THE NIGERIAN JURIDICAL REVIEW

FACULTY OF LAW
UNIVERSITY OF NIGERIA, ENUGU CAMPUS

ISSN: 2651-6055 Journal Homepage: https://www.tnjr.uneclaw.ng

Strengthening the Legal Framework for Personal Data Protection in Nigeria

Festus Okechukwu Ukwueze

To cite this article: Festus Okechukwu Ukwueze 'Strengthening the Legal Framework for Personal Data Protection in Nigeria' (2020-2021) 16 *The Nigerian Juridical Review*, pp 124 – 142.

To link to this article: https://doi.org/10.56284/tnjr.v16i1.16

STRENGTHENING THE LEGAL FRAMEWORK FOR PERSONAL DATA PROTECTION IN NIGERIA

Festus Okechukwu Ukwueze*

Abstract

Advancement in Information Communication Technology (ICT) has brought to the fore the need for the protection of individuals' personal data. In today's digital age, the personal data of individuals are routinely collected and stored in databases of both private and public establishments. Such personally identifiable information can easily be analyzed with fascinating accuracy, rapidly transmitted, and put to unimaginable uses. This situation has placed the regulation of personal data collection and uses on the front burner in many nations. The weak or total absence of regulation of personal data poses serious challenges to the security of lives and property of individuals and can constitute a serious disincentive for the adoption of beneficial technology. Employing the doctrinal methodology, this article examines the legal framework for personal data protection in Nigeria with the aim of assessing the adequacy or otherwise of relevant extant regulations in protecting the personal data of Nigerians and other people doing business in Nigeria. Looking at the state of the law in some developed and developing countries, the paper notes that the current state of regulation in Nigeria is still a far cry from what obtains in most countries of the global North and some sister African countries. It, therefore, concludes that there is a compelling need for a stronger regulatory framework for data privacy in Nigeria.

Keywords: Right to Privacy, Personal Data Protection, Rights of Data Subject, Personal Data Protection Regulation, Nigeria Data Protection Regulation 2019

1. Introduction

Digitisation and information communication technology have simplified the collection, storage and dissemination of information.[1] Buying and selling of goods and services, banking and other financial transactions are increasingly being conducted online. Nigeria has joined the rest of world to embrace the multifarious uses of digital and telecommunications technology, with the attendant benefits which include lower costs, speed and convenience and the associated challenge of the security of individual's personal data.[2] With modern computing technology, data can be collected and analysed with fascinating

* LLB, LLM, PhD (Nig), Senior Lecturer, Department of Commercial and Corporate Law, University of Nigeria, Nsukka. E-mail: festus.ukwueze@unn.edu.ng.

[1] M Nuruddeen, 'An Appraisal of the Legal Requirements of Electronic Commerce Transactions in Nigeria' (2011)3(1) *Bayero University Journal of Public Law*164–183, 165.

[2] DJ Ibegbulem and FO Ukwueze, 'Deconstructing Nigeria's Data Protection Regime from Consumer Protection Perspective' (2021) 13(1) *The Law, State and Telecommunications Review* 94 – 118, 96.

accuracy and transmitted or distributed to long and dispersed areas with lightning speed. Without a robust legal framework for personal data protection, enormous amounts of personally identifiable information (PII) can be collected, stored, processed and transmitted without the knowledge or consent of the data subjects.[3] If personal data get into wrong hands, they can be put to uses that can be injurious to the data subjects. Furthermore, absence of legal protection of personal data raises serious challenges to security of lives and property of individuals, and can discourage individuals from engaging in online transactions out of fear of their PII being misused.[4] This article examines the legal framework for personal data protection in Nigeria with a view to assessing its adequacy in protecting the personal data of Nigerians and other people in the country. It adopts the doctrinal method and analyses relevant Nigerian statutes that protect personal data of individuals. It is divided into five sections of which this introduction is the first. The second section highlights the importance of privacy of personal data and the need for their protection. The third section identifies the relevant laws on personal data protection in Nigeria prior to the issuance of the Nigeria Data Protection Regulation 2019 (NDPR), and analyses them to show the level of protection of personal data they provide. The penultimate section discusses NDPR analysing its key provisions to determine their adequacy to provide the much needed protection of personal data in Nigeria. The last section is the conclusion which also contains the key recommendations of the article.

2. Significance of Personal Data Protection Laws

Personal data refer to information relating to an identified or identifiable natural person.[5] A data subject therefore is a natural person 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.[6] Personal data ranges from a name, address, a photo, a phone number, an email address, bank details, medical information, to other unique identifier such as, Internet Protocol (IP) address, Media Access Control (MAC) address, International Mobile Equipment Identity (IMEI) number, International Mobile Subscriber Identity (IMSI) number, Integrated Circuit Card Identifier (ICCID) or Subscriber Identity Module (SIM) and so on.[7]

---

[3] Ibid.

[4] Joseph M Jones and Leo R Vijayasaratgy, 'Internet Consumer Catalog Shopping: Findings from an Exploratory Study and Directions for Future Research' (1998) 8(4) *Internet Research,* 322

[5] Nigeria Data Protection Regulation 2019 (NDPR) r 1.3 (xix).

[6] Ibid r 1.3 (xiv)

[7] Ibid r 1.3 (xxi).

Technology has radically changed the ways and manners of doing many things. Buying and selling of goods and services online (e-commerce), is steadily gaining popularity. Banking and other financial operations are increasingly being conducted online and many organisations now collect payments through digital platforms.[8] Many educational institutions operate e-learning programmes, conduct examinations and publish results online. Digital transactions often involve the transfer of money and the exposure of customers' personal information and data over telecommunication networks and trading platforms. Sometimes, such information gets exposed beyond the expected point, thereby rendering them susceptible to the activities of hackers and fraudsters.

Data protection laws have evolved to protect individuals against misuse, misappropriation or unlawful disclosure of their PII by regulating all activities relating to personal data which collectively is referred to as the processing of personal data. Processing of personal data covers all operations performed on personal data such as the collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.[9] The type of information and data that require protection are wide and varied personal information such as gender, health status, personal relationships, addresses, telephone numbers, internet activities, banking transactions, medical records, etc.[10]

Without legal regulation of personal data, the privacy of individuals as well as the security of their lives and property will remain precarious and susceptible to activities of rogues and mischief makers. Thus, data protection regulations are used to secure individuals' rights to privacy.

3. Data Protection Laws in Nigeria

3.1 Right to Privacy under the Constitution

Flowing from the 'right to privacy' enshrined in numerous international human rights instruments,[11] the Nigerian Constitution guarantees and protects the citizens' right to privacy of their homes, correspondence, telephone

[8] Ibid.

[9] NDPR r 1.3 (r).

[10] Aaron Olaniyi Salau, 'Data Protection in an Emerging Digital Economy: The Case of Nigerian Communications Commission - Regulation without Predictability?' 7th International Conference on Information Law and Ethics, 22-23 February 2016 <https://icil.gr/download.phpfen=years/2016/downloads/speakers/0083-salau-abstract-en-v1.pdf> accessed 15 December 2019.

[11] Such as the Universal Declaration of Human Rights, art 12; International Covenant on Civil and Political Rights, art 17; American Convention on Human Rights, art 11; and European Convention for the Protection of Human Rights and Fundamental Freedoms, art 8.

conversations and telegraphic communications.[12] However, there is a consensus of opinion that although this constitutional provision envisages protection of citizens' personal information, it does not constitute sufficient legal instrument for individuals to enforce their right to control the access to, retention and the use of their personal information.[13] The Constitution does not define 'privacy' and its conceptualisation of the term appears too narrow; thus it has been rightly argued that the ambit of the constitutional right to privacy does not address the complex issues relating to collection, storage, processing, control and use of individuals' personal information and other online contents.[14]

3.2 Cybercrimes (Prohibition, Prevention, etc) Act 2015 (Cybercrimes Act)

The Cybercrimes Act which gives effect to the Economic Community of West African States (ECOWAS) Directive on Fighting Cyber Crime [15] deals specifically with cyber security. The stated objectives of the Act include promote cyber security and the protection of computer systems and networks, electronic communications, intellectual property and privacy rights.[16]

The Act provides that the President may on the advice of the National Security Adviser by order designate certain computer systems or networks as Critical National Information Infrastructure (CNII) which should comprise computer systems or networks that are vital to the nation, such that their incapacity or interference would have a debilitating impact on the nation's security, economy, public health and safety.[17]The Presidential Order on CNII may prescribe minimum standards, guidelines, rules or procedure relating to, among other things, the protection and general management of critical information infrastructure; access to, transfer and control of data in any critical infrastructure; the storage or archiving of data or information designated as CNII; and any other matter required for the adequate protection, management and control of data and other resources in any CNII.[18]

The Act creates and prescribes the punishment for a number of offences that relate to privacy and e-commerce. These include unlawful access to a computer system or network for fraudulent purpose or to obtain data that are

[12] Constitution of the Federal Republic of Nigeria 1999 (as amended) (hereinafter, the 1999 Constitution) s 37.

[13]LA Abdulrauf 'New Technologies and the Right to Privacy in Nigeria: Evaluating the Tension between Traditional and Modern Conceptions' (2016) 7 *Nnamdi Azikiwe University Journal of International Law and Jurisprudence,* 113.

[14] See Udo Udoma and Bello-Osagie, 'Data Privacy Protection in Nigeria' <https://www.uubo.org/media/1337/data-privacy-protection-in-nigeria.pdf> accessed 23 October 2019.

[15]Directive C/DIR. 1/08/11 – Directive on Fighting of Cyber Crime within ECOWAS done at Abuja on 19 August 2011.

[16]Cybercrimes Act s 1.

[17]Cybercrimes Act s 3 (1).

[18]Cybercrimes Act, s 3(2).

vital to national security; tampering with CNII; wilful interception of electronic messages, e-mails and electronic money transfer; wilful misdirection of electronic messages; unlawful interception of computer data; identity theft and impersonation; cyber-stalling and cyber-squatting; manipulation of Automated Teller Machine/Point of Sale (ATM/POS) terminals; phishing, spamming and spreading of computer virus, and other computer related fraud and offences.[19] Section 38 of the Act imposes a duty on communications service providers in relation to records retention and protection of personal data. A service provider is mandated to keep all traffic data and subscriber information as may be prescribed by the authority responsible for the regulation of communication services in the country, for a period of two years.[20] Service providers shall at the request of the authority or any law enforcement agency, preserve, hold, retain or release any traffic data, subscribers' information, non-content and content data. Any data retained, processed or retrieved by the service provider at the request of any law enforcement agency shall not be utilised except for legitimate purposes as provided in the Act, any other legislation, regulation or by an order of a court of competent jurisdiction.[21] Anyone exercising any function in this regard is enjoined to have due regard to the individual's right to privacy under the Constitution and to take appropriate measures to safeguard the confidentiality of the data retained, processed or retrieved for the purpose of law enforcement.[22]

The Act imposes heavy penalties for the various offences ranging from terms of imprisonment of two years to life imprisonment with options of fines ranging from ₦1 million to ₦7million and in some cases both imprisonment and fine. It makes provisions for victim compensation in addition to any penalty prescribed, as it mandates that the court 'shall' order a person convicted of an offence under the Act to make restitution to the victim of the false pretence or fraud by directing the person, where the property involved is money, to pay to the victim an amount equivalent to the loss sustained by the victim and in any other case, to return the property or pay an amount equal to the value of the property where the return of the property is impossible or impracticable. An order of restitution under the Act may be enforced by the victim or by the prosecutor on behalf of the victim in the same manner as a judgment in a civil action.[23]

Even though the Cybercrimes Act contains certain provisions relating to personal data protection, for all intents and purposes, it does comprehensively regulate the various aspects privacy of data subjects' personal information in e-commerce environment. For example, it seeks to prevent unlawful interference

[19] Ibid, ss 5 - 36.
[20] Ibid s 38(1).
[21] Ibid s 38(4).
[22] Ibid s 38(5).
[23] Ibid, s 49 (1) and (2).

with computer data but does not contain provisions on how personal data of individuals can be lawfully collected, stored processed and used by individuals and organisations that engage in online transactions with the data subject. To that extent, it does not provide full protection for PII of data subjects on computer networks.

3.3 Official Secrets Act 1962

The Official Secret Act (OSA)[24] aims to secure public safety by protecting official government information, prohibiting entry into or photographing or making sketches of defence establishments, restricting photography during a state of emergency and controlling mail forwarding agencies.[25]Section 1 of the Act prohibits unauthorised access to, reproduction, retention or transmission of any classified matter[26] on behalf of the government. For purposes of controlling mail forwarding agencies, section 4 of the Act empowers the Minister responsible for security and public safety to make regulations for controlling the manner in which any person conducts any organisation for receiving letters, telegrams, packages or other matter for delivery or forwarding to any other person, and providing for the furnishing of information and keeping of records by persons having or ceasing to have the conduct of such an organisation. Failure to comply with regulations so made constitutes an offence under the Act. Penalties for offences under the Act range from terms of imprisonment of up to 14 years or fines between ₦100 – ₦200 or both fine and imprisonment.[27]

It is obvious that the thrust of OSA is the protection of government records and related matters and not the protection of personal information of individuals. It can only provide protection for personal information where such information is part of a public record.

3.4 Freedom of Information Act 2011

This statute was enacted to provide for access to public records and information, protect public records and information to the extent consistent with the public interest as well as to protect personal privacy of individuals.[28] The Freedom of Information Act (FIOA) mandates every public institution to record and keep information about all its activities, operations and businesses in a manner that facilitates public access to such information.[29]It establishes the right of any person to access or request information, whether or not contained in any written

[24] No 29 of 1962, Cap O3, LFN 2004.
[25] Official Secret Act (OSA) ss 1 – 4.
[26] Classified matter means 'any information or thing which, under any system of security classification, from time to time, in use by or by any branch of the government, is not to be disclosed to the public and of which the disclosure to the public would be prejudicial to the security of Nigeria'. See OSA, s 9.
[27] OSA s 7.
[28] See the long title to the Freedom of Information Act (FOIA).
[29]FOIA, s 2.

form, which is in the custody or possession of any public official, agency or institution. An applicant for such information does not need to demonstrate any specific interest in the information sought. Any person entitled to the right to information can institute proceedings in court to compel any public institution to comply with the provisions of the Act.[30]

In spite of the wide latitude which FOIA affords for public access to records and information held by public institutions, the Act provides for circumstances where a public institution can deny an application for such information.[31] One of such circumstance is where the information sought is personal[32]and its disclosure would constitute an invasion of personal privacy. In such a situation, a public institution must deny an application for such information and can only disclose such information if the individual to whom it relates consents to the disclosure; or the information is already publicly available or where the disclosure would be in the public interest, and if the public interest in the disclosure of such information clearly outweighs the protection of the privacy of the individual to whom such information relates.[33]

The provisions of FOIA do not cover proper custody of personal information retained by public institutions. More worrisome is the fact that the Act does not make any provision for redress for an individual whose personal information is disclosed in circumstances where such information ought not to be disclosed. On the contrary, section 27 of FIOA provides immunity against the public institution in such circumstances as well as immunity against criminal or civil action against the recipient of such information for further publishing of the information.

3.5 Child Rights Act 2003

In furtherance of the constitutional provision, the Child Rights Act 2013 (CRA) reasserts the right to privacy as it relates to children for his/her privacy, family life, home, correspondence, telephone conversation and telegraphic communications.[34] This right of the child is however made subject to the rights of parents and legal guardians to exercise reasonable supervision and control over the conduct of their children and wards.[35] To ensure that the right of the child to privacy is respected at all stages of child justice administration in order to avoid harm being caused to the child by undue publicity which may lead to labelling, CRA prohibits the publication of any information that may lead to the

[30]Ibid, s 1.
[31] Ibid s 19.
[32] Personal information is 'any official information held about an identifiable person, but does not include information that bears on the public duties of public employees and officials'. See FOIA, s 31.
[33]FOIA, ss 12 and 14.
[34] CRA, s 8 (1) and (2).
[35] Ibid, s 8 (3)

identification of a child offender. It further stipulates that records of a child offender shall be kept strictly confidential and closed to third parties and made accessible only to persons directly concerned with the disposition of the case or other duly authorised persons.[36]

Evidently, CRA attempts to protect information of children and does not extend to adults. It does not make provisions for how personal data of children can be lawfully collected, stored processed, used or transmitted.

3.6 Sector Specific Regulatory Statutes

A number of statutes that regulate certain sectors of the Nigerian economy contain provisions that protect the privacy of individuals in relation that the particular sectors which they govern. These include the National Health Act 2014 (NHA), the Nigerian Identity Management Commission Act (NIMC) Act 2007[37] the Statistics Act 2007,[38] the Consumer Protection Framework (CPF) of the Central Bank of Nigeria (CBN) and various regulations of the Nigerian Communications Commission (NCC). Section 26 of NHA imposes a duty of confidentiality on medical information of individuals including information relating to the individual's health status, treatment or stay in a health establishment and no person may disclose such information unless the individual (patient) consents to the disclosure in writing or any law requires the disclosure or the non-disclosure represents a serious threat to public health, as witnessed during the Ebola outbreak of 2014. In the case of a minor or other person who is unable to give consent, the disclosure can only be made at the request of the parent, guardian or legal representative of such a person. Section 29 imposes a duty on persons in charge of health establishments that are in possession of a user's health records to set up control measures to prevent unauthorised access to those records and to the storage facility in which they are kept. Failure to observe this duty is an offence punishable on conviction by a term of imprisonment not exceeding two years or a fine of ₦250,000.00.

The Statistics Act has provisions which protect the privacy and confidentiality of private information. Section 26(2) of the Act provides that data collected for statistical purposes shall be treated as confidential and prohibits data producers from disclosing information that is of individual nature obtained in the course of their work. Also section 26 of the NIMC Act provides that no person or body corporate shall have access to the data or information contained in the database with respect to a registered individual entry except with the authorisation of the Commission.[39]The Commission can authorise such

[36] Ibid, 205.
[37] No 23 2007.
[38] No 9 2007.
[39] The National Identity Management Commission (NIMC) established by the Act to maintain a national database, registration of individuals and issuance of national identification cards; NIMC Act, s 5.

access only if an application for the information is made with the authority of that individual or the individual consents to the provision of that information, unless the provision of the information is in the interest of national security, necessary for purposes connected with the prevention or detection of crime or for any other purposes as may be specified by the Commission in a regulation when strictly necessary in public interest.

Paragraph 2.6 of CPF directs that appropriate measures should be established to guarantee protection of data subjects' assets and privacy. Every financial institution should at all times protect data subjects' financial and personal information and should not disclose such information to third parties without the consent of the data subject whose information is sought to be disclose except where such disclosure is required by law or ordered by statute. All personal information of customers (including those with closed accounts) shall be kept in confidence by financial institutions. As a duty of care, financial institutions are obliged to safeguard the privacy of their customers' data.

The above statutes and guidelines to some extent protect privacy but they lack provisions granting individuals' positive control over access to, usage and disclosure of their information by the various entities. An area where Nigerian consumer or data subject had substantial legal right to the control of collection access and usage of his or her personal information is in the telecommunications industry. Nigeria's telecommunications sector regulator, the Nigerian Communications Commission (NCC) in furtherance of its responsibility under the Nigerian Communications Act 2003 (NCA) has made and published several regulations and guidelines for the sector. Relevant for this discourse are the Consumer Code of Practice Regulation 2007 (CCPR) [40] and the Registration of Telephone Subscriber Regulation 2011 (RTSR).[41]CCPR stipulates the minimum standard and set of practices for the provision of services to consumers by licensees (telecommunications service providers). Part VI of the General Consumer Code of Practice (GCCP) annexed as a schedule to CCPR sets out the responsibility of a licensee in the protection of individual customer's information. Paragraph 35 (1) of the Code provides that a licensee may collect and maintain information on individual consumers reasonably required for its business purposes. However, the collection and maintenance of information on individual consumers shall, among other things, be fairly and lawfully collected and processed; processed for limited and identified purposes; relevant and not excessive; accurate; and protected against improper or accidental disclosure. Also, licensees are required to meet generally accepted fair information principles including notice, consumer or data subject choices on collection, use and disclosure of their personal information, their access to collected

[40]SI No 32 of 2007.
[41]SI No 35 of 2011.

information to ensure accuracy, security measures to protect such information and redress mechanisms to remedy any failure to observe the measures.[42]

RTSR complements the GCCP and makes elaborate provisions for data protection, confidentiality and release of subscribers' personal information. Regulation 9(1) of RTSR provides for the right of any subscriber whose personal information is stored in the Central Database[43] or a licensee's database to view the said information and to request updates and amendments thereto. A subscriber's information contained in the Central Database shall be held on a strictly confidential basis and no person or entity shall be allowed access to such information and no licensee shall release personal information of a subscriber to any third party (including security agencies) without obtaining the prior written consent of the subscriber except in accordance with the provisions of NCA, regulations and any guidelines or instrument issued from time to time. Even in such permitted circumstances, the data can only be released in a format determined by NCC.[44]RTSR prohibits and criminalises dealing with subscriber information in any manner inconsistent with its provisions, including retaining, duplicating, utilising a subscriber's information in any business, commercial or other transactions.[45]

While it can positively be asserted that NCC's CCPR and RTSR afford adequate protection to data subjects' personal information, they are of sectoral applications and their scope of application is restricted to the telecommunications industry alone.

3.7 Common Law Tort of Privacy

Commentators do not agree on the utility of tort of privacy in the protection of personal information in Nigeria. Nwauche asserts that a comprehensive protection of information privacy can be achieved through the tort of privacy which not only protects intrusion into individuals' privacy space but also information disclosure.[46]While noting that, strictly speaking, there is no cause of action for information privacy at common law,[47] he opines that the tort of breach of confidence protects information privacy, and is important in the development of a constitutional right to privacy. It has even been argued that some principles of information privacy may be gleaned from various tort actions, such as trespass, defamation, nuisance and passing-off. On the other

[42] General Consumer Code of Practice 2007 para 35(2).
[43]'Central Database' means subscriber information database, containing the biometric and other registration information of all telecommunications service subscribers in the country, which the Commission is required to establish and maintain; RTSR r 4(1).
[44]RTSR r 10.
[45]RTSR r 9(3).
[46] ES Nwauche, 'The Right to Privacy in Nigeria'(2007) 1 *Review of Nigerian Law and Practice* 63, 84.
[47]*Wainwright v Home Office* [2003] 3 WLR 1137.

hand, Abdulrauf[48] asserts that, unlike the later development in the English common law which permitted tort actions for breach of privacy, the law applicable in Nigeria does not recognise breach of privacy as an independent tort; rather what is applicable in Nigeria is an equitable action for breach of confidence which is limited in protecting privacy as it involves violation of trust in a relationship. Since there may not by any relationship of trust requiring confidence between individuals and entities that can collect, retain and use their personal information and thereby violate their right to privacy, the tort action for breach of trust cannot provide adequate protection for information privacy.[49]

A clear distinction can be drawn between privacy of space and privacy of information. While tort actions such as trespass, nuisance, defamation, passing-off and deceit can protect the invasion of privacy of space and false information concerning a person, they are not directed at protection of personal information particularly where such information is true. The equitable action of breach of confidence is anchored on relationship of trust between the two parties and cannot stand in the absence of such a relationship which need not exist for there to be violation contemporary information privacy. It has been rightly noted that one way to conceptualise the development of English law on privacy is that it is 'a creative…fusion of a 'right-based' conception of privacy, reflecting the influence of the European Convention on Human Rights with the traditional incremental approach of the English common law.' [50] Thus, privacy of information cannot be conceptualised under the English common law of tort as received in Nigeria[51]and tort actions could not provide the needed protection for information privacy; hence the need for legislation in the area.

4. Nigeria Data Protection Regulation 2019

This is the first general regulation on data protection in Nigeria. The Nigerian Information Technology Development Agency (NITDA) or the Regulation) in the exercise of its statutory mandate to create a framework for planning, research, development, standardization, application, coordination, monitoring, evaluation and regulation of information technology practices in Nigeria by developing standards, guidelines and regulations for that purpose,[52] issued the Nigeria Data Protection Regulation (NDPR/the Regulation) in January 2019.

[48]Abdulrauf (n 9) 121.
[49] Ibid.
[50] David Lindsay and Sam Ricketson, 'Copyright, Privacy and Digital Rights Management' in AT Kenyon and M Richardson, (eds) *New Dimensions in Privacy Law: International and Comparative Perspectives*, (New York, Cambridge University Press, 2006) 121, 137.
[51] See Interpretation Act Cap I 23 LFN 2004 s 32(2).
[52] Nigerian Information Technology Development Agency Act No 28 of 2007 s 6.

4.1 Objectives, Scope and Application

The stated objectives of the Regulation are to safeguard the rights of natural persons to data privacy; foster safe conduct of transactions involving the exchange of personal data; prevent manipulation of personal data; and ensure that Nigerian businesses remain competitive in international trade, through the safeguards afforded by a just and equitable legal regulatory framework on data protection and which regulatory framework is in tune with global best practices.[53]

NDPR applies to the processing of personal data notwithstanding the means by which the data processing is being conducted, and to all natural persons resident in the country as well as Nigerians residing outside the country.[54] A data subject under NDPR is an identified or identifiable natural person – 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.[55] Extending the scope of the application of the Regulation to the protection of personal data of Nigerian citizens residing outside Nigeria is laudable, but it raises the question of its enforceability outside Nigeria. Its enforceability on Nigerian citizens abroad will depend on collaboration with regulatory and law enforcement authorities in other countries.[56]

4.2 Governing Principles of Data Processing

NDPR sets down principles of data processing covering fair and lawful processing, purpose specification, accuracy, consent, security and accountability, comparable to those found in the data protection statutes of other jurisdictions.[57]Regulation 2.1(1) provides that personal data are to be:

(a) collected and processed in accordance with specific, legitimate and lawful purpose consented to by the data subject; provided that:
   i. a further processing may be done only for archiving purposes in the public interest, scientific, historical or statistical research purposes; and
   ii. any persons or entity carrying out or purporting to carry out data processing shall not transfer any personal data to any person.
(b) adequate, accurate and without prejudice to the dignity of human person;
(c) stored only for the period within which it is reasonably needed; and

[53]NDPR, r 1.0.
[54]Ibid r 1.2.
[55] Ibid r 1.3 (xiv)
[56] The Regulation, para 2.11(a) and 4.3(a).
[57] See for example, GDPR, art 5; UKDPA s 34(1), elaborated on in ss 35 - 40; POPIA, chap 3; Singapore's Personal Data Protection Act (PDPA), No 26 of 2012 pts IV – VI; and US Federal Trade Commission's Information Practice Principles (FIPPs).

(d) secured against all foreseeable hazards and breaches such as theft, cyber-attack, viral attack, dissemination, manipulations or any kind, damage by rain, fire or exposure to other natural elements.

Processing of data is lawful if at least one of the follows applies:

(a) the data subject has given consent to the processing of his or her personal data for one or more specific purposes;
(b) processing is necessary for the performance of a contract to which the data subject is a 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 data controller is subject;
(d) processing is necessary in order to protect the vital interests of the data subject or of another natural person; or
(e) processing is necessary for the performance of a task carried out in the public interest or in the exercise of official public mandate vested in the controller.[58]

Processing of personal data in all forms of commercial and other transactions in which data subjects daily engage in, qualifies as lawful purpose under the Regulation. Thus, personal data of a data subject collected while window shopping on the Internet will satisfy the requirement of lawful purpose since such a visit to the website of a business is necessary preliminary to entering into the contract. NDPR prohibits improper motives in processing of personal data; thus, consent for data processing shall not be sought, given or accepted in any circumstance that may directly or indirectly engender propagation of atrocities, hate, child rights violation, criminal acts and anti-social conducts.[59]Although this provision is necessary to prevent the negative acts in question, the requisite motive can only be determined when any of the acts which are sought to be prevented has taken place except where there has been a manifest conduct towards its commission.

Under regulation 2.3, personal data shall not be obtained except the specific purpose of the collection is made known to the data subject. The data controller is under obligation to ensure that the consent of a data subject is obtained without fraud, coercion or undue influence. A data subject shall have the option to object to the processing of personal data relating to him which the data controller intends to process for the purposes of marketing and should be expressly offered the mechanism to object to any form of data processing free of charge.[60]A pertinent question here is whether it is only when the data controller intends to process data for marketing purposes that the data subject's right to object arises. If so, how would the data subject be aware of the intention to

[58] Ibid r 2.2
[59] Ibid r 2.4 (a)
[60] Ibid r 2.8.

process his or her personal data for the said purpose so as to raise the necessary objection?

Data processors and controllers are accountable to NITDA or a reputable regulatory authority for data protection.[61] Contracts between data controllers and third parties for processing of personal data must be in writing and it is the responsibility of the data controller to ensure adherence to the regulation.[62] Accordingly they are required to take reasonable measures to ensure that the other party to the data processing contract does not have a record of violating data processing principles set out in the regulation. This presupposes that there should be publicly available records of violations data processing principles to enable data controllers verify the credibility of entities they intend to engage for processing of personal data. Without such records, it will be difficult to hold them liable for not taking reasonable measures as required to ensure that such persons do not have records of violation of data processing principles. The Regulation does not make provision for the establishment of such a database.

Anyone involved in data processing or the control of data shall develop security measures to protect same; such measures include but are not limited to, protecting systems from hackers, setting up firewalls, storing data securely with access to specific authorised individuals, employing data encryption technologies, developing organisational policy for handling personal data (and other sensitive or confidential data), protection of emailing systems and continuous capacity building for staff.[63] The prescribed security measures for the protection of personal data appear to be adequate as they cover all conceivable hazards and breach. However, unlike the legislation of other countries, NDPR does not require responsible parties to regularly confirm the effective implementation of the safeguards and update such safeguards in response to new risks or deficiencies in previously implemented safeguards.[64] Such a provision is necessary to ensure that responsible parties are under obligation to regularly upgrade their security measures in view of the rapidity with information technology evolves.

4.3 Rights of Data Subjects

NDPR confers a number of rights on the data subject. These include rights to:

(a) information relating to data processing;[65]

(b) have personal data deleted;[66]

(c) restrict processing of personal data;[67]

---

[61] NDPR, r 2.4 (b)
[62] Ibid r 2.7.
[63] Ibid, r 2.6
[64] GDPR art 24(1); POPIA s 19(2)(d) and GDPA s 28(2)(d).
[65] NDPR r 3.1(1).
[66] Ibid, r 3.1(9).

(d) be notified of rectification, erasure or restriction of personal data;[68]

(e) and receive and transmit personal data.[69]

Data controller are mandated to provide the data subject any information relating to processing of data in a concise, transparent, intelligible and easily accessible form, using clear and plain language. A data subject has the right to request the controller to delete personal data or to impose on the data controller restriction in processing his or her personal data under certain circumstance. The data controller shall communicate any rectification or erasure of personal data or restriction to each recipient to whom the personal data have been disclosed unless this proves impossible or involves disproportionate effort. In that case, if the data subject requests, the controller shall inform him or her about those recipients.[70] A data subject has 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. A data subject also has the right to transmit those data to another controller without hindrance from the controller to which the personal data have been provided, where the processing is based on consent or contract, and the processing is carried out by automated means.[71] Similarly, in the exercise of right to data portability, a data subject has the right to have his or her personal data transmitted directly from one controller to another, where this is technically feasible; provided that 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.[72]

The security measures and information requirement under NDPR falls short of what obtains in other jurisdictions where responsible parties are required, as soon as it is reasonably possible, to notify not only the regulatory authorities but also the affected data subject(s), where there are reasonable grounds to believe that the personal data of a data subject has been accessed or acquired by any unauthorised person, providing sufficient information to allow the data subject to take protective measures against the potential consequences of the compromise.[73] The absence of a mandatory requirement of prompt notice to the regulator and data subjects may result in total non-disclosure or delay ins disclosure of data compromise, which will consequently impede protective mitigation measures by the data subject. Furthermore, NDPR does not prescribed any mitigating measures that can be adopted on the occurrence of

[67] Ibid, r 3.1(13).
[68] Ibid, r 3.1(13).
[69] Ibid, r 3.1(14).
[70] Ibid, r 3.1(13)
[71] Ibid, r 3.1(14)
[72]Ibid, r 3.1(15)
[73] GDPR art 34; UKDPA ss 67 and 68; POPIA s 22 and GDPA s 31

personal data breach. This omission is not peculiar to it but is noticeable in even seemingly extensive data protection laws including the GDPR. Although a cardinal aim of data protection laws is the prevention of such breaches, there is need to include in such laws remedial steps to be taken in the event of a breach, since even the most extensive and efficiently enforced data protection laws cannot be fool proof, in light of continuous technological advancement and increasing sophistication of cyber criminals.

4.4 Penalty for Default

NDPR imposes liability on any person who breaches the data privacy rights of any data subject. In addition to any other criminal liability, it imposes fines as follows:

(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.
(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 ₦2 million whichever is greater.[74]

Any breach of the regulation shall be construed as a breach of the provisions of the NITDA Act 2007.[75] Under the Act, any person or corporate body who contravenes or fails to comply with the provisions of the Act commits an offence.[76] Where an offence is committed by a body corporate or firm or other association of individuals, ~~every~~ the chief executive officer or the body corporate or any officer acting or purporting to act in that capacity ~~or~~ on behalf commits an offence, unless he proves that the act or omission constituting the offence took place without his knowledge, consent or connivance.[77]Anybody, corporate or individual who commits an offence under the Act where no specific penalty is provided, is liable on conviction to a fine of ₦200,000.00 or imprisonment for a year or to both such fine and imprisonment, for a first offence and a fine of ₦500,000.00 or to imprisonment for a term of three years or to both such fine and imprisonment, for a second and subsequent offence.[78]

4.5 Enforcement and Redress Mechanisms

Within three months after the date of issuance of NDPR, all public and private organisation in Nigeria that control data of natural persons were to make available to the general public their respective data protection policies.[79] Every data controller was required to designate a data protection officer for the

[74] NDPR r 2.10
[75]Ibid r 4.2(6). The import of this also may be that the penalty provisions of sections of the NITDA Act apply to the contravention of NDPR.
[76]NITDA Act s 17(1).
[77]Ibid s 17(3).
[78]Ibid s. 18(1).
[79] NDPR r 4.1(1)

purpose of ensuring adherence to the regulation, relevant data privacy instruments and date protection directives of the controller. However, a data controller may outsource data protection to a verifiably competent firm or person.[80] Every data controller or processor shall ensure continuous capacity building for her data protection officers and the generality of her personnel involved in any form of data processing.[81] The three months grace period given to relevant data controllers to comply with the provisions of the Regulation is evidently too short to enable them set up the required data protection mechanisms. Under the GDPR a transitional grace period of two years was recommended for compliance[82] while POPIA stipulates a grace period ~~was~~ of one year which may be extended to an additional period of up to three months.[83] Three months only, as provided in NDPR, for a country that did not have a prior regulation that required the kind of skill and technical capacity envisaged under the Regulation, is to say the least, a herculean task. This period eventually proved to be too short as it was only on 11 July 2019 (six months after its issuance in January 2019) that NITDA released a draft framework for its implementation, known as the Draft Implementation Framework[84] On 18 May 2020, the Agency issued the Guidelines for the Management of Personal Data by Public Institutions in Nigeria 2020 for the implementation of the Regulation within public institutions in Nigeria.[85] It was not until November 2020 that NITDA published NDPR Implementation Framework,[86] a guide to assist data controllers and data administrators/processors understand the controls and measures they need to introduce into their operations in order to comply with the NDPR.

NITDA is mandated to register and license Data Protection Compliance Organisations (DPCOs) who shall on behalf of the Agency and subject regulations and directives of the Agency, monitor, audit, conduct training and data protection compliance consulting to all data controllers.[87] Where a data

[80] Ibid r 4.1(2)
[81] Ibid r 4.1(3).
[82] GDPR Preamble para 171.
[83] POPIA s 114(1) and (2).
[84] See NITDA, *Nigeria Data Protection Regulation 2019: Draft Implementation Framework,* <https://nitda.gov.ng/wp-content/uploads/2019/01/Nigeria%20Data%20Protection%20Regulation.pdf> accessed 5 November 2020.
[85] NITDA, Guidelines for the Management of Personal Data by Public Institutions in Nigeria, 2020 <https://nitda.gov.ng/wp-content/uploads/2020/11/GuidelinesForImplementationOfNDPRInPublicInstitutionsFinal11.pdf> accessed 15 June 2021.
[86] NITDA, NDPR 2019: Implementation Framework, 2020 <https://nitda.gov.ng/wp-content/uploads/2021/01/NDPR-Implementation-Framework.pdf> accessed 15 June 2021.
[87] NDPR r 4.1(4)

controller processes the personal data of more than 1000 data subjects in a period of six months, a soft copy of the summary of the audit shall be submitted to the Agency while on annual basis, a data controller who processes the personal data of more than 2000 data subjects in a period of 12 months shall, not later than the 15 of March of the following year, submit a summary of its data protection audit to the Agency.[88] The mass media and the civil society have the right to uphold accountability and foster the objectives of the regulation.[89] Without prejudice to the right of a data subject to seek redress in a court of competent jurisdiction, NITDA is mandated to set up an Administrative Redress Panel (ARP) to handle complaints of breach of the regulation and recommend appropriate remedies.[90] In October 2019, NITDA inaugurated an ARP which is comprised of industry professionals and representatives of relevant government agencies that will provide an alternative dispute resolution mechanism to address grievances in a non-litigious manner.[91]

5. Conclusion

NDPR is currently the most comprehensive legislation on personal data protection Nigeria. Although not as comprehensive as the GDPR or the personal data protection laws of some African countries notably, South Africa and Ghana, it provides a pedestal on which the country can progressively fashion a robust data privacy regulation. In spite of the shortcomings in its provisions, some which have been highlighted above, there appears to be a consensus of opinion that it is a step in the right direction[92] and a welcome development[93] and should be implemented to logical conclusion, as it provides some measure of protection for personal data that hitherto did not exist.

One major shortcoming of NDPR is that it is a subsidiary legislation. Although a subsidiary legislation has the force of law as the enabling statute, because it does not pass through the rigorous law making process of the legislature, its provisions may not be very robust. A full Act establishing an independent regulator specifically charged with the responsibility for the regulation of personal data in the fashion of UKGDP, GDPA and POPIA is

[88] Ibid r 4.1 (6) and (7).
[89] Ibid r 4.1(8).
[90] Ibid r 4.2.
[91] One Trust Data Guidance 'Nigeria: NITDA Issues Statement on Data Protection <https://www.dataguidance.com/news/nigeria-nitda-issues-statement-data-protection> accessed 12 April 2022.
[92] Oyeyemi Aderibigbe, 'An outlook on the Nigerian Data Protection Regulation 2019'*Businessday* (11 April 2019) <https://businessday.ng/legal-business/article/an-outlook-on-the-nigerian-data-protection-regulation-2019/> accessed 5 November 2019.
[93] See also D Oturu 'An Overview of Big Data and Data Protection in Nigeria' (19 April 2019) <https://www.aelex.com/wp-content/uploads/2019/05/An-overview-of-Big-Data-and-data-protection-in-Nigeria-1-compressed.pdf> accessed 2 Nov 2019.

preferable. There is a Bill[94] presenting pending before the Senate of the National Assembly, having earlier been passed by the House of Representatives, which seeking to enact an Act to establish a Data Protection Commission for the protection of personal data and to regulate the processing personal information and related matters. The National Assembly is urged to expedite action on the passage of the Bill and to use it to establish a robust legal framework for personal data protection and lay to rest the lurking argument on the legitimacy of NDPR and the worrisome foot-dragging by NITDA in its implementation.

In the meantime, there is an urgent need for NITDA to step up the implementation of the NDPR. Complaints from data subject are important to trigger off administrative and other enforcement mechanisms in a regulation such as NDPR. Public awareness is vital in ensuring effective enforcement of a protective regulation such as NDPR. If individuals whose rights are protected by a regulation are not aware of the steps to take to enforce the rights granted them under the regulation, such rights become a mirage. To ensure effective enforcement of NDPR there is a need for NITDA to put in place an efficient public enlightenment programme to educate Nigerians on their rights and the redress mechanisms under the NDPR.

[94] SB 1 2019.