DATA PRIVACY PROTECTION AND THE RIGHT TO PRIVACY IN NIGERIA: AN ASSESSMENT OF THE NATIONAL INFORMATION TECHNOLOGY DEVELOPMENT AGENCY (NITDA) DATA PROTECTION REGULATIONS OF 2019

Dr. Shaba Sampson*, Kwame-Okpu Aghogho*

Abstract

Data Privacy is occasionally referred to as 'Information Privacy'. It builds on the established notion of privacy to regulate the relationship between the collection and dissemination of personal data, technology, the public expectation of privacy, as well as legal and political issues surrounding Data Privacy. This paper discusses the Data Protection Regulations of 2019 as issued by the National Information Technology Development Agency. It is the closest item in the Nigerian legal framework that adopts a deliberate and comprehensive approach to the issue of Data Privacy protection in the country. The paper found that the term Data Privacy, and Data Privacy protection in Nigeria are not only closely related but intertwined; andthe constitutional provision for privacy and the models of Data Privacy protection together with the Acts and Regulations which provide for Data Privacy protection all form one

* PhD (Unizik); Lecturer in the Faculty of Law, Federal University, Oye-Ekiti, Ekiti State. Email: sampsonshaba@gmail.com; phone: 08035048499.

** LL.M (ABUAD); LL.B (BIU); B.L; currently a PhD student at Afe Babalola University, Ado-Ekiti, Ekiti State. Phone: 08131160153.

stream of protective mechanism. Data Protection Regulations of 2019 is, no doubt, a commendable yet flawed attempted piece of legislation to regulate and provide for Data Privacy protection in Nigeria. The paper concludes that as it stands, the Data Protection Regulations of 2019 is a watershed in establishing protection standards for the rights of Data Subjects and the protection of personal data of natural persons in Nigeria.

Keywords: Data, Information, Privacy Regulation, Rights, Technology.

1. Introduction

The universally recognized right to privacy protects the individual from unauthorized intrusion, this right by extension protects the place of abode and information belonging to the individual. In Nigeria, the right to privacy is a Fundamental Right guaranteed under the Constitution of the Federal Republic of Nigeria 1999 (as amended), specifically in Section 37 which provides that "the privacy of citizens, their homes, correspondence telephone conversations and telegraphic communications is hereby guaranteed and protected."

This right envisages that unauthorised access to the person of or information about an individual is tantamount to an intrusion, which is a violation of the right. It is on the basis of this that several laws are passed to guard against these violations. With advancements in information communications technology (hereinafter 'ICT') and a data driven approach to communications, buying and selling, all of which impact everyday life, privacy in the digital age is besieged by new threats, threats beyond the

contemplation of the early privacy protection laws. These threats include; viruses and worms[1], collection of unnecessary data, data transfer over unsecured channels, unauthorized sharing of personal data, cyber-attacks[2], web tracking[3] and government surveillance. Data Privacy protection has had to develop in the area of privacy protection in a bid to combat these threats. Data Privacy protection regulates the relationship between the collection and dissemination of personal data, technology, the public expectation of privacy, the ability an individual has to determine what personal data in a computer system can be shared with third parties as well as legal and political issues surrounding Data Privacy. Data Privacy legislation creates rights for individuals often referred to as Data Subjects, obligations for data processors and controllers and sanctions for data processors and controllers who breach the rights of Data Subjects. The best Data Privacy protection regimes also create a supervisory agency to oversee an enforcement mechanism.

---

1 Viruses and worms are two of the most common forms of malicious software or malware. They can infect a system without the owner's consent and create duplicates of their codes that can spread to other programs and computers. The effects of these small programs can range from being mildly annoying to being critically damaging to entire databases and software. One of the most dangerous ways they threaten Data Privacy is by opening a backdoor on computer systems and software for attackers to access passwords, Internet Protocol addresses, banking information, and other personal data.

2 A major threat to privacy in today's digital world are the cybercriminals who target computer information systems, infrastructures, computer networks, or personal computer devices to expose, alter, disable, destroy, steal or gain unauthorized access to or make unauthorized use of information stored thereon.

3 A variety of internet companies and services can collect browsing data and share computer address with third-party advertisers and companies. With this data companies that have no direct interaction with an individual can build up a pretty good profile of the individuals internet habits and web browsing. This can turn out to be particularly invasive.

2. Protection of Personal Data: Arriving at a Terminology

There is a difficulty among scholars to select the appropriate terminology to describe this *sui generis* protection afforded personal information[4]. While some scholars prefer to use the term 'privacy' or 'information privacy', others use the term 'data protection'[5]. Recently, there has come to be the increased usage of another term 'Data Privacy' among researchers and scholars in the field of study. The phrase even finds its way into the Nigerian Data Protection Regulations (hereinafter 'NDPR'). It also appears in the works of revered scholars in the field. In explaining his preference for the term 'Data Privacy', Bygrave argues the term (Data Privacy) reduces the over-inclusion problem associated with the term 'privacy'[6], and it communicates better the central interests at stake. Based on this argument by Bygrave alongside the ease at which the term Data Privacy embodies the protection of personal information by fusing the words data and privacy together, this paper will adopt the term 'Data Privacy'.

3. Models of Data Privacy Protection

There are primarily four models of Data Privacy protection, namely; sectoral laws, comprehensive laws, self-regulation and the use of technology based systems. Of the four models, sectoral laws and comprehensive laws are the major avenues through which

---

4 LukmanAdebisiAbdulrauf, 'The Legal Protection Of Data Privacy In Nigeria: Lessons From Canada And South Africa' [2015] <*https://repository.up.ac.za/bitstream/handle/2263/53129/Abdulrauf_Legal_2016.pdf?sequence=1*> accessed 10February2020

5 *Ibid*

6 L.A Bygrave 'Data privacy law: An international perspective'[2014] <*http://www.oxfordscholarship.com/view/10.1093/acprof:oso/9780199675555.001.0001/acprof-9780199675555*> accessed 10January2020

legal frameworks on Data Privacy are built because they involve the making of laws. Self-regulation is utilized by companies and industries who establish codes of practice to make sure their respective operations do not violate Data Privacy. Technology based systems refer to the protection employed by individuals to protect their data; these include anti-spyware, anti-virus scanners and encryption.

4. Data Privacy Protection in Nigeria

In 2016, the United Nations Conference on Trade and Development (hereinafter 'UNCTAD') observed that the number of national data protection laws has grown rapidly, but major gaps persist. Some countries have no laws in this area, some have partial laws, and some have laws that are outdated and require amendments[7]. Nigeria falls into the last two categories. Currently, Nigeria has no legislation that deliberately provides for thorough and comprehensive data protection principles. The approach to data protection in Nigeria is one that favours a sectoral model[8]; it is therefore made up of sector specific regulations and legislations that by virtue of their provisions have a bearing on Data Privacy. The resultant effect is that Data Privacy protection in Nigeria is a complex maze of disconnected policies and laws which when taken together fall short of achieving the required standard. This standard is encapsulated in the Fair Information Principles

---

[7] United Nations Conference On Trade And Development, 'Data protection regulations and international data flows: Implications for trade and development'[2016]<*https://unctad.org/en/PublicationsLibrary/dtlstict2016d1en.pdf*> accessed 10February2020

[8] Folabi Kuti, Ugochukwu Obi, Seth Azubuike, 'Nigeria' in Alan Charles Raul (ed) The Privacy, Data Protection and Cyber security Law Review- Edition 4 (The Law Reviews, 2017), 50-66

(hereinafter 'FIPS')[9], which are a set of standards governing the collection and use of personal data and addressing issues of privacy and accuracy. It appears across jurisdictions and can be found in the best data privacy protection laws. Although there is in existence the NDPR which is the closest item in the Nigerian legislative framework resembling a comprehensive Data Privacy protection effort, problems still exists with Data Protection in Nigeria, for example, there is yet to be established an independent supervisory authority tasked with overseeing Data Privacy protection in Nigeria. When these shortcomings are considered alongside the growing rates at which the citizens of the country use ICT to engage in social, economic and cultural activities, it raises the question as to how effectively these transactions and interactions that involve so much personal information are processed and safeguarded., because at the end of the day, poor and unlawful processing of personal information has human right implications and touches upon the constitutionally guaranteed right to privacy. Also, due to globalization, Nigeria and its citizens

[9] These principles, known as the Fair Information Principles or Fair Information Practices (FIPs), are a set of standards governing the collection and use of personal data and addressing issues of privacy and accuracy FIPs appear across jurisdictions and can be found in the various data privacy protection laws. The principles are as follows: Principle 1: Personal data must be processed fairly and lawfully; Principle 2: Personal data shall only be used in accordance with the purposes for which it was collected; Principle 3: Personal data must be adequate, relevant and not excessive; Principle 4: Personal data must be accurate and where necessary kept up to date; Principle 5: Personal data must be kept for no longer than is necessary; Principle 6: Personal data must be processed in accordance with the rights of Data Subjects; Principle 7: Appropriate technical and organizational measures must be established to protect the data; Principle 8: Personal data must not be transferred outside a jurisdiction unless adequate provisions are in place for its protection.

form part of the ever expanding international market involved in the delivery of goods and services, and with a robust legal framework in place Nigerian citizens will be safeguarded from brazen acts of Data Privacy violations by Shylock corporations.

5. An Overview of the Current Legal Framework for Data Privacy Protection in Nigeria

The entire gamut of laws on a specific subject is referred to as the legal framework. A legal framework comprises a broad system of rules, procedures, which govern and regulate particular subjects in a given jurisdiction[10]. In Nigeria the protection of Data Privacy is largely dependent on the protection of privacy itself. Consequently the reality is that the legal framework for Data Privacy protection in Nigeria primarily consists of the constitutional framework for the protection of privacy in Nigeria.[11] In addition to the Constitution of the Federal Republic of Nigeria 1999 (as amended), the legal framework for data Privacy protection in Nigeria is comprised of the following:

i. The Credit Reporting Act (hereinafter CRA) of 2017. The CRA provides a platform for "credit information providers" to provide credit bureaus with information relating to 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. The credit bureau may then share such information with "credit information users" that satisfy certain conditions. From the above, it is clear that CRA contains provisions that impact upon Data Privacy, therefore it is unsurprising

[10] Iheanyi Samuel Nwankwo, 'Information Privacy in Nigeria', in Alex Makulilo (ed), *Africa Data Privacy Laws* (Springer: 2016) 45

[11] S. 37 Constitution of the Federal Republic of Nigeria (CFRN) 1999 (as amended). this section provides for the right to private and family life.

that Section 9 of the Act reiterates the rights of Data Subjects (i.e. persons whose credit data are held by a credit bureau) to the privacy, confidentiality and protection of their credit information, and prescribes the preconditions under which Data Subjects' credit information may be disclosed. Also Section 5 of the Act requires credit bureau to maintain credit information for at least six years from the date on which such information was obtained, after which the information should be archived for a further period of 10 years. It may thereafter be destroyed by the credit bureau.

ii. Cybercrimes (Prohibition, Prevention, Etc) Act 2015. The Cybercrimes Act has as its general purpose the prevention and prosecution of cybercrimes. Section 38 (1) of the act places a duty on computer and mobile network and communication service providers to retain traffic data and subscriber information for a period of two years. Section 38(2) (5) also requires such service providers to have regard to the individual's right to privacy under the Constitution and to take measures to safeguard the confidentiality of data processing for the purpose of law enforcement. Section 37 of the Cybercrimes Act mandates financial institutions to put in place effective measures to safeguard the sensitive data of their customers.

iii. The National Identity Management Commission (hereinafter 'NIMC') Act of 2007 which provides for the establishment of a National Identity Database and the NIMC to be charged with the responsibilities for maintenance of the National Database, the registration of individuals, and the issuance of general Multi-purpose

Identity Cards; and for related matters[12]. By virtue of this mandate, the NIMC Act regulates one of the biggest entities in Nigeria handling personal information.

iv. Terrorism (Prevention) Act 2011 (as amended): This Act was originally passed into law in 2011. It was amended in 2013 by Terrorism (Prevention) (Amendment) Act 2013 which provided for extra-territorial application of the Act and strengthening of terrorist financing offences; and for related matters. The Act amongst other things prohibits acts of terrorism, proscribes organizations comprising two or more persons associated for the purpose of engaging, participating or collaborating in an act of terrorism or promoting, encouraging or exhorting others to commit an act of terrorism[13]. In addition to the Cyber Security Act, the Act creates a regime for intelligence gathering in Nigeria. To this end, the provision for intelligence gathering under Section 29 authorizes communications surveillance in Nigeria for purposes specified in the Act.

v. The Freedom of Information Act: The objective of the Act is to ensure that the public is not denied access to public information. However, the Act sets out private information as an exemption (although it may be requested by the public), thereby ensuring privacy of personal information.

Ministries, and statutory agencies established by law in Nigeria are sometimes empowered to make regulations that would in addition to any legislation apply to and govern their sphere of operations. Regulations made in pursuance of that power are called subsidiary

[12] NIMC Act Preamble, Section 1.

[13] Terrorism (Prevention) Act 2013 (as amended) Section 2 .

legislations. A subsidiary legislation has been defined by the Interpretations Act 1964[14] as any order, rules/regulations rules of court or bye-laws made in exercise of powers conferred by an Act. Subsidiary legislations have also been judicially defined by the Court of Appeal in *Njoku v Iheanatu,* that "a subsidiary legislation is made or enacted under and pursuant to the power conferred by a principal legislation or enactment. It derives its force and efficacy from the principal legislation…"[15] In Nigeria, it is not uncommon to see sector specific regulations and directives affecting Data Privacy by the National Communications Commission (hereinafter 'NCC')[16], the Central Bank of Nigeria (hereinafter CBN)[17] and the National Information Technology Development Agency (hereinafter NITDA)[18]. These sector specific regulations also form part of the Nigerian legal framework on Data Privacy protection.

i. The NCC Consumer Code of Practice Regulations, 2007 for telecommunication service providers. This Code applies only to providers of communication services in

[14] The Interpretation Act, CAP I23 LFN 2004.

[15] [2007] (CA/PH/EPT/454/2007), [2008] LPELR-3871 (CA).

[16] The NCC is the regulatory body for the telecommunications industry in Nigeria established in 2003. Pursuant to the powers conferred by Section 70(1) (g) of The National Communications Commission Act 2003, the NCC published the NCC Consumer Code of Practice Regulations 2007 for telecommunication service providers.

[17] The CBN can make subsidiary legislation in exercise of powers conferred on it by Section 51 of the CBN Act of 2007 (as amended) and Section 55 of the Banks and Other Financial Institutions Act of 2007, (as amended).

[18] The National Information Technology Development Agency (NITDA) was established by the NITDA Act, 2007 as the statutory agency with responsibility to develop information technology in Nigeria. Section 6 of the act authorizes the NITDA to develop guidelines for electronic governance and to monitor the use of electronic data interchange. The NITDA Data Protection Regulations were issued pursuant to this mandate.

Nigeria. It sets out principles to regulate the collection and maintenance of consumers' personal information and requires such service providers to ensure the protection of such information. The Code further requires telecommunication companies to implement appropriate policy to ensure proper collection, use and protection of consumer information, and to ensure that third parties with whom telecommunication companies transact with have adopted appropriate measures for the protection of consumer information.

ii. The NCC Registration of Telephone Subscribers Regulation (hereinafter 'RTS'), 2011 applicable to telecommunications companies. The RTS as a subsidiary legislation was introduced to command the compulsory registration of SIM Cards so as to make data available for the NCC and to assist security agencies combat scams, kidnapping-related offences, terrorist activities, *etcetera.* The provisions that have an impact on Data Privacy are mere safeguards that in operation protect Data Privacy. Data Privacy is not the actual business of the regulations and the RTS is therefore inadequate to protect and fulfill privacy expectations including data protection, dignity and other fundamental rights of subscribers.

iii. The CBN Consumer Protection Framework, 2016. This subsidiary legislation imposes a burden on financial institutions to maintain the confidentiality and privacy of all financial services rendered to customers present or past. Appropriate data protection measures and staff training programs are to be put in place to prevent unauthorized access, alteration, disclosure, accidental loss or destruction of customer data. Financial services

providers are also required to obtain the written consent of consumers before their data is shared with third parties or used for promotional offers.

5.1. National Information Technology Development Agency Data Protection Regulations, 2019

The Nigeria Data Protection Regulation was issued in August 2019 pursuant to the mandate given to the NITDA by Section 6(c)) of the NITDA Act. As a regulation, the NDPR applies to all transactions intended for the processing of personal data and to actual processing of personal data notwithstanding the means by which the data processing is being conducted or intended to be conducted and in respect of natural persons residing in Nigeria or residing outside Nigeria but of Nigerian descent. This makes the NDPR the only item in the Nigerian Data Privacy protection framework that is concerned primarily with data protection.

Part two of the NDPR, contains the NDPR's manifestation of the FIPs. The issue of consent as it relates to the collection and processing of personal data is topical, it is therefore worth noting that the NDPR contains decent provisions on it. To this end they are provided for under Section 2.3 of the NDPR. The NDPR strives to meet international standards in the sphere of Data Privacy protection. so apart from directing that data be collected and processed in accordance with the FIPs, the guidelines dedicate Section 1.3 to important definitions of consent[19], data[20], personal

[19] Under the NDPR, Consent means any freely given, specific, informed and unambiguous indication of the Data Subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her. NDPR Section 1.3 (c)

[20] Under the NDPR, Data means characters, symbols and binary on which operations are performed by a computer. Which may be stored or transmitted

data[21], personal data breach[22],sensitive personal data[23], Data Subject[24], data controllers[25], processing[26] all of which are important towards the proper protection of Data Privacy. In a bid to adequately regulate the collection and processing of personal information in Nigeria, the NDPR in Section 2.5 directs any medium through which personal data is being collected or processed to display a simple and conspicuous privacy policy in

in the form of electronic signals is stored in any format or any device. NDPR Section 1.3 (d)

[21] Under the NDPR, Personal Data means 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, and other unique identifier such as but not limited to MAC address, IP address, IMEI number, IMSI number, SIM and others. NDPR Section 1.3 (q)

[22] Under the NDPR, Personal Data breach means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed. NDPR Section 1.3(s)

[23] Under the NDPR, 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. NDPR Section 1.3 (v)

[24] Under the NDPR, Data Subject means an identifiable person; one who can be identified directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity. NDPR Section 1.3 (k)

[25] Under the NDPR, Data Controller means any person, public authority, Agency or any other body which alone or jointly with others, determines the purposes and means of the processing of personal data. NDPR Section 1.3 (g)

[26] Under the NDPR, Processing means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by

line with the NDPR which the class of Data Subjects that is being targeted can understand[27]. The NDPR directs that the privacy policy shall in addition to any other relevant information contain the Data subject's consent, personal information, purpose data is sourced, the technical method for collection and storage, condition for access by third parties, available remedies in the event of violation of any privacy policy[28], the time frame for remedy, and any limitation clause (provided that no limitation clause shall avail any Data Controller who acts in breach of the principles set out in section 6).

The NDPR also provides for requirements that data controllers should abide by in deciding whether, personal data should be transferred outside Nigeria. According to the Regulations:

> Any transfer of personal data which are undergoing processing or are intended for processing after transfer to a foreign country or to an international organisation shall take place subject to the other provisions of this Regulation and the supervision of the Honourable Attorney General of the Federation (hereinafter HAGF).[29]

Generally, the effect of the above provision is that personal data cannot be transferred outside Nigeria unless subject to the above provisions under the supervision of the HAGF. However, where the Data subject consents to the proposed transfer, if required to

---

transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction. NDR Section 1.3 (r)

27 This directive ought to be complied within three months of the issuance of the NDPR (NDPR Section 3.1).

28 NDPR, S. 5(g).

29 NDPR, S. 2.11(a-e).

meet certain objective such as conclusion of contract or, necessary in the interest of the public, or for a legal or defence or, for the protection of the data subject himself or other persons the above requirements making the transfer subject to the supervision of the AGF may be dispensed with.[30]

Part three of the NDPR clothe Data Subjects with specific rights with respect to any information connected to their personal data. Under the Regulations, a Data subject entitled to be provided with information affecting his interest in writing; the protection of his data where ever it is transferred; the right to rectify or delete any incorrect data concerning him without any delay.[31]

By virtue of Section 3.2.1, a breach of any of the above rights entitles the Data Subject to approach the Administrative Redress Panel (hereinafter ARP) established by the NITDA under the NDPR. The ARP is empowered under Section 3.2(a) to administratively determine issues arising from the NDPR without prejudice to the right of a Data Subject to seek redress in a court of competent jurisdiction. This provision has been lauded as a "novel input…considering the technical nature of data protection which makes it practically impossible for regular courts to resolve myriads of complaints brought by Data Subjects in a timely and efficient manner"[32] The rights of Data Subjects are central to effective Data Privacy protection, an importance that is visibly manifested in one of the FIPs. So it is commendable that the NDPR creates rights for Data Subjects as well as an avenue to seek

---

30 *Ibid*, S. 2.12.

31 *Ibid*, s. 2.13.

32 Femi Daniel 'Issues Arising from the Nigerian Data Protection Regulation 2019 (Part 2)' [2019] <*https://dnllegalandstyle.com/2019/issues-arising-from-the-nigerian-data-protection-regulation-2019-part-1-femi-daniel/*:> accessed 31 January 2020

redress in the event of violation. Anyone found to be in breach of the data privacy rights of any Data Subject is liable under the NDPR. By the provision of Section 2.10, such a person shall, in addition to any other criminal liability be liable to:

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 sum of two million naira whichever is greater

On the issue of implementation, the NDPR in Section 3.1.2 directs every Data Controller to designate a Data Protection Officer (hereinafter 'DPO') for the purpose of ensuring adherence to the Regulation, relevant data privacy instruments and data protection directives of the data controller, to facilitate adherence the NDPR permits a data controller to outsource data protection to a verifiably competent firm or person. In a bid to ensure that the level of protection afforded is not stagnant, Section 3.1.3 of the NDPR directs a Data Controller or Processor to ensure continuous capacity building for her DPOs and the generality of her personnel involved in any form data processing. To further ensure implementation, Section 3.1.4 gives the NITDA the power to license Data Protection Compliance Organisations (hereinafter 'DPCOs') who shall on behalf of the NITDA monitor, audit, conduct training and data protection compliance consulting to all Data Controllers under this Regulation. The NDPR provides that the DPCOs shall be subject to Regulations and Directives of NITDA issued from time to time. However commendable these provisions appear on paper, it is quite

early to reach a decision on how effective they are in practice considering that the Regulations were issued barely over seven months ago.

It is trite that a law is only as good as its enforcement mechanism, it must be noted that in this area, the NDPR does not match up with the best Data Privacy protection legislation all of which create a supervisory authority The NDPR does not create a supervisory authority despite making an overt reference to one in Section 2.11 (d).The NDPR does however designates the NITDA or any other statutory body or establishment having government mandate as relevant authority for the purpose of the Regulation and to deal solely or partly with matters relating to personal data.[33]

6. Shortcomings of the Nigerian Data Protection Regulation

With regard to its provisions the NDPR falls short in several instances. Firstly, the Guidelines fail to provide for personal data processing operations concerning public security, defense, national security and the activities of the nation in areas of criminal law. An issue also arises in the area of enforcement, while the NITDA Act[34] empowers the NITDA to in conjunction with the Standards Organization of Nigeria enforce the guidelines which it issues, the absence of a specialized supervisory authority or office tasked with enforcement, is a huge drawback to effective implementation.

In the event of a breach of its provisions excluding the provision for the rights of Data Subjects, the NDPR fails to create corresponding penalties for breaches, instead there is a provision in Section 3.22 to the effect that any breach of this Regulation shall be construed as a breach of the provisions of the NITDA Act of

[33] NDPR Section 1.3(u)

[34] NITDA Act Section 17(5)

2007and the Guidelines issued under that Act. The NITDA Act in Section 16 (1) (a) and (b) provides for liability of up to N200, 000 or imprisonment for a term of three years or both; such fine and imprisonment for breach of guidelines and standards issued by NITDA for a second and subsequent offence, to a fine of N 500,000.00 or to imprisonment for a term of 3 years or to both such fine and imprisonment.

7. Intersecting NITDA Data Protection Regulation of 2019 with the Right to Privacy

The inception of human society triggered a revolution in the aspect of information. Since then, information is considered one of the most important and priced assets any member of the society can possess. Therefore, man continuously strives to ensure the protection of information from those who may want to take advantage and manipulate it in a way and manner that is injurious to others. Following the invention and access to the internet and the World Wide Web (www),[35] the ability to gain access to information has increased exponentially, leading to the need for a more detailed and comprehensive mode of protection of information or, as it is presently known, 'data'.

Nigeria is a member of the international community and an active participant in global affairs. With the world becoming a global

[35] The World Wide Web was invented by Sir Tim Berners-Lee a British computer scientist in 1989. He was born in London, and his parents were early computer scientists, working on one of the earliest computers. Growing up, Sir Tim was interested in trains and had a model railway in his bedroom. After graduating from Oxford University, Berners-Lee became a software engineer at CERN, the large particle physics laboratory near Geneva, Switzerland. Scientists come from all over the world to use its accelerators, but Sir Tim noticed that they were having difficulty sharing information.

village, couple with the size of Nigeria's population and her status as a developing country, the need to manage, monitor, regulate, *etcetera*, the flow of information within her territory had, of necessity, arisen hence the enactment of the NITDA Act in 2007 and the NITDA Data Protection Regulation of 2019.

These enactments raise the question: whether these legislations are infringement on the provisions of section 37 of the Constitution of the Federal Republic of Nigeria which protects the right to privacy.[36] In doing this, it is important first of all, to examine the import and objectives of the NITDA Act and the NITDA Data Protection Regulation. It is also apposite to assess the statutory stand point on the provision of section 37 CFRN and the relationship between these three pieces of legislation.[37]

7.1 The National Information Technology Development Agency (NITDA) Act 2007

The NITDA Act of 2007 is an agency-establishing Act. In other words, its enactment was for the establishment of the National Information Technology Development Agency.[38]Though the operations of NITDA started in 2001, six years before the Bill was passed into law, the agency was commissioned in 2007 following the signing into law of the NITDA Bill.[39]

---

[36] CFRN (as amended) s. 37 is in Chapter IV and thus a fundamental right which abhors any form of infraction except through the due process of the law.

[37] That is the NITDA Act, the Regulations and section 37 CFRN 1999 (as amended).

[38] NITDA Act 2007 (Pt. 1), section 1

[39] Wikipedia, 'National Information Technology Development Agency', <*https://en.wikipedia.org/wiki/National_Information_Technology_Development_Agency*>, accessed March 19, 2020.

The Explanatory Memorandum[40] to the Act states that 'this Act established the National Information Technology Development Agency to plan, develop and promote the use of Information technology in Nigeria.' Some of the powers conferred on the NITDA by the Act include, to create a frame work for the planning, research, development, standardization, application, coordination, monitoring, evaluation and regulation of Information Technology practices, activities and systems in Nigeria and all matters related thereto and for that purpose, and which without detracting from the generality of the foregoing, shall include providing universal access for Information Technology and systems penetration including rural, urban and under-served areas.[41] It also empowers NITDA to provide guidelines to facilitate the establishment and maintenance of appropriate information technology and systems application and development in Nigeria for public and private sectors, urban-rural development, the economy and the government.[42]

According to the Act, the NITDA has the mandate to develop guidelines for electronic governance and monitor the use of electronic data interchange and other forms of electronic communication transactions as an alternative to paper-based methods in government, commerce, education, the private and public sectors, labour, and other fields, where the use of electronic communication may improve the exchange of data and information.[43]

7.2 NITDA Data Protection Regulation 2019

40 The NITDA Act 2007.

41 *Ibid*, part 1, section 6(a).

42 *Ibid*, part 1, section 6(b).

43 *Ibid*, part 1, section 6(c).

According to the preamble of the NITDA Data Protection Regulation 2019[44], the Agency, following the mandate by section 6(c), recognizes that information systems have become critical information infrastructure which must be safeguarded, regulated and protected against atrocious breaches. It noted the relevance for protection over information generally and data privacy and the imperativeness of the emerging data protection regulations within the international community geared towards security of lives and property. In order to foster the integrity of commerce and industry in the volatile data economy, as well as being conscious of the concerns and contributions of stakeholders on the issue of privacy and protection of Personal Data against grave consequences usually occasioned by unregulated Personal Data processing all added up in favour of this regulation in addressing these challenges.

The objectives of this Regulation are, among others to safeguard the rights of natural persons to data privacy[45]; to foster safe conduct for transactions involving the exchange of Personal Data[46]; to prevent manipulation of Personal Data[47]; and, to ensure that Nigerian businesses remain competitive in international trade through the safe-guards afforded by a just and equitable legal regulatory framework on data protection and which is in tune with best practice[48].

8. Constitutional Provision on the Right to Privacy (Section 37 CFRN 1999 (as amended)

44 Herein called the 'Regulation'.

45 NITDA Data Protection Regulation 2019, Part one, section 1.1 (a).

46 *Ibid*, section 1.1(b).

47 *Ibid*, section 1.1 (c).

48 *Ibid*, section 1.1 (d).

Chapter IV of the 1999 Constitution of the Federal Republic of Nigeria contains provisions on fundamental rights. These rights originate from the International Covenant on Civil and Political Rights of 1966[49]. These are rights that are considered inalienable and inherent to all human beings simply for being part of humanity. These rights include the right to life and liberty, freedom from slavery and torture, freedom of opinion and expression, the right to private and family life, and many more[50].

Of these rights, the right to private and family life is our primary concern for the purpose of this paper. The tenor, apt and the terse tone of the provision of s.37 does not leave any one in doubt of the sanctity of information, held or shared and the integrity of the family institution. The section provides that the privacy of citizens, their homes, correspondence, telephone conversations and telegraphic communications is hereby guaranteed and protected. Similarly, the ICCPR provides on this same right as follows:

> No one shall be subjected to arbitrary or unlawful interference with his privacy, family, home or correspondence, nor to unlawful attacks on his honour and reputation. Everyone has the right to the protection of the law against such interference or attacks.[51]

---

[49] ICCPR, 1966 particularly, Part III articles 6 to 27.

[50] United Nation, 'Human Rights',<*https://www.un.org/en/sections/issues-depth/human-rights/*>, accessed March 20, 2020. The gist about these rights and their safeguards are contained in sections 33 to 46 of the Constitution of the Federal Republic of Nigeria 1999 (as amended).

[51] ICCPR, Article 17. This provision is similar to the Universal Declaration of Human Rights of 1945, Article 12.

The European Convention on Human Rights (ECHR) on the hand states that "everyone has the right to respect for his private and family life, his home and his correspondence."[52] This right not only operates to protect the individuals' privacy within the confines of what is lawful, it more importantly enhances the humanity of mankind which is a necessary product of freedom. It affords the individual the opportunity to protest against unlawful searches, entry into private premises for whatever purpose, confiscation of personal information, the bursting and tapping of personal information gadgets, *etcetera,* by the government and its agencies.[53] The elements of this right in its elaborate form includes, privacy of the individual which protects an individual against unlawful invasive procedures such as drug testing, blood testing; privacy of the home: which includes protection from unlawful entry or harassment of an individual's home; and privacy of correspondence, conversations and communications: it also protects the privacy of an individual's mail, telephones conversations, email and other forms of communication.[54] No doubt, the practice and application of this right peculiarly differ from state to state, and most often than not fluctuates over period of time, especially in the areas of state security, public order, the protection of confidential and secrete information, *etcetera*[55].

---

[52] ECHR, Article 8(1).

[53] E. A. Oji, 'Right to Private and Family Life and Right to Freedom of Thought, Conscience and Religion (Sections 37 and 38 of the 1999 Constitution)', in O Okpara (ed) *Human Rights Law & Practice in Nigeria Vol. 1* (Chenglo Ltd., 2005) 230.

[54] '11 Rights Every Nigerian Should Know About',<*https://lawpadi.com/11-rights-every-nigerian-should-know-about/*>, accessed March 20, 2020.

[55] D Voorhoof, 'The European Convention on Human Right: The Right to Freedom of Expression and Information restricted by Duties and Responsibilities in a Democratic Society', [2015] <*https://www.researchgate.net/publication/294124628*>*3.*Accessed on

Privacy of the human person is one right that is of utmost sensitivity and unqualified importance. Notwithstanding, the Constitution allows a derogation on this provision in deserving situation in the interest of defence, public safety, public order, public morality or public health. It may also be derogated on for the purpose of protecting the rights and freedom of other persons;[56] interferences by public authorities may also be justified to protect the secrete character of confidentiality of certain classified communications, information or data.[57]

However, every of such derogation by the authorities must not be arbitrarily or unlawfully carried out. They must conform and follow constitutional provisions or safeguards which are considered permissible by law and acceptable in a democratic society. This requirement serves as a fortification mechanism to the privacy provision against unlawful and unwanted incursions into the private lives of persons by foreign agents. The implication of this is that any interference based on a law properly enacted by a body with power to so do, in this case the National Assembly, becomes lawful and non-arbitrary and therefore not an infringement on the right to privacy.[58] It also follows that where a person gives permission for the invasion of his privacy, such interference would not necessarily be seen as an infringement of the person's privacy.

13/07/2020.

56 CFRN 1999 (as amended), s.45(1)(a & b).

57 Voorhoof, (n.55) p.17.

58 *Ibid*, s.45(2)

Section 45 of the CFRN sets out situations and circumstances under which the derogation from the provisions of sections 37[59], 38[60], 39[61], 40[62] and 41[63] of the same constitution is considered to be reasonably justifiable in a democratic society[64]. These derogations include that the provision of right to life shall not invalidate any law that is reasonably justifiable in a democratic society in the interest of defence, public safety, public order, public morality or public health or for the purpose of protecting the rights and freedom or other persons.[65]

9. NTDA Act, NITDA Data Protection Regulation and Section 37 of the CFRN

On the question whether the NITDA Act and its data protection regulation pose as infringements on the right to privacy as provided for by section 37 CFRN, an understanding of how these two statutes view privacy and its need for protection would shed some useful light.

The NITDA Act, being an agency establishing Act, does not categorically state the mandates or provisions regarding the data privacy of a person. It, however, has the ability to develop

---

59 Right to private and family life.

60 Right to freedom of thought, conscience and religion.

61 Right to freedom of expression and the press.

62 Right to peaceful assembly and association.

63 Right to freedom of movement.

64 Exceptions to the inviolability of these rights come to the fore during emergency and the processes must comply with relevant laws to ensure that the citizens are not unduly shortchanged of their fundamental rights.

65 CFRN, Section 45(1) (a and b). Articles 8(2) and 10(2) of the European Convention on Human Rights of 1950 (which came into force in 1953) has a similar provision. See also article 4(1&2) ICCPR 1966.

guidelines for electronic governance and monitor the use of electronic data interchange and other forms of electronic communication transactions as an alternative to paper-based methods in government, commerce, education, the private and public sectors, labour, and other fields, where the use of electronic communication may improve the exchange of data and information.[66]

To achieve these goals, it created the NITDA Data Protection Regulation of 2019, as afore mentioned. This regulation however does contain provision with regard to the privacy of persons. Section 1.1(a) has, as one of its objective, the responsibility to safeguard the rights of natural persons to data privacy. It also categorically provides that this Regulation shall not operate to deny any Nigerian or any natural person the privacy rights he is entitled to under any law, regulation, policy or contract for the time being in force in Nigeria or in any foreign jurisdiction, within its purview.[67] It also aims to foster safe conduct for transactions involving the exchange of Personal Data, as well as, to prevent manipulation of Personal Data.[68]

The regulation also stipulates among its governing principles that Personal Data shall be collected and processed in accordance with specific, legitimate and lawful purpose consented to by the Data Subject.[69] It also explains what constitute lawfully processing, adding, *interalia*, that the Data Subject has given consent to the processing of his or her Personal Data for one or more specific

---

66 NITDA Act 2007, section 6(c).

67 NITDA Regulation, section 1.2(c).

68 *Ibid*, section 1.1 (b)&(c).

69 *Ibid*, section 2.1.

purposes[70], which must state the means of procuring consent from a Data Subject.

From the above, it is clear that the NITDA, through its regulation, is extremely particular on the subject of the prevention of and protection from the infringement on the right of data privacy. The regulation has provided for measures to protect the data of both natural persons and otherwise. In order to stress this point, the regulation provides for the advancement of right to privacy by stating that:

> Notwithstanding anything to the contrary in this Regulation, the privacy right of a Data Subject shall be interpreted for the purpose of advancing and never for the purpose of restricting the safeguards Data Subject is entitled to under any data protection instrument made in furtherance of fundamental rights and the Nigerian laws.[71]

10. Conclusion

It has been stated that the NITDA Act of 2007 is an agency-establishing Act that bestows the power to create regulations as it deems fit, which led to the creation of the NITDA Data Protection Regulation of 2019. It has also been established from the point above that these statutes do not infringe on the right to privacy as provided for by section 37 of the 1999 Constitution of the Federal Republic of Nigeria. However, they do, in their own way, contribute to the protection and safeguarding of the right to privacy. These regulations are necessary to the growth and

---

70 *Ibid*, section 2.2.

71 *Ibid*, section 2.9.

efficiency of the Nigerian information, technology and telecommunication sectors.

In light of the above, the NDPR which arrived rather late represents a commendable yet flawed attempt to regulate and provide for Data Privacy protection in Nigeria. While serving as a watershed in establishing protection standards, rights of Data Subjects and protecting the personal data of natural persons in Nigeria, the implementation of the provisions of this regulation is however, still a far cry from the intendments of the drafters as realities show.