THE LEGAL REGIME FOR DATA PROTECTION IN NIGERIA: THE NIGERIA DATA PROTECTION COMMISSION IN FOCUS*

Abstract
Data privacy and data protection has become a subject of great importance in very recent times. This is considering the critical status of personal data which is in more cases than not, is equated to a person's identity. Against this backdrop, several countries have advocated for stronger data protection mechanisms of citizens' personal data. To combat data breaches and abuses, the presence of an effective regulatory body is apposite. This article assessed the Nigeria Data Protection Commission (NDPC) which is currently the main regulatory body for data protection in Nigeria. It examined its establishment, functions, powers, duties, recent activities, challenges and prospects. The paper found that the primary data protection regulatory body of the Nation has so far achieved commendable milestones within its short years of operation and is poised to scoring a higher index as far as data protection matters are concerned if certain mechanisms are put in place. These mechanisms include increased funding, private sector cooperation and participation in data protection. The study recommended, amongst others, cooperation from private citizens through prompt reportage of privacy invasion cases by corporations, institutions and so on.

Keywords: Data Protection, Data Privacy, Nigeria Data Protection Commission, Legal Regime

1. Introduction

The advent of the internet age came with exponential changes. The 'dot com' boom brought about an exponential increase in the amount of data created and stored across the internet. As a result, the security of personal data shared online has become a real national concern, with state actors, organizations, and hackers constantly attempting to exploit information of data subjects that should be handled ethically for commercial or malicious purposes.[1] According to TechCabal,[2] data protection in Nigeria is still in a dire state. In the first quarter of 2023, Nigeria was ranked as the 32nd country with most privacy breaches in the world. This coincided with a 64% increase in breaches from 2022.[3] In 2019, the National Information Technology Development Agency, NITDA began investigating Banks, Financial Technology companies and Telecommunication companies for breach of data privacy in Nigeria. The then regulatory body issued a total of N15 million fines to those found guilty, showing that the government is aware of the gravity of these issues. In 2021, a Lagos based Fintech, E-Settlement, was fined N5 million for data breach after an audit of its activities and processes uncovered a data breach. Also in 2019, Business Day reported that the Nigerian Yellow Card website was compromised. This was a serious issue because the website contained sensitive health data of Nigerians that use the air travel service. Unfortunately, the Government did not respond to this alarming report as is ordinarily expected. Many websites in Nigeria have loopholes that make them vulnerable to hackers. Also, these days, a lot of sites use HTTP cookies.[4]

A corollary effect of the dire state of Nigeria's data protection has been the unethical use of the personal data of Nigerians by companies. For instance, some companies particularly loan Apps, employ unethical debt collection methods whereby they surreptitiously gain access to the contacts or phone directory of their clients and disclose the transaction details of the defaulting clients to the contacts in a bid to harass the defaulters to pay. This has resulted in psychological damage on Nigerians who were affected.[5] However, with the level of sophistication

***By Ikenga K.E. ORAEGBUNAM**, **PhD (Law), PhD (Phil.), PhD (Rel. & Soc.), PhD (Edu. Mgt., in view), MEd, MA (Rel & Soc), LLM, MA (Phil), BTh, BA, BPhil, BL**, Professor and Formerly Head, Department of International Law and Jurisprudence, Faculty of Law, Nnamdi Azikiwe University, P.M.B. 5025, Awka, Anambra State, Nigeria. Email: ikengaken@gmail.com; ik.oraegbunam@unizik.edu.ng. Phone Number: +2348034711211; and

***Tega EDEMA, LLB, LLM, PhD Candidate**, Faculty of Law; Law Lecturer, Admiralty University of Nigeria, Ogwashi-Uku; 08133518440; tegaedema342@gmail.com

[1].Warren O.' The Emergence and Evolution of the Nigerian Data Protection Regulation' *Linkedin* <https://www.linkedin.com/pulse/emergence-evolution-nigerian-data-protection-warren-oluwasanya/> accessed 24th January 2024

[2]Muktar Oladunmade, 'Nigeria has suffered several data breaches recently, and its Data Protection Commissioner wants to change that' *Techcabal* <https://techcabal.com/2023/06/30/nigeria-data-protection-commissioner/> accessed 26th January 2024

[3] ibid

[4]Chidinma Amunta, 'Challenges of Data protection and compliance in Nigeria' *Linkedin* <https://www.linkedin.com/pulse/challenges-data-protection-compliance-nigeria-amuta-mba-llb> accessed 26th Janaury 2024

[5](n.2)

and innovation that comes with the internet today, there are associated risks with digital privacy, cybersecurity, and ethical use of data.[6]

The NDPC was initially a body under the National Information Technology Development Agency (NITDA) under the aegis of Nigerian Data Protection Bureau (NDPB). In 2022, the NDPB was formed and operated as an arm of the NITDA. The major functions of the NDPB were to implement the NDPR. However, in order to align with the ECOWAS Act on personal data protection and the requirement for an independent supervisory authority on data protection, the NDPC was floated as a body separate from the NITDA.[7] On June 12 2023, the Nigeria Data Protection Act (NDPA) came into effect. The NDPA established the Nigeria Data Protection Commission which is now the major regulatory body for data protection in Nigeria. The vision of the NDPC is to be a resilient world class institution for the protection of data privacy. The mission of the NDPC is making data privacy a cornerstone of sustainable digital economy in Nigeria.[8] The core values of the commission are accountability, fairness, integrity and transparency.

2. Establishment of the NDPC

Section 4 of the NDPC establishes the NDPC as follows;
(1) There is established the Nigeria Data Protection Commission (in this Act, referred to as "the Commission").
(2) The Commission —
(a) shall be a body corporate, with perpetual succession and a common seal;
(b) may sue or be sued in its corporate name; and
(c) may acquire, hold and dispose of its property.
(3) The Commission —
(a) shall have its head office in the Federal Capital Territory; and
(b) may maintain other offices, in any part of Nigeria, for the purposes of achieving the objects of the Commission.
(4) Subject to the approval of the Council, the National Commissioner may acquire other offices and premises for the use of the Commission.

3. Functions of the Commission

Section 5 of the NDPA outlines the functions of the Commission;
The Commission shall;
(a) regulate the deployment of technological and organisational measures to enhance personal data protection;
(b) foster the development of personal data protection technologies, in accordance with recognised international best practices and applicable international law;
(c) where necessary, accredit, license, and register suitable persons to provide data protection compliance services;
(d) register data controllers and data processors of major importance;
(e) promote awareness on the obligation of data controllers and data processors under this Act;
(f) promote public awareness and understanding of personal data protection, rights and obligations imposed under this Act, and the risks to personal data;
(g) receive complaints relating to violations of this Act or subsidiary legislation made under this Act;
(h) collaborate with any relevant ministry, department, agency, body, company, firm, or person for the attainment of the objectives of this Act;
(i) ensure compliance with national and international personal data protection obligations and best practice;
(j) participate in international fora and engage with national and regional authorities responsible for data protection with a view to developing efficient strategies for the regulation of cross-border transfers of personal data;
(k) determine whether countries, regions, business sectors, binding corporate rules, contractual clauses, codes of conduct, or certification mechanisms, afford adequate personal data protection standards for cross-border transfers;
(l) collect and publish information with respect to personal data protection, including personal data breaches;
(m) advise government on policy issues relating to data protection and privacy;
(n) submit legislative proposals to the Minister necessary for strengthening personal data protection in Nigeria; and
(o) carry out other legal actions as are necessary for the performance of the functions of the Commission.

[6] ibid
[7] Muktar Oladunmade, 'Nigeria has suffered several data breaches recently, and its data protection commissioner wants to change that' <https://techcabal.com/2023/06/30/nigeria-data-protection-commissioner/>
[8] NDPC, 'About Us' <https://ndpc.gov.ng/Home/about> accessed 29th January 2024

4. Powers of the Commission

Section 6 of the Act stipulates the powers of the commission as follows;

The Commission shall have powers to —

(a) oversee the implementation of the provisions of this Act;

(b) prescribe fees payable by data controllers and data processors in accordance with data processing activities;

(c) issue regulations, rules, directives and guidance under this Act;

(d) prescribe the manner and frequency of filing, and content of compliance returns by data controllers and data processors of major importance to the Commission;

(e) call for information from a person, or inspect any documents with respect to anything done under this Act;

(f) conduct investigations into any violation of a requirement under this Act or subsidiary legislation made under this Act by a data controller or a data processor;

(g) impose penalties in respect of any violation of the provisions of this Act or subsidiary legislation made under this Act;

(h) acquire assets, and sell, let, lease, or dispose of any of its property; and

(i) perform such other acts as are necessary to give effect to the functions of the Commission.

5. Recent Regulatory Activities and Achievements of the NDPC

Delisting non-compliant Data Processing Compliance Officers (DPCOs)

Generally, DPCOs are licenced under the Nigeria Data Protection Regulation (NDPR) to provide compliance services and guide their clients whether in the public or private sectors to adhere to privacy guidelines under the NDPR. Article 1(3j) of the Nigerian Data Protection Regulation provides that a Data Protection Compliance Organisation (DPCO) is any entity duly licensed by NDPB for the purpose of training, auditing, consulting and rendering services aimed at ensuring compliance with this Regulation or any foreign Data Protection law or regulation having effect in Nigeria. A DPCO may be one or more of the following; Professional Service Consultancy firm, IT Service Provider, Audit firm and a Law firm. The services provided by licensed DPCOs include data protection regulations compliance and breach services for data controllers and data administrators; data protection and privacy advisory services; data protection training and awareness services; data regulations contracts drafting and advisory; data protection and privacy breach remediation planning and support services; information privacy audit; data privacy breach impact assessment; data protection and privacy due diligence investigation and outsourced Data Protection Officer etc.

In the early part of 2023, the Nigeria Data Protection Bureau (NDPB) revoked the operating licence of 19 Data Protection Compliance Organizations (DPCOs). The goal behind this move by the NDPB was in pursuit of sanitizing the nascent data protection industry. The nineteen (19) DPCOs were delisted as licensed operators having failed to meet the minimum requirements of the NDPR including shoddy "filing of annual compliance audit returns" on behalf of their clients.[9] At the time, many DPCOs failed to demonstrate the requisite professionalism and capacity to carry through with data protection tasks despite their face-value qualification. DPCOs are allowed to carry out training, auditing, consulting, and provide such services or products in line with compliance requirements with the NDPR. Like the erstwhile NDPB, the NDPC is expected to evaluate data controllers and data processors on other performance metrics including but not limited to implementation of NDPR compliant privacy policy; sensitization of data subjects on data subjects' rights; filing of annual compliance audit returns and globally acceptable information security certifications.".[10]

Public Partnership with Data Protection Agencies/Job Creation

The NDPC has tasked itself with the duty to create awareness on the need for data protection compliance by corporations. Due to its data protection awareness campaign, several organisations now offer about 17 different services that did not exist before the commencement of the campaigns. This has resulted in the creation of over 9,000 jobs within three years. Furthermore, there has been an increase of organisations offering these services from seventeen (17) organisations to 168 organisations'.[11]

Licensing of DPCOS

To address this deficit, the commission started licensing data protection compliance organisations. These are companies with expertise in data privacy protection. As of November, 2023, one hundred and sixty-three (163) DPCOs have been licensed by the Commission.

[9]Olajide Deji, 'Nigeria Data Protection Bureau delists 19 DPCOs' *NDPC* <https://ndpc.gov.ng/Home/NewsDetails/18> accessed 22 January 2024

[10]Ibid

[11](n.2)

Investigation and Inquiry Processes

According to the NDPC's modus operandi, data protection and privacy complaints are received from the public and investigated. The companies involved are allowed to provide background information on the allegations and disprove any wrongdoing. After the NDPC completes an investigation and finds that a data controller or processor has violated provisions of the law, the data protection law recommends a range of actions. The affected companies may be required to pay compensation to data subjects, disclosing the profits it made from the violation. In the event of a fine, companies found guilty of violations may be fined a maximum amount of N10 million or 2% of its annual gross revenue in the preceding year, depending on whichever figure is greater.[12] In 2023, it was reported that OPay, Meta and DHL may be asked to pay 2% of their gross revenues in 2022 as fines if found guilty of data privacy violations according to Section 48 (5) of the Nigeria Data Protection Act of 2023. OPay, a digital banking company is being investigated over claims that it opened accounts for people without their consent. On the other hand, there were complaints that Meta engaged in behavioural advertising targeting customers without their consent.[13] As of January 2024, the Commission reports that in the area of complaints and investigations, it had received over 1,000 complaints, and after a thorough review, 50 of such cases have been verified, while investigations are currently ongoing on 17 major cases. These cases cover several sectors such as finance, technology, education, consulting, government, logistics and gaming\lottery among others.[14]

Imposition of Fines and Penalties

So far, the NDPC has generated over N400 million from fine imposition in ensuring compliance with data protection and its remedial actions.[15] There have been few instances where the NDPC used the sledgehammer on companies found guilty of privacy invasion. One of such notable cases is the *Soko Lending Company Limited case*. In 2021, the NITDA imposed a fine of N10 million on Soko Loans company for data breaches and privacy violations. The facts of the case were that investigation by NITDA revealed that Soko Loans grants its customers uncollateralised loans, requiring loanees to download its mobile application on their phone and activate a direct debit in the company's favour. The App gained access to the loanee's phone contacts. According to one of the complainants, when he failed to meet up with his repayment obligations due to insufficient credit in his account on the date the direct debit was to take effect, the company unilaterally sent privacy invading messages to the complainant's contacts. Investigation revealed that complainants' contacts who were neither parties to the loan transaction nor consented to the processing of their data have confirmed the receipt of such messages. The Agency made strident efforts to get Soko Loan to change the unethical practice but to no avail. After the Agency's investigation team secured a lien order on one of the company's accounts by which it could come up with privacy enhancing solutions for its business model, Soko Loan decided to rebrand and directs its customers to pay into its other business accounts. The Agency's investigation further revealed that the company embeds trackers that share data with third parties inside its mobile application without providing users information about it or using the appropriate lawful basis. NITDA found Soko Loan and its entities in violation of the following legal provisions: Use of non-conforming privacy notice, contrary to Article 2.5 and 3.1(7) of the NDPR; insufficient lawful basis for processing personal data, contrary to Articles 2.2 and 2.3 of the NDPR; illegal data sharing without appropriate lawful basis, contrary to Article 2.2 of the NDPR; unwillingness to cooperate with the data protection authority, contrary to Article 3.1 (1) of data protection implementation framework; and Non-filing of NDPR Audit reports through a licensed data protection compliance organisation (DPCO), contrary to Article 4.1(7) of the NDPR.

In view of the foregoing and in consideration of its implication on the privacy of Nigerians and erosion of trust in the digital economy, NITDA imposed a monetary sanction of N10 million naira on Soko Lending Company Limited. Other sanctions include, a directive restricting further privacy invading messages being sent to any Nigerian until the company and its entities show full compliance with the NDPR; a directive that the company pay for the conduct of a Data Protection Impact Assessment by a NITDA appointed DPCO on its operation; and placement on a mandatory Information Technology and Data Protection oversight for 9 months. Furthermore, NITDA has taken preliminary steps for handling the criminal aspects of this case by referring same to the

[12]Joseph Olaoluwa, 'OPay, DHL, Meta may face steep fines as NDPC begins investigation into alleged data privacy violations' <https://techcabal.com/2023/10/10/opay-dhl-meta-risk-fines-as-ndpc-begins-privacy-investigation/> accessed 26th January 2024

[13]ibid

[14]PeopleGazette, 'Nigeria's data privacy violators fined N400 million, says NDPC' <https://gazettengr.com/nigerias-data-privacy-violators-fined-n400-million-says-ndpc/> accessed 29 January 2024

[15]ibid

Nigerian Police to determine if the executives of the company are liable to imprisonment for violating Section 17 of the NITDA Act, 2007.[16]

6. Prospects of the NDPC

Creation of Regulations for Quick Dispensation of Regulatory Activities: The NDPC plans to create rules and regulations for emerging technology which will enable it easily and promptly attend to data protection complaints etc matters without the need to amend the existing law by legislative process. The NDPC has been empowered to carry out such functions including the imposition of fines on companies that have committed a breach of data protection, hence the flexibility of the NDPA. The law empowers the commission to issue regulations, which would be as powerful as the Act itself.[17] So far, the Commission has inaugurated the Nigeria Data Protection Act – General Application and Implementation Directive (GAID) Drafting Committee.[18]

Independence in its Operation: The Commission hopes to investigate breaches even without a public complaint. The Commission states that this is one of its principal functions, i.e conducting independent investigations in any sector that has to do with personal data protection wherever there is a data breach and to make binding decisions. However, Companies have the right to appeal, with the Supreme Court being the final arbiter.[19] The commission also intends to be self-funding and self-sustaining within the shortest possible time particularly by generating its revenue through its activities such as fines etc.

7. Challenges of Data Protection Regulation in Nigeria

Low Number of Certified Data Protection Officers
The NDPC reports that there are just about 10,000 certified data protection officers whereas there is a need for up to 500,000 data protection officers.[20] Due to the low amount of expertise in data protection services in Nigeria, the commission has had to employ a public-private partnership model.[21]

Unreported/Low Reportage of Data Breaches
Several cases of data breach or abuse go unreported daily. Amunta[22] outlines several reasons for this dilemma. First of all, the laws are not properly enforced, so there is no strict mandate for companies to report data breaches across board, not to mention that the firms in breach might not even have the professionals employed to help to prevent the problem in the first place or handle it afterwards. Secondly, regulatory bodies don't often pay attention to these issues until it affects someone important. Other reasons are the secrecy, lack of trust and the fear of repercussion or excommunication from the industry. These reasons and more make it so that data breaches are not reported even though the law mandates that they should be reported within 72 hours of breach.[23] Furthermore, not only are the consumers unacquainted with their right to data protection and privacy, most of the companies that collect these data are also unaware of the duty of care owed to their customers to protect the said data and it is alarming the rate at which people's private information is shared and even sold, sometimes. More often than not, without the help of the government, many organizations in Nigeria will still continue to knowingly or unknowingly breach data privacy or themselves remain targets of cyber-attacks.[24]

Poor Record Keeping
Nigeria has a severe problem of poor record keeping and maintenance, with replete effects on a daily basis. Private firms are both culpable and vulnerable because up to 8 in 10 firms in Nigeria experience cybersecurity breaches regularly. In any case, most of these organizations do not have an employed Data Controller or Compliance Officer. This is likely because in this part of the world, information about individuals can be

[16]NITDA, 'Sanctions SokoLoan for Privacy Invasion' *NITDA* <https://nitda.gov.ng/nitda-sanctions-soko-loan-for-privacy-invasion/4914/> accessed 20th Janaury, 2024
[17](n.2)
[18]PeopleGazette, 'Nigeria's data privacy violators fined N400 million, says NDPC' <https://gazettengr.com/nigerias-data-privacy-violators-fined-n400-million-says-ndpc/> accessed 29 January 2024
[19] (n.2)
[20]Leadershipng, 'Nigeria Needs 500,000 Data Protection Officers, Says NDPC' < https://leadership.ng/nigeria-needs-500000-data-protection-officers-says-ndpc/> accessed 28th Janaury 2024
[21](n.2)
[22]Chidinma Amunta, 'Challenges of Data protection and compliance in Nigeria' <https://www.linkedin.com/pulse/challenges-data-protection-compliance-nigeria-amuta-mba-ll bl/?trk=public_profile_article_view> accessed 29th January 2024
[23] ibid
[24] (n.22)

captured by companies and agencies that those individuals never interacted with. Amunta notes that it is rather regrettable that Nigeria is still grappling with data privacy and protection in this day and age where the world is already moving towards Web 3.[25]

8. Conclusion and Recommendations

From the above discourse, it is concluded that the regulatory environment for data protection in Nigeria is vibrant and spells hope for citizens and corporations alike. The implementation of some of the recommendations herein will only help to further strengthen the existing regulatory framework. It is therefore recommended as follows. The NDPC could award incentives and sanctions for cooperation or the lack thereof to public and private bodies involved on the issue of data protection. The Commission could ensure that companies are conducting ethical practices with the data they collect from others, and issue guidelines as to the level of cyber protection companies should meet in exchange for certifications that improve their goodwill before the country. This way, the motivation to take data protection and privacy more seriously would be encouraged. There is need for education and awareness. The NDPC should engage in more education and awareness campaigns on the importance of data protection and compliance with data protection laws. Users should be taught the importance of their data, their rights under existing laws, and the best ways to ensure they are protected from misuse. Increased responsibilities for corporations are also necessary. Companies should also be tasked with educating their members about data protection. Data protection practitioners should be adequately trained on the content of the laws, how to apply them, and the ethics of responsibility. Companies should ensure that systems of checks and balances are in place and routine previews are done on their cloud computing systems to ensure that the privacy of company information as well as those of their clients is safe. Privacy ethics should also be taught to employees as part of company policy. A constitutional amendment is required to ensure that data privacy is enshrined in the Country's constitution as a fundamental right and to eliminate the confusion amongst Judges on whether data privacy is a fundamental right protectable under the Constitution such as other traditional human rights like fair hearing or a civil wrong. Judges should be encouraged to participate in data protection judicial activism. As opined by Aloamaka,[26] given the complex nature of technology and data privacy, it may be necessary to establish a specialized Court comprising a new generation of Judges who are well-versed in technology and data privacy matters. These Judges would possess the expertise required to handle cases related to data breaches and privacy violations. This specialized Court would provide a forum where legal matters pertaining to technology and data privacy can be addressed with a high level of understanding and competence.[27]

[25]ibid
[26]P.C Aloamaka, 'Data Protection and Privacy Challenges in Nigeria: Lessons from other Jurisdictions' *UCC Law Journal* (2023) 3 (1) pp. 281-321
[27]ibid