer data on conviction attracts an imprisonment for a term of not less than 3 years or to a fine of not less than N7,000,000.00 or to both fine and imprisonment.⁶²

⁵⁵ Paragraph 2.10 of the Regulation

⁵⁶ 2% of global annual turnover or €10 million, whichever is higher; or 4% of global annual turnover or €20 million, whichever is higher

⁵⁷ Comparing privacy laws: GDPR v. Nigeria Data Protection Regulation. OneTrust DataGuidance Available at: https://www.dataguidance.com/sites/default/files/gdpr_v._nigeria.pdf

⁵⁸ Article 4.2 of the Regulation

⁵⁹ Paragraph 5.4 of the CBN Consumer Protection Regulations 2020

⁶⁰ Ibid, Paragraph 7.2.

⁶¹ Section 7 of the Cybercrimes Act, 2015

⁶² Ibid, S. 8

One of the more serious offences in the field of data privacy and data protection in Nigeria is for a person to access data or information in the national identity database without lawful authorization. Such unlawful and unauthorized access, attracts on conviction, an imprisonment of not less than ten years without the option of a fine.⁶³

Breach or non-compliance with provisions of the regulation, Guideline or Framework is an offense under Section 17 of the NITDA Act 2007.⁶⁴ The NDPR creates a fiduciary relationship between the Data Controller and the data subject. One of the consequences of that legal relationship is that the data controller could be prosecuted for criminal breach of trust for the mishandling of the personal data of the data subject.

Under the National Health Act, failure of the person in charge of a health establishment who is in possession of a user's health records to set up control measures to prevent unauthorized access to those records and to the storage facility in which, or system by which, records are kept is an offence that is liable on conviction to imprisonment for a period not exceeding two years or to a fine of N250,000.00 or both.⁶⁵ Unlawful access to data or information in the National Identity Database attracts a penalty on conviction, to imprisonment for 5 (five) years or more or not less than N5 million fine or both A fine of N1, 000,000 (One Million Naira) on conviction 10 (ten) years imprisonment of the representative of the company & N10, 000,000 (Ten million Naira) fine on the corporate body for every instance of breach.⁶⁶

Amending/correcting and deleting records/ information from files, records, computer systems and/or the National Identity Database without the necessary approvals. All employees, licensee's & Enrollees 3 (Three) or more years Imprisonment or a fine of not less than N250,000 or both 3 Years imprisonment or N7 million fine or both.⁶⁷ Any person who being an enrollees, employees & licensee, records and sends false information into the database shall be liable on conviction to 3 (Three) or more years Imprisonment or a fine of not less than N250,000 or both.⁶⁸ It is important to note that

⁶³ Section 28 NIMC Act, 2007

⁶⁴ Section 17 (4) NITDA provides: Where a person or body corporate fails to comply with the guidelines and standards prescribed by the Agency in the discharge of its duties under this Act, such person or body corporate commits and offence. See also Paragraph 7.0 (a) of the Guideline

⁶⁵ Section 16 (1) of the National Health Act

⁶⁶ Section 6 (1) Cybercrime (Prohibition & Prevention Act) 2015 and S. 28 (3) NIMC Act & Regulations

⁶⁷ Section 28 (1) (A) & (2) NIMC Act and Section 13 Cybercrime (Prohibition & Prevention) Act 2015

⁶⁸ 28(1)(c) & (2) NIMC Act

even when the State opts for a criminal prosecution for breach of personal data, the Administration of Criminal Justice Act to make orders for victim compensation. The fact of a criminal prosecution does not lock the data subject out of remedies especially if the defendant profited from the misuse of the personal data.

6. Conclusion

The examination of the constitution and twelve data privacy related laws reveal that the issues of data privacy and data protection are in the growing stages in Nigeria. The two instruments that deal specifically with data protection are subsidiary legislation and most of the data privacy law pre-dated the specialized legislation. The laws made after the specialized data protection law however seek to integrate into the specialized law. In the light of the peculiarities of the socio-political environment, ownership of personal data is in certain specific databases vested in the state with incidents of ownership conferred in the data subjects.

What is apparent from the examination of the concept of personal data in Nigeria is that data protection is not being executed by design. The concept is that when a system for processing personal data is planned or envisaged, the requirements of data protection law are not applied as an afterthought but are integrated into all stages of the system's lifecycle, including its design and construction.⁶⁹ There needs to be a systematic alliance between legal and technical experts in order to have effective regulations. Nigeria should not position itself for digital exploitation.

There should be an intentional drive to empower its citizens not just to survive but to thrive in the digital economy. This requires data literacy skills which has been described to include the ability to ask and answer real-world questions from large and small data sets through an inquiry process, with consideration of ethical use of data, to select, clean, analyse, visualize, critique and interpret data, as well as to communicate stories from data and to use data as part of a design process.⁷⁰ Whether the data protection legal framework is human rights or market model should not be a zero-sum game for Nigeria. A hybrid

⁶⁹ Lee A. Bygrave, Data Protection by Design and by Default in S. Garben, L. Gromley, K. Purnhagen (eds.), Oxford Online Encyclopedia of European Union Law (Oxford University Press 2022)

⁷⁰ Wolff, A., Gooch, D., Caverio Montaner, J.J, Rashid, U., Kortuem, G., (2016). Creating an understanding of data literacy for a data-driven society. The Journal of Community Informatics, 12(3), 9-26. Available at: www.ci-journal.net/index.php/ciej/article/view/1286.

model that accommodates commercialization of personal data to the benefit of the corporation and the data subject and protects the human rights of individuals and groups should be implemented and enforced in Nigeria.