Towards a Data Protection Legislative Framework in Nigeria:

Assessing the Regulatory and Legislative Attempts to Enact a Data Protection Law

2021

Meta TECH HIVE ADVISORY PARADIGM INITIATIVE

Published by Paradigm Initiative

2021

Authors

Sandra Musa

Samuel Ngwu

Reviewer and Copy editing

Damilola Ogunmuko

Design and Layout

Kenneth Oyeniyi

This report was written by Tech Hive Advisory, published by Paradigm Initiative with support from Meta.

Table of Content

Executive Summary

This report focuses on Nigeria's legislative and regulatory journey towards enacting comprehensive data protection legislation. The report is divided into five major parts, introduction and conclusion inclusive. The first part introduces the report, while the second part focuses on the brief history of data protection. The international and African data protection landscape was examined while briefly exploring the history of Africa's data protection. The second part also chronicles the legislative attempts in Nigeria. Finally, it probes relevant legislative and regulatory attempts from 2000 to 2020 while looking at the objectives of the laws, their data protection provisions, and their shortcomings.

The third part examines existing frameworks in Nigeria, such as the Nigeria Data Protection Regulation 2019. In doing this, the regulatory framework was examined, highlighting the key provisions and the inadequacies. In particular, the report highlighted some of the areas that the Nigeria Data Protection Regulation has been successful. Under this part, the report further mentions laws, regulations, and guidelines that impact data protection in Nigeria.

The fourth part of the report focuses on the recommendations for enacting comprehensive legislation. The recommendations, amongst others, note that there is a need for a comprehensive legal framework for personal data protection in Nigeria and that the enactment of such legislation should involve the collaboration of the government, experts, and relevant stakeholders.

Generally, the report finds that:

1. There has been a long legislative journey by the Nigerian government to enact comprehensive data protection legislation.
2. As a country, Nigeria has not shown political commitment towards ratifying or ensuring compliance with African regional frameworks on data protection.
3. Existing data protection frameworks partly provides data protection provisions for Nigerians; however, they still reflect inadequacies that require review.

4. There are secondary legislation providing bits and pieces of data protection provisions. However, because these frameworks were not originally made to regulate data protection, they contain insufficient provisions protecting personal data in Nigeria.

The final part of the report concludes that legislation has to improve tremendously considering technological demands. It noted the weakness of existing legislations and the role of policymakers, the courts, and other relevant stakeholders in creating a comprehensive law.

Methodology

This report employed a qualitative approach, including literature review, policy, legal and judicial analysis. Published In addition, published journals, online and traditional media reports, academic works and governments' documents were analysed. This report also incorporated the documented and informed opinions of writers, researchers, academics, civil society organisations, journalists, and human rights advocates.

The reference to the framework includes both legislative attempts and the creation of secondary legislation by regulators under their establishing laws.

1.0: Introduction

The proliferation of personal data through its processing has been beneficial to governments, corporations, and individuals. For individuals, this has enabled access to personalised services and a better consumer experience. For corporations, access to personal data has improved customer service and enabled quicker decision-making processes.[1] Access to personal data is also beneficial to governments and has helped design policies, plan interventions, and anticipate possible regulatory changes. Nevertheless, despite the benefits, the spread and availability of personal data expose individuals to a wide range of risks. For example, individuals face the risk of having their data used for undisclosed purposes. Also, unwarranted and unauthorised disclosure may occur, causing psychological and reputational harm, financial loss, and loss of control over information.

Owing to these issues occasioned by the processing of personal data, data protection laws have established rights and principles to protect the autonomy of individuals and to protect them from unlawful intrusions. Data protection laws are essential to enforce the rights of data subjects in the event of a violation and uphold the sanctity of these rights. Also, laws and regulations on data protection are necessary to hold organisations liable for violations arising from data processing activities. As a result, Nigeria has made various legislative and regulatory efforts towards enacting comprehensive legislation. These efforts can be seen in the various data protection bills that policymakers and governmental agencies have put forward. Other efforts are noticeable in various laws and bills incorporated within their framework, data protection provisions.

Against this backdrop, the objective of this report is to examine Nigeria's legislative and regulatory attempts towards regulating the processing of personal data. To achieve this

[1] Desai R, 'How Important Is DATA for Your Business?' (Medium, 6 September 2019) <https://towardsdatascience.com/how-important-is-data-for-your-business-c15a35c6935e> accessed 9 October 2021

objective, the report will be structured into five broad parts. After this introduction, the second part traces the history of data protection, briefly looking at its development internationally while focusing on its growth in Africa, particularly Nigeria. Then, considering the history of data protection in Nigeria, the report will focus on the regulatory and legislative attempts before the Nigeria Data Protection Regulation 2019, their provisions, and their inadequacies. The third part examines the existing framework in Nigeria with particular reference to the Nigeria Data Protection Regulation 2019 and the Draft Data Protection Bill 2020, highlighting and analysing their substantive provisions. The fourth part examines other laws that impact and intersect with data protection. Finally, the fifth part provides some reflections on what a progressive data protection model for Nigeria should contain and concludes the report with recommendations on the need for comprehensive data protection legislation and establishing an independent institution to administer the law.

2.0: The Emergence and Development of Data Protection

The development of data protection laws arose from recognising the risks involved in data processing and the need to protect individuals' personal information. This development was primarily due to the rapid advances in information and communications technologies (ICTs).[2] The German State of Hesse enacted the first data protection legislation in 1970.[3] This development was followed by enacting national data protection laws in Sweden,[4] the United States of America,[5] Germany,[6] and France.[7]

In the international scene, further advancement in technology with implications for transborder data flow led to international interest in data protection, thus making data protection more than a domestic affair. The first global instrument addressing data protection evolved from the Convention for the Protection of Individuals with regards to the Automated Processing of their Personal Data.[8] The Convention was adopted in 1980 by the Council of Europe (CoE).[9] This instrument is the first-ever binding international instrument on data protection. All 47 Member States of the CoE have so far ratified the Convention.[10] In addition, the Convention can be ratified by non-members of the CoE and

[2] Privacy and human rights—Overview. (n.d.). <http://gilc.org/privacy/survey/intro.html#fnlnk0035> accessed 16 July 2021

[3] Data Protection Act 1970

[4] Data Act 1973

[5] Privacy Act 1977

[6] Federal Data Protection Act 1977

[7] Data Protection Act 1977

[8] Convention for the Protection of Individuals with regards to the Automated Processing of their Personal Data 1980 <https://www.coe.int/en/web/conventions/full-list/-/conventions/webContent/en_GB/7%20834785> accessed 16 July 2021

[9] The Council of Europe is an international organisation founded in the wake of World War II to uphold human rights, democracy, and the rule of law in Europe. The Council was founded on May 5, 1949, and is headquartered in Strasbourg, France.

[10] The member States include Albania, Andorra, Armenia, Austria, Azerbaijan, Belgium, Bosnia and Herzegovina, Bulgaria, Croatia, Cyprus, Czech Republic, Denmark, Estonia, Finland, France, Georgia, Germany, Greece, Hungary, Iceland, Ireland, Italy, Latvia, Liechtenstein, Lithuania, Luxembourg, Malta, Monaco, Montenegro, Netherlands, North Macedonia, Norway, Poland, Portugal, Republic of Moldova, Romania, Russian Federation, San Marino, Serbia, Slovak Republic, Slovenia, Spain, Sweden, Switzerland, Turkey, Ukraine, and the United Kingdom.

has been endorsed by Argentina, Cabo Verde, Mauritius, Mexico, Morocco, Senegal, Tunisia, and Uruguay.[11] In 2001, the Convention approved an Additional Protocol.[12] The Protocol was made to consider the increase in exchanges of personal data across national borders and the need to ensure the effective protection of human rights and fundamental freedoms, particularly the right to privacy.[13]

In 2018, the Convention was modernised.[14] This modernisation resulted from the need to promote at the global level the fundamental values of respect for privacy and protection of personal data, contribute to the free flow of information, and reinforce international cooperation between the Parties to the Convention.[15]

Shortly after the Convention, the Guidelines Governing the Protection of Privacy and Transborder Data Flows[16] was adopted by the Organisation for Economic Cooperation and Development (OECD) in 1981. This Guideline sets out minimum standards for processing personal data. These standards are said to be minimum because of inadequate provisions for the protection of personal data. The Convention also sets out basic principles for managing personal data by the Member States and guides for their implementation. The Guidelines were revised in July 2013 with new provisions enhancing the data security measures and breach notification systems to notify authorities and individuals of security breaches.[17]

[11] Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data <https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/108> accessed 16 July 2021

[12] Additional Protocol to the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data regarding supervisory authorities and transborder data flows 2001 <https://rm.coe.int/1680080626> accessed 16 July 2021

[13] Additional Protocol to the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data regarding supervisory authorities and transborder data flows 2001, Preamble.

[14] Modernised Convention for the Protection of Individuals with Regard to the Processing of Personal Data 2018 <https://search.coe.int/cm/Pages/result_details.aspx?ObjectId=09000016807c65bf > accessed 16 July 2021

[15] Modernised Convention for the Protection of Individuals with Regard to the Processing of Personal Data 2018, Preamble

[16] OECD guidelines on the protection of privacy and transborder flows of personal data 1981—Oecd. (n.d.). <https://www.oecd.org/digital/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm> accessed 16 July 2021

[17] Revised Guidelines Governing the Protection of Privacy and Transborder Data Flows 2013 <https://www.oecd.org/sti/ieconomy/oecd_privacy_framework.pdf> accessed 16 July 2021

2.1 Data Protection in Africa

As a result of the proliferation of international instruments on data protection, there began to emerge other global and regional Frameworks across Europe, Asia, and America which embedded the principles of these foundational instruments. The adoption of data protection frameworks began in 2001, with Cape Verde enacting the first data protection law. This was followed by Seychelles in 2003, Burkina Faso and Tunisia in 2004, Senegal in 2008, and Morocco in 2009. With this development, more African countries enacted data protection frameworks. For example, in 2011, Gabon, Lesotho, and Angola passed a data protection framework. Ghana followed closely in 2012, Côte d'Ivoire, Mali and South Africa in 2013, and Chad and Madagascar in 2015. Between 2016 and 2021, Benin Republic, Egypt, Niger, Kenya, Rwanda, Uganda, Togo, and Zambia enacted similar frameworks.[18]As a result, over thirty African countries now have a specific data protection law, and nineteen have established or designated a regulator with the obligation to enforce the law.[19]

In addition, at the continental and regional levels, there have been concerted efforts towards establishing data protection regimes and frameworks. Primarily, these attempts have been driven by regional bodies within the continent. These attempts took place notwithstanding the non-recognition of the right to privacy by the African Charter on Human and Peoples' Rights (African Charter). However, the Declaration of Principles on Freedom of Expression and Access to Information in Africa adopted by the African Commission on Human and Peoples' Rights contains the protection of the right to privacy and protection of personal information by defining principles, establishing legal safeguards and recommending independence for the data protection regulator.[20]

[18] 'Data Protection and Privacy Legislation Worldwide | UNCTAD' <https://unctad.org/page/data-protection-and-privacy-legislation-worldwide> accessed 20 September 2021

[19] Africa Data Protection <https://www.africadataprotection.com/index.html> accessed November 25, 2021.

[20] Declaration of Principles on Freedom of Expression and Access to Information in Africa (2020) <https://www.achpr.org/public/Document/file/English/Declaration%20of%20Principles%20on%20Freedom%20of%20Expression_ENG_2019.pdf> accessed November 25, 2021.

2.1.1 East African Community (EAC) Framework for Cyber laws 2008 & 2011

As a part of these efforts, in 2008, the East African Community (EAC) Framework for Cyber laws was adopted as a data protection framework for the member states. The EAC Cyber laws frameworks were developed in 2008[21] and 2011[22] by the EAC Council of Ministers. These frameworks contain recommendations made by member states on how national laws can be reformed to facilitate electronic commerce, the use of data security mechanisms, and communication technologies to protect consumers in an online environment and protect individual privacy. The EAC frameworks are not binding on member States and only seek to harmonise the law reform process and provide international best practices. However, the frameworks fell short of providing specific guidance on incorporating them into domestic contexts.

2.1.2 Economic Community of West African States (ECOWAS) Supplementary Act on Personal Data Protection 2010

In 2010, the Economic Community of West African States (ECOWAS) also made an effort to enact a data protection framework by issuing the Supplementary Act on Personal Data Protection.[23] The Act was made by the Heads of State and Government of the ECOWAS to establish legal protection for collecting, processing, transmission, storage, and use of personal data.[24] The Act applies to any processing (automated or otherwise) of personal data by a natural person, the state, local communities, and public or private corporate bodies.[25] It also applies to processing undertaken in the territory of a member state and to processing for public security, defence, investigation, and prosecution of criminal offences

[21] Draft EAC Legal framework for Cyberlaws (2008) <http://www.eac.int/index.php?option=com_docman& task=doc_view&gid=632&Itemid=148> accessed 16 July 2021

[22] Framework for Cyberlaws, Phase II (UNCTAD, 2011) <http://r0.unctad.org/ecommerce/docs/EAC_Framework_PhaseII.pdf> accessed 16 July 2021

[23] Ecowas Supplementary Act on Personal Protection of Information A/SA.1/01/10. <www.tit.comm.ecowas.int/wp-content/uploads/2015/11/SIGNED-Data-Protection-Act.pdf> accessed 16 July 2021

[24] Overview of the legal framework on privacy. Center for Human Rights 2021.<https://chr.gchumanrights.org/ courses/course-v1:chr+rpdp+2021/courseware/8b7aacf3952f4d2b94289b4d8 1f5a88d/ad299d4233664018b8d7ed 327964ef10/1?activate_block_id=block-v1%3Achr%2Brpdp%2B2021%2Btype%40vertical% 2Bblock%40d8 d6bc30030744c699b00bf6557aed71> accessed 16 July 2021

[25] ECOWAS Supplementary Act, Articles 3(1) and (2)

or State security.[26] However, the Act expressly excludes processing carried out by an individual in the course of personal or domestic activities.[27]

The Act sets out formalities for obtaining the authorisation and opinion of the data protection authority and when it will be needed to process personal data;[28] the establishment, composition, duties, powers, and status of the data protection authorities for the member states;[29] the data protection principles;[30] transfer of personal data to a non-member of the Economic Community of West African States (ECOWAS);[31] and the rights of data subjects[32]. In addition, the Act prohibits direct prospecting (marketing) and automated decision-making.[33]

The Act complemented its revised ECOWAS Treaty[34] and was made to bind all ECOWAS Member States without ratification directly.[35] However, the direct application of the Act is inconsistent with the provision of the Country's Constitution. Therefore, section 12(1) of the 1999 Constitution of the Federal Republic of Nigeria (as amended),[36] it is provided that,

> *No treaty between the Federation and any other country shall have the force of law to the extent to which any such treaty has been enacted into law by the National Assembly.*

The court reinforces this provision in *Abacha v Fawehinmi*[37] where it was stated that,

> *It is, therefore, manifest that no matter how beneficial to the country or the citizenry, an international treaty to which Nigeria has become a signatory may be, it remains unenforceable if it is not enacted into the law of the country; by the National Assembly.*

---

[26] ECOWAS Supplementary Act, Article 3(2) and (3)
[27] ECOWAS Supplementary Act, Article 4
[28] ECOWAS Supplementary Act, Articles 7 to 13
[29] ECOWAS Supplementary Act, Articles 14 to 22
[30] ECOWAS Supplementary Act, Articles 23 to 30
[31] ECOWAS Supplementary Act, Article 36
[32] ECOWAS Supplementary Act, Articles 38 to 45
[33] ECOWAS Supplementary Act, Articles 34 and 35
[34] ECOWAS Treaty 1975 <https://www.ecowas.int/wp-content/uploads/2015/01/Revised-treaty.pdf> accessed 16 July 2021
[35] 'Treaty | Economic Community of West African States(ECOWAS)' <https://www.ecowas.int/ecowas-law/ treaties/> accessed 16 July 2021
[36] Constitution of the Federal Republic of Nigeria 1999 (As amended) <http://www.nigeria-law.org/Constitution OfTheFederalRepublicOfNigeria.htm> accessed 16 July 2021
[37] [1996] 9 NWLR (Pt. 475)710

Thus, for any international instrument to be binding and enforceable in Nigeria, it must be domesticated or transposed to domestic legislation by the National Assembly. In other words, due to Nigeria's dualist approach, international law, including treaties, have no force of law within the country unless it has been domesticated into national legislation. A similar requirement is also present in the constitutions of other West-African countries.[38] Apart from this restriction in enforcing the Act in member States, the Act has been criticised for not providing clear sanctions for a member state that fails to incorporate it into its domestic laws.[39]

2.1.3 Southern African Development. Community (SADC) Model Law on Data Protection (2010)

Africa's regional and sub-regional harmonisation efforts also witnessed the adoption of a Data Protection Framework by the Southern African Development. Community. The Southern African Development. Community (SADC) Model Law on Data Protection (2010) was adopted as a data protection framework. The SADC Model Law on Data Protection (SADC Model Law)[40] was developed by the SADC and the Communication Regulators' Association of South Africa (CRASA). However, this instrument is not binding and only guides member states to establish their national data protection frameworks.

2.1.4 Central Africa (ECCAS) Model Law and (CEMAC) Draft Directives on Data Protection 2013

The Economic Community of Central African States (ECCAS) comprises eleven member states. The Communauté économique et monétaire de l'Afrique centrale (CEMAC) shall consist of six French-speaking members states who are also members of the ECCAS.[41] In

[38] These countries include Ghana, Sierra Leone, the Gambia and Liberia, Benin, Senegal, Mali, Burkina Faso, Côte d'Ivoire, Guinea Bissau, Togo, Niger, and Guinea. Without national legislation, the treaty will not have the force of law in these countries. However, in Cape Verde, which adopts a monist approach, international laws and treaties are superior to national laws; as such, the ECOWAS Act is directly applicable in the country.

[39] AB Makulilo, 'Myth and reality of harmonisation of data privacy policies in Africa' (2015) 31 Computer Law & Security Review 78, 82.

[40] Data Protection: Southern African Development Community (SADC) Model law <https://www.itu.int/en/ ITUD/Projects/ITU-ECACP/HIPSSA/Documents/FINAL%20DOCUMENTS/FINAL% 20DOCS%20ENGLISH/ sadc_model_law_data_protection.pdf> accessed 16 July 2021

[41] The member countries of ECCAS, founded in 1983, are Angola, Burundi, Cameroon, Congo-Brazzaville, Democratic Republic of Congo, Gabon, Equatorial Guinea, Chad, Rwanda, and Sao Tome and Principe: see ECCAS. The six French-speaking countries are Cameroon, Equatorial Guinea, Central African Republic, Congo-Brazzaville, Gabon, and Chad.

2013, the ECCAS adopted three texts as 'model laws' on data protection. CEMAC adopted these laws as 'draft directives' on data protection, electronic communications, and cybercrime.[42]

2.1.5 African Union Convention on Cybersecurity and Personal Data Protection 2014

The African Union (AU) has attempted to adopt a continent-wide framework to protect personal data at the continental level. Thus, in 2011, the Draft African Union Convention on Establishing a Credible Legal Framework for Cyber Security in Africa was introduced. Subsequently, in 2013, the African Union Convention on Confidence and Security in Cyberspace was introduced.[43] However, this instrument was not adopted, but on 27 June 2014, the African Union, instead, adopted the African Union Convention on Cyber Security and Personal Data Protection (Malabo Convention) as a continent-wide instrument. [44] However, the Convention is yet to come into force as it is yet to obtain the required fifteen ratifications for it to come into force.[45] The Convention was made to recognise the need to balance the protection of privacy and the free flow of data on the one hand and the use of information and communication technologies on the other hand.[46] Therefore, a single data protection law should be applied to all member states instead of establishing a unified legal framework for all members. The Convention guides them towards establishing their cybersecurity and data protection laws.

---

[42] ECCAS Model Law / CEMAC Directives on Cybersecurity (Data protection, e-transactions, cybercrime) (in French) <http://www.itu.int/en/ITU-D/Projects/ITU-ECACP/HIPSSA/Documents/REGIONAL%20documents/ projets_des_lois_types-directives_cybersecurite_CEEAC_CEMAC.pdf> accessed 16 July 2021

[43] Draft African Union Convention on the Confidence and Security in Cyberspace <https://ccdcoe.org/uploads/2018 /11/AU-130101-DraftCSConvention.pdf> accessed 16 July 2021

[44] African Union Convention on Cybersecurity and Personal Data Protection 2014 <https://au.int/sites/default/ files/treaties/29560-treaty-0048_-_african_union_convention_on_cyber_security_and_personal_data_protection _e.pdf> accessed 16 July 2021

[45] African Union Convention on Cybersecurity and Personal Data Protection 2014, Article 36. So far, Benin, Ghana, Chad, Mozambique, Rwanda, Togo, Tunisia, Comoros, Congo, Guinea Bissau, Mauritania, Sierra Leone, Sao Tome & Principe, and Zambia have signed the Convention. However, countries like Senegal, Guinea, Mauritius and Ghana, Chad, Angola, Togo, Namibia, Mozambique, and Rwanda have ratified the Convention. Nigeria has neither signed the Convention nor ratified it.
See African Union, 'List of countries which have signed, ratified/acceded to the AU Convention on Cyber Security and Personal Data Protection. <https://au.int/sites/default/files/treaties/29560-sl-african%20union%20convention%20on%20cyber%20security%20and%20personal%20data%20protection.pdf> accessed 16 July 2021. This list excludes the new countries mentioned in the body of the work.

[46] African Convention on Cybersecurity and Protection of Personal Data 2014, Preamble

The scope of the Convention is provided for under Article 9. The Convention applies to public and private sectors generally and to automated and non-automated processing. It applies to processing relating to 'public security, defence, research, criminal prosecution or State security' but is subject to some exceptions defined by specific provisions in existing laws. However, it does not apply to processing exclusively for an individual's 'personal or household activities, but it applies to 'systematic communication to third parties or for dissemination.' The Convention also does not apply to any processing for journalistic or research purposes if conducted within professional codes of conduct and any processing for artistic or literary expression.[47]

The Convention sets out data processing principles to guide data controllers and the rights of data subjects under Article 13 – 19.[48] It also articulates the obligations of the data controller under Articles 20 – 23. Furthermore, the Convention prohibits the processing of sensitive data unless one of ten exceptions under Article 14 is satisfied. Furthermore, the prior authorisation of the Data Protection Authority is required for the processing of sensitive data.[49] Finally, the Convention imposes obligations on signatories to develop legal, policy, and regulatory measures to promote cybersecurity governance and control cybercrime.[50]

The establishment, composition, and duties of an independent National Personal Data Protection Authority in the member states are also provided.[51] The Convention requires the member States to establish an independent national data protection authority (DPA). The tasks are primarily to monitor and enforce compliance with the data protection legislation, receive complaints from data subjects, and sanction offenders. The Convention safeguards the independence of the DPA and forbids any public authority from giving instructions to the DPA or its members. It also prohibits government members, executives, or shareholders of companies operating in the information and communications sectors from being

[47] Malabo Convention, Article 14(3)

[48] Consent and legitimacy of personal data processing; lawfulness and fairness of processing; purpose, relevance, and storage of personal data; accuracy; transparency; confidentiality and security of personal data.

[49] Malabo Convention, Article 10(4)

[50] Malabo Convention, Article 25.Orji UJ, 'The African Union Convention on Cybersecurity: A regional response towards cyber stability?', in Masaryk University Journal of Law and Technology, 12, 2, pp. 92

[51] Malabo Convention, Articles 11 and 12

appointed to the DPA. Lastly, members of the Commission enjoy full immunity for opinions expressed in the pursuit of their duties.[52] Under Article 12, the DPA is given broad powers to impose remedies and sanctions.

To facilitate the implementation of the Malabo Convention, the African Union Commission collaborated with the Internet Society to develop the Personal Data Protection Guidelines for Africa.[53] The Guidelines provide recommendations on what stakeholders should consider when enacting a data protection framework. The Guidelines envisage new principles like data minimisation, privacy by design, accountability of data controllers, codes of conduct, and certification.

Although laudable, the Convention, just like the ECOWAS Act, is yet to be ratified and domesticated in Nigeria. Until it is domesticated and passed as a law by the National Assembly, the Convention has no force of law in Nigeria.[54]

2.1.6 African Declaration on Internet Rights and Freedoms 2014

Also, in 2014, some civil society organisations working on Internet governance in Africa and some prominent human rights organisations in Africa introduced the African Declaration on Internet Rights and Freedoms.[55] The Declaration protects the privacy of personal data on the internet and data security. The Declaration also makes provisions against mass surveillance.[56] Concerning data protection, the Declaration provides data processing principles like fairness, purpose specification, accuracy, transparency, and the establishment of data breach notification mechanisms. The African Commission on Human

[52] Malabo Convention, Article 11(6 - 8)

[53] 'Personal Data Protection Guidelines for Africa' (Internet Society) <https://www.internetsociety.org/resources/ doc/2018/personal-data-protection-guidelines-for-africa/> accessed 9 October 2021

[54] Constitution of the Federal Republic of Nigeria, 1999, Section 12

[55] The African Declaration on Internet Rights and Freedoms was launched at the 18th annual Highway Africa Conference at Rhodes University in Grahamstown, South Africa, on 7 September 2014, following a soft launch a week earlier at the Global Internet Governance Forum in Istanbul. See <http://www.article19.org/resources.php/ resource/37682/en/african-declaration-on-internet-rights-and-freedomslaunched> accessed 16 July 2021

[56] Ibid

and Peoples' Rights and the United Nations Educational, Scientific and Cultural Organization (UNESCO) are saddled with implementing the Declaration.[57]

2.1.7 Declaration on Principles of Freedom of Expression and Access to Information in Africa 2019

This Declaration is yet another effort towards data protection in Africa.[58] In 2019, the African Union Commission on Human and Peoples' Rights made a laudable initiative by recognising the right to privacy, notwithstanding the failure of the African Charter on Human and Peoples' Rights (African Charter) to recognise this right. This initiative was the Declaration on Principles of Freedom of Expression and Access to Information in Africa.[59] The Declaration elaborates on data protection in Africa and shows the region's effort towards data protection. The Declaration provides for the protection of personal information, establishes principles for data processing, and mandates the independence of data protection authority.[60]

2.2 Legislative and Regulatory Attempts on Data Protection in Nigeria

In Nigeria, there have been various attempts at enacting comprehensive data protection legislation. These attempts find expression in the multiple Bills that have come before lawmakers in Nigeria, and none have been passed into law.[61] Although one of the attempts – the Data Protection Bill of 2019 – was passed before the two legislative chambers and sent to the President for assent. However, the President declined to assent to the Bill and did not publicly provide a reason for the refusal.[62] Government agencies also attempted to

---

[57] Greenleaf G and Cottier B, 'Comparing African Data Privacy Laws: International, African and Regional Commitments' (Social Science Research Network 2020) SSRN Scholarly Paper ID 3582478 <https://papers.ssrn. com/abstract=3582478> accessed 9 October 2021

[58] 'African Commission on Human and Peoples' Rights Legalinstruments' <https://www.achpr.org/legalinstruments/ detail?id=69> accessed 9 October 2021

[59] Declaration on Principles of Freedom of Expression and Access to Information in Africa 2019 <https://www.achpr.org/public/Document/file/English/Declaration%20of%20Principles%20on%20Freedom%20of%20Expression_ENG_2019.pdf> accessed 16 July 2021

[60] Principle 40 and 42 of the Declaration

[61] T. Kio-Lawson, Right to be Forgotten", Business Day 1 June 2014 <http://businessdayonline.com/2014/06/right-to-be-forgotten/#.VF5UKjTF9yJ> accessed 16 July 2021

[62] Appraisal of the Nigeria Data Protection Bill 2019 <https://www.linkedin.com/pulse/appraisal-nigeria-data-protection-bill-2019-ridwan-oloyede/> accessed November 25, 2021.

propose a law or introduce sector-specific guidelines or regulations on data protection. [63] This section will review government policies, proposed bills, and sector regulations geared towards processing personal information.

2.2.1 Nigerian National Policy for Information Technology 2000

The Nigerian National Policy for Information Technology 2000 (IT Policy)[64] is arguably the first attempt by the Federal government to protect personal data using a policy framework.[65] One of the general objectives of the IT Policy is to promote legislation (Bills & Acts) for the protection of online business transactions, privacy, and security.[66] One of the governance plans under the policy is the ratification of a Data Protection Act to safeguard the privacy of National computerised records and electronic documents.[67]

The IT Policy places the duty on the Federal government to promote and guarantee freedom and rights to information and its use, protect individual privacy, and secure justice for all by passing relevant Bills and Acts.[68] Other laudable objectives of the policy include: to protect government data, records, and information in digital form; to establish and enforce Cyber laws to combat computer crime; to enthrone public confidence in the use, application, and sharing of information; to promote acceptable standards, authenticity and integrity in IT use nationwide; and to enhance freedom and access to digital information at all levels while protecting personal privacy.[69] The strategies for achieving this also involve the National Information Technology Development Agency (NITDA), the Ministry of Justice, and the private sector to realise the objectives of freedom of access and rights to information and privacy and confidentiality.[70]

---

[63] The National Identity Management Commission (NIMC) developed a Personal Information Protection Bill, and the National Information Technology Development Agency (NITDA) published two guidelines on data protection in 2013 and 2017.

[64] NITDA Website. https://www.researchictafrica.net/countries/nigeria/Nigerian_National_Policy_for_Information _Technology_2000.pdf

[65] NITDA Website. https://www.researchictafrica.net/countries/nigeria/Nigerian_National_Policy_for_Information_ Technology_2000.pdf

[66] Nigerian National Policy for Information Technology 2000, Paragraph 4 xxiii.

[67] Nigerian National Policy for Information Technology 2000, Paragraph 3.3, p. 6.

[68] Nigerian National Policy for Information Technology 2000, Paragraph 13.1, p. 32.

[69] Nigerian National Policy for Information Technology 2000, Paragraph 13. 2 (iv) (v) (vi) (vii) (viii), p. 32.

[70] Nigerian National Policy for Information Technology 2000, Paragraph 13.3 (ii), p. 33.

However, it is vital to note that the policy has no legal backing and is without the force of law. Also, the policy was fraught with unrealisable objectives and strategies. For instance, the vision statement of the policy aims "to make Nigeria an IT capable country in Africa and a key player in the information society by the year 2005, using IT as the engine for sustainable development and global competitiveness", yet there is a low literacy level in Nigeria. Also, the policy has not been impactful. For example, a National Information and Communication Technology (ICT) Policy 2012[71] was introduced after the 2000 Policy, but the policy does not refer to privacy and data protection.

2.2.2 Computer Security and Critical Information Infrastructure Protection Bill 2005

The Computer Security and Critical Infrastructure Protection Bill aims to address computer security and designate and protect critical information infrastructure.[72] Under Part 11, the Bill deals explicitly with how data should be retained, protected, and used. Section 4 of the Bill provides that any data retained, processed, or retrieved by the service providers like telecommunication companies at the request of any law enforcement agency shall not be utilised except for legitimate purposes. Furthermore, the utilisation of the data retained, processed, or retrieved shall constitute legitimate purpose only with the consent of individuals to whom the data applies or authorised by a court of competent jurisdiction or other lawful authority.[73] However, the Bill does not specify the 'other lawful authority.' This requirement is too broad a scope and may leave room for abuse. Another shortcoming of the Bill is that it is limited to personal data obtained from service providers like telecommunications service providers, not financial institutions or other industries.

Generally, the Bill does not adequately address data protection issues because it does not define personal data. Also, the Bill mentions data subjects' rights but does not provide for these rights. In addition, the Bill does not provide for the appointment of a regulatory body

[71] 'The Nigeria National ICT Final Draft Policy, 2012 • Page 1 • ICT Policy Africa' <https://ictpolicyafrica.org/en/ document/3fb9w5vigsn?page=1> accessed 9 October 2021

[72] Computer Security and Critical Infrastructure Protection Bill 2005 <www.cybercrime.gov.ng/site/index.php?option=com_content&task=view&id=20&Itemid=56> accessed 16 July 2021

[73] Computer Security and Critical Information Infrastructure Protection Bill 2005, Section 4

to supervise or enforce the provisions of the law (i.e., a data protection authority). Similarly, the Bill does not contemplate the circumstances where the personal data needs to be utilised without the consent of the data subjects and contains no provision on data breach notification.

2.2.3 Cyber Security and Data Protection Agency (Establishment, etc.) Bill, 2008

This Bill represents one of the earliest attempts to address data protection in Nigeria.[74] However, the provisions of the Bill had nothing to do with the security of personal information. This is because it contains no substantive provisions on data protection that are generally known in data protection law. In addition, the interpretation section of the Bill is grossly inadequate. For example, section 38 defines data as including a representation of information, knowledge, facts, concepts, or instructions intended to be processed, being processed, or has been processed in a network. This is not a proper approach to define personal data under a data protection law. Furthermore, it does not define processing which is a key concept in data protection law.

The Bill made extensive provisions on cybersecurity. It proposed the establishment of a cyber-security and information protection agency charged with the responsibility to adopt measures to eradicate the Commission of cyber-crimes and maintain a liaison with the Attorney General of the Federation and Inspector General of Police on the arrest and subsequent prosecution of the offenders.[75] However, the function of the Cyber Security Establishment and Information Protection Agency revolves around investigating and combating cybercrimes and has nothing to do with data protection as a human right.[76]

Also, a look at the Bill shows that the members that constitute the Cyber Security and Information Protection Agency are mainly government functionaries. This makes the Agency fall short in the general requirement of independence of data protection authorities. The stated functions of the Agency as prescribed by the Bill also do not fall within the scope

[74] Cyber Security and Data Protection Agency (Establishment, etc.) Bill, 2008 <https://docs.google.com/document/d/1W7pBJrb9_Z0C2RkBTlnS8LEtIuBmSzVu17655VvnqDU/edit?usp=sharing> accessed 11 October 2021

[75] Cyber Security and Data Protection Agency Bill 2008, Section 4(c)(g)

[76] Cyber Security and Data Protection Agency Bill 2008, Section 4(b)

of a typical DPA.[77] A reading of the Bill in its entirety shows that it was not intended to cater for data protection but was for cybersecurity instead. Additionally, the inclusion of the phrases "Data Protection" in the title of the Bill and "Information Protection" in the name of the Agency is misleading. Thus, while the Bill provided and contained laudable provisions on cybersecurity, it fell short of providing for the security of personal information.

2.2.4 Privacy Bill, 2009

Shortly after the Cybersecurity Bill 2008, the Privacy Bill was introduced in 2009.[78] The Bill contains provisions on data protection but does not provide the basic rules for data processing.[79] The Bill applies solely to government agencies and grants them wide powers and exemptions to collect personal data.[80] The Bill emphasised access to information rather than data protection.[81] The Bill establishes a Privacy Directorate as a supervisory agency to enforce the Bill[82] but did not provide for its independence which is an essential requirement for the effective functioning of the body. Also, the requirement that the office of the Privacy Directorate should be established under the Executive arm of government is evidence that the Bill did not provide for its independence.[83] The Bill also contains some ambiguous provisions. For example, Section 2 provides that a government institution shall not collect personal information unless it specifically relates to an operating programme or activity of the institution. Yet, what amounts to an "operating programme or activity" was neither explained nor defined in any part of the Bill.

---

[77] Cyber Security and Data Protection Agency Bill 2008, Section 2 & 4

[78] Privacy Bill 2009. <https://docs.google.com/document/d/1OB_d8PvKjfuOsOjYlpjnTXe7FhatiSNGBojL9wWJzso /edit?usp=sharing> accessed 11 October 2021; See also Abdulrauf LA, Fombad CM, Personal Data Protection in Nigeria: Reflections on Opportunities, Options and Challenges to Legal Reforms <https://repository.up. ac.za/bitstream/handle/2263/59126/Abdulrauf_Personal_2017.pdf;jsessionid=ED31E213C7F512674DE0591F3EF8413A?sequence=1> accessed 16 July 2021

[79] Privacy Bill 2009, Part IV & VI

[80] Privacy Bill 2009, Part IV & VI

[81] Privacy Bill 2009, Part V

[82] Privacy Bill 2009, Part IX

[83] Privacy Bill 2009, Section 48

2.2.5 Data Protection Bill, 2010

The Data Protection Bill 2010 was another attempt to enact data protection legislation in Nigeria.[84] The Bill provides rights to data subjects.[85] These include the right to access personal data,[86] prevent processing likely to cause damage or distress,[87] prevent processing for direct marketing purposes,[88] rights concerning automated decision-making[89] and rights to rectification, blocking, erasure and destruction.[90] In addition, the Bill provides data protection principles such as lawfulness and fairness[91], purpose limitation,[92] data minimisation,[93] data accuracy[94], storage limitation[95] and security[96]. Furthermore, the Bill prohibits the transfer of personal data to a country outside Nigeria, except the recipient country has adequate protection for the rights and freedoms of data subjects.[97] However, the Bill did not provide criteria for determining what will amount to an adequate level of protection or who will carry out the adequacy assessment.

Although Section 10 of the Bill provides elaborate provisions on what constitutes sensitive personal data, the Bill does not contain any extra safeguards surrounding such data processing. Also, the objective of the Bill is couched in a somewhat ambiguous fashion. The Bill's provision on scope and application does not state if it applies to private and public agencies. The Bill does not provide for a supervisory agency, as is the case under the Privacy Bill 2009 considered above. It also failed to provide an exemption for journalistic, national security, and public interest processing personal data. Finally, the Bill

---

84 Data Protection Bill 2010 <https://docs.google.com/document/d/1jqUNZXkJNZgItcEzjoFXrEPNAW2Ok22pb6 QxrDqkbNI/edit?usp=sharing> accessed 11 October 2021

85 Data Protection Bill (2010), Section 1 (1)(e)

86 Data Protection Bill (2010), Section 2

87 Data Protection Bill (2010), Section 3

88 Data Protection Bill (2010), Section 4

89 Data Protection Bill (2010), Section 5

90 Data Protection Bill (2010), Section 7

91 Data Protection Bill 2010 section 1(1) (a)

92 Data Protection Bill (2010), Sections 1(1) (b)

93 Data Protection Bill (2010), Section 1(1)(c)

94 Data Protection Bill(2010),Section 1(1)(d)

95 Data Protection Bill(2010),Section 1(2)

96 Data Protection Bill (2010), Section 1 (3)

97 Data Protection Bill (2010), Section 1(4)

lacks an enforcement framework and merely creates offences without stipulating punishments.[98]

2.2.6 Personal Information and Data Protection Bill, 2012

The Personal Information and Data Protection Bill[99] was proposed by the National Identity Management Commission (NIMC)[100] as part of its initiatives on data protection in Nigeria. Broadly, the Bill seeks to establish rules on the processing of personal information in a manner that recognises the right to privacy of individuals concerning their data. It also recognises the need for organisations to process personal data for purposes that a reasonable person will consider appropriate.[101] However, the requirement of reasonableness gives a wide gamut to entities to extend the scope of their processing on reasonableness, which is highly subjective. The Bill applies to organisations and every person that collects, uses, or discloses personal data during commercial activities.[102] Also, Section 2(2) of the Bill excludes government institutions from its application which is contradictory since the NIMC, a government institution, is the sponsor of the Bill. This implies that the Bill does not apply to the NIMC, an organisation carrying large-scale personal data processing activities.

Furthermore, the Bill provides for the data processing principles but provides them under Schedule 1 of the law rather than in the main text of the Bill. Under Section 4.1, the Bill provides for the establishment of the Office of the Privacy Commissioner;[103]however, this provision does not grant immunity and independence to the Commissioner, as is the case in the ECOWAS Act, the Malabo Convention and Declaration on Principles of Freedom of Expression and Access to Information in Africa. Other issues with the Bill include: it does not provide rules on transborder flow of personal data. Furthermore, although data subjects

[98] Data Protection Bill (2010), Sections 8(3) (4) (5)

[99] Personal Information and Data Protection Bill 2012 <https://www.nimc.gov.ng/docs/reports/personal_info_bill.pdf> accessed 16 July 2021

[100] The NIMC is a government agency with the mandate to establish, own, operate, maintain, and manage the National Identity Database in Nigeria". It is also to register persons within the scope of the Act and assign
Unique National Identification Number (NIN). Furthermore, the NIMC also is to issue National Identity Cards to Nigerians.
See <https://www.nimc.gov.ng/> accessed 16 July 2021

[101] Personal Information and Data Protection Bill 2012, Section 1

[102] Personal Information and Data Protection Bill 2012, Section 2(1)

[103] Personal Information and Data Protection Bill 2012, Section 4.1

are allowed to file complaints concerning violations of their rights under the Bill when it comes to enforcing these rights, the remedies are limited to resolving complaints through dispute mechanisms such as mediation and conciliation. Finally, it does not provide criminal justice sanctions for violation of the Bill, and it prioritises consent over other lawful basis. It is also important to mention in concluding that there are several inconsistencies in the Bill. One such inconsistency is that the Bill refers to personal health information in its definition section but nowhere else in the Bill was this mentioned. Noteworthy is that in 2016 the Bill was rendered moot.

2.2.7 National Guidelines on Data Protection 2013

The National Guidelines 2013 was made by the National Information Technology Development Agency (NITDA) under Section 6 of the NITDA Act.[104] Section 6 of the Act articulates the functions of the Agency, including the power to develop guidelines.[105] The Guidelines cover the processing of personal data wholly or partly by automatic means. It also covers non-automatic processing of personal data that form part of a filing system or are intended to form part of a filing system. However, the Guidelines did not cover the processing of personal data processing operations concerning public security, defense, national security, and the nation's activities in areas of criminal law.[106] Furthermore, the Guideline articulates principles to guide the processing of personal data.[107]

The Guidelines also creates an obligation on organisations to designate a particular employee as a "Data Security Officer" whose duties will be to ensure that the organisation adheres and complies with privacy policies and procedures, ensure that individual data is protected, and provides effective oversight for the collection and use of personal information.[108] The Officer will also be responsible for adequate data protection and

[104] National Information Technology Development Agency Act 2007 < https://nitda.gov.ng/wp-content/uploads/2020/11/NITDA-ACT-2007-2019-Edition1.pdf> accessed 16 July 2021

[105] Ibid

[106] Draft National Guidelines on Data Protection 2013, Paragraph 1.3. (1) (2).

[107] Draft National Guidelines on Data Protection 2013, Paragraph 3.1

[108] Draft National Guidelines on Data Protection 2013, Paragraph 2.4.1.

management within that organisation, training and educating employees on compliance with the privacy and data security policies, and developing recommended practices and procedures to ensure compliance.[109]

However, it is noteworthy that while NITDA placed reliance on Section 6 of the NITDA Act to develop the Guidelines, this power is questionable. This is because Section 6 does not expressly state "data protection, security or privacy" as subject matters in which NITDA is authorised to develop guidelines. It is therefore doubtful whether the Agency can make it a data protection guideline in this regard.

2.2.8 Electronic Transactions Bills

Different versions of this proposed law have been mooted at the two federal legislative houses. Mainly to regulate the emergence of electronic commerce and transactions, recognise the use of electronic signatures, among other things. But, unfortunately, none of the various versions of the law ever made it to law. Part of the proposals under these Bills includes the protection of personal data.

2.2.8.1 Electronic Transactions Bills 2010

In 2010, an Electronic Transactions Bill 2010 (SB. 446) was introduced and sponsored by eleven members of the Senate.[110] The objectives of the Bill are to provide a legal and regulatory framework for conducting transactions using electronic or related media, protecting consumers' rights and other parties in electronic transactions and services, protecting personal data, and facilitating electronic commerce in Nigeria.[111]

The Bill was made to provide legal recognition for electronic commercial transactions where parties have accepted to contract through electronic means, either expressly or by conduct.

---

[109] Ibid

[110] Electronic Transactions Bill 2010 <https://www.ictpolicy.org/uploads/Electronic%20Transactions%20Act,% 202010.pdf> accessed 16 July 2021. A list of the sponsors of the Bill are contained in the body of the Bill. The sponsors are Senator Nkechi Nwaogu, Senator Felix K. Bajomo, Senator James E. Manager, Senator Ayo Arise, Senator Chimaroke Nnamani, Senator Audu Idris Umar, Senator Ahmad M. Maccido, Senator Patricia N. Akwashiki, Senator Gbenga Ogunniya, Senator Patrick E. Osakwe, and Senator Mohammed A. Muhammed.

[111] Electronic Transactions Bill 2010, Section 1

However, the Bill contains data protection provisions to cater to the data protection issues arising from electronic transactions. The Bill provides a list of six lawful bases for the processing of personal data and entrenches data processing principles.[112] In addition, the Bill recognises the right of data subjects to be informed of data processing activities where the data subject has made a request and any other relevant information.[113] However, under Section 20(2), the Bill makes the right to information subject to administrative fees. This provision is right restricting as it is contrary to the right of information.

Furthermore, the Bill grants data subjects the right to object to the processing of their data for direct marketing purposes.[114] It places a duty on data holders to implement appropriate technical and organisational measures and exercise reasonable care to protect personal data against accidental or unlawful destruction or accidental loss and against unauthorised alteration, processing, disclosure, or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing.[115] Under Section 25, the Bill provides that the National Information Technology Development Agency consult with any appropriate regulatory body and develop rules and guidelines for Nigeria's data protection.

However, the provisions of the Bill do not comprehensively address data protection in Nigeria. This lapse can be attributed to the fact that the Bill was not originally made to cater to data protection. For instance, it does not provide for administrative and enforcement machinery for the operation of the Bill, such as a data protection authority. Similarly, the Bill does not provide some important rights of data subjects. For example, the Bill does not account for the right to object to the use of personal data for direct marketing purposes, the right to require data controllers to ensure that no decision based solely on automated processing significantly affects data subjects, and the right to require data controllers to rectify, block, erase or destroy personal data in certain circumstances.

[112] Electronic Transactions Bill, 2010, 18 & 18(1)
[113] Electronic Transactions Bill, 2010, 20(1) (2)
[114] Electronic Transactions Bill, 2010, 21(1)
[115] Electronic Transactions Bill, 2010, 23(1)

2.2.8.2: Electronic Transactions Bill 2015

The Electronic Transactions Bill 2015 (SB. 015) was introduced and sponsored by Senator Hope Uzodinma.[116] The objectives of the Bill are to provide a legal and regulatory framework for conducting transactions using electronic or related media, protecting consumers' rights and other parties in electronic transactions and services, protecting personal data, and facilitating electronic commerce in Nigeria.[117]

Like the Electronic Transactions Bill 2010, the Bill was not originally made to cater to data protection, but it contains data protection provisions to address the data protection issues arising from electronic transactions. The Bill contains similar provisions to the previous Bill but introduces amendments to avoid ambiguity. Under Section 18(1)(5), the Bill makes additions to Section 18(1)(5) of the 2010 Bill. The Bill provides that personal data shall not be saved or stored for longer than necessary to fulfil the purpose for which it was obtained. Also, the Bill deleted Section 20(2) of the 2010 Bill, which makes the right to information subject to the payment of administrative fees.

However, like the 2010 Bill, the Bill does not comprehensively address data protection in Nigeria. This lapse is also attributable to the fact that the Bill was not originally made to cater to data protection. For instance, it does not provide for the establishment of a data protection authority. Also, it does not provide for some important rights of data subjects. Issues such as the right to consent to the use of personal data for direct marketing purposes, the right to require data controllers to ensure that no decision based solely on processing by automatic means significantly affects data subjects, and the right to require data controllers to rectify, block, erase, or destroy the Bill does not consider personal data in certain circumstances.

Another version of the Bill made it to the legislature in 2013 and another in 2017.[118] In 2019, two attempts were made to reintroduce the 2015 Bill. An Electronic Transactions Bill,

---

[116] Electronic Transactions Bill 2015< https://www.ictpolicy.org/uploads/TheElectronicTransactionBill2015% 20NIGERIA.pdf.> This information was obtained from the body of the Bill.

[117] Electronic Transactions Bill 2015, Section 1

[118] Conference of Committee on Electronic Transaction Bill, https://placng.org/i/wp-content/uploads/2019/12/Report-of-the-Conference-Committee-on-Electronic-Transactions-Bill-2017.pdf 26 August 2021

2019 (SB 155) was introduced and sponsored by Senator Ibikunle Oyelaja Amosun at the Senate House. The Bill is currently awaiting the report of the Banking Insurance and Other Financial Institutions Committee of the Senate.[119] In the same year, an Electronic Transaction Bill, 2019 (HB 384) was introduced into the House of Representatives by Honourable Uzoma Nkem Abonta.[120] The Bill is currently at the stage of the first reading.

2.2.9: Digital Rights and Freedom Bills

2.2.9.1. Digital Rights and Freedom Bills 2015

In 2015, the Net Rights Africa Coalition of civil society organisations, led by Paradigm Initiative, developed and presented a Digital Rights and Freedom Bill to the Nigerian government.[121] The Bill provided for a broad range of digital rights, including the right to data protection, freedoms of online expression, opinion and information, the right to peaceful online assembly and association, and safeguarding human rights regarding surveillance and interception of communication.[122] In addition, the Bill makes it the duty of government agencies to ensure compulsory digital literacy both in school and out of school.[123] The Bill placed service providers under a strict responsibility to protect the privacy rights of owners against violation. It recognised the need to compensate victims of illegal surveillance and provided for enforcement of victims' rights. The Bill makes it an offence for any person to undertake illicit surveillance of communications and imposes a prison term of 10 years or a payment of compensation, not less than 7 million Naira (₦7,000,000) or both.

The right to online privacy is protected under this Bill.[124] The Bill covers the data and information privacy of every Nigerian. Any entity that holds the data of any Nigerian, including data in the cloud, is made accountable to such citizens under the provisions of

[119] Placbillstrack, 2017. <https://placbillstrack.org/view.php?getid=6699> accessed 16 July 2021

[120] Placbillstrack, 2017. <https://placbillstrack.org/view.php?getid=6807> accessed 26 August 2021

[121] Paradigm Initiative Nigeria, Press Release: Presentation of Digital Rights and Freedom Bill, 23 April 2015, https://paradigmhq.org/pin-andnetrightsng-coalition-presents-digital-rights-and-freedom-bill/ accessed 26 August 2021; see also Policy and Legal Advocacy Centre, Digital Rights and Freedom Bill Analysis, 2016, <https:// placbillstrack.org/view.php?getid=1801> accessed 26 August 2021

[122] Digital Rights and Freedom Bill 2015, Sections 1(3), 1(4), 8, 9, 15

[123] Digital Rights and Freedom Bill 2015, Section 10

[124] Digital Rights and Freedom Bill 2015, Section 1(1)

this Bill.[125] The Bill addresses the safeguard of freedom of expression online and provides that concerns about hate speech should not be abused to discourage citizens from engaging in legitimate democratic debate on matters of general interest.[126] It makes it the duty of the courts to make a distinction between, on the one hand, genuine and serious incitement to extremism and, on the other hand, the right of individuals (including journalists and politicians) to express their views freely.

The Bill was passed by both Houses of the National Assembly in April 2019 and was presented to the President for assent.[127] The President, however, declined assent explaining that "the scope of the bill should be limited to the protection of human rights within the digital environment to reduce the challenge of duplication and legislative conflict in the future."[128] Also, that the Bill "covers too many technical subjects and fails to address any of them extensively."[129]

2.2.9.2 Digital Rights and Freedom Bills 2019

In 2019, owing to the President's refusal of the 2015 Digital Rights and Freedom Bill, a new Bill was presented as a revision of the 2015 Bill. The 2019 Bill unbundled data protection and the provisions concerning surveillance, monitoring and interception while focusing on human rights within the digital environment. The revised Bill was presented in the House of Representatives as a new Bill known as the Digital Rights and Freedom Bill, 2019. The Bill is currently awaiting the report of the Committee of the Whole House.

The Bill's objective is to, amongst other things, promote the freedoms of expression, assembly and association online; guarantee the fundamental privacy rights of citizens in the use and development of technologies. It also seeks to affirm the freedom and constitutional right to communicate freely without fear of undue monitoring and interference, accord data protection more priority, guarantee human rights offline and

[125] Digital Rights and Freedom Bill 2015, Section 2

[126] Digital Rights and Freedom Bill 2015, Section 7

[127] Solomon Fowowe, Buhari Declines Assent to Digital Rights Bill, Four Others, The Guardian Nigeria, 20 Mar 2019, <https://guardian.ng/news/buhari-declines-assent-to-digital-rights-and-freedom-bill-four-others/> accessed 26 August 2021

[128] Adeboye Adegoke, Digital Rights and Privacy in Nigeria <https://ng.boell.org/sites/default/files/2020-08/Digital%20Rights%20and%20Privacy%20in%20Nigeria_0.pdf> accessed 26 August 2021

[129] President Buhari has rejected a bill seeking to protect the rights of internet users in Nigeria from infringement| Pulse <https://www.pulse.ng/bi/politics/buhari-rejects-digital-rights-bill-a-bill-seeking-to-protect-the-rights-of-internet/zztwxz1> accessed 26 August 2021

online, provide sufficient safeguards against abuse and provide opportunities for redress.[130] The provisions of this Bill apply throughout the Federal Republic of Nigeria.[131]

The Bill protects the online privacy of Nigerians by prohibiting unlawful interference with an individual's online privacy.[132] It requires that personal data be kept in confidence by imposing a statutory duty of confidentiality on anyone handling personal data.[133] The Bill allows private data requests as long as it complies with laid down legal procedures.[134] The Bill imposes an obligation on organisations to ensure confidentiality and integrity of information by putting technical and organisational measures to secure data.[135] The Bill recognises exceptions to the right to online privacy.[136] They are the administration of criminal justice or crime prevention purposes. This must, however, comply with the provisions of the Nigerian Constitution.[137]

The Bill guarantees other rights such as the right to anonymity,[138] freedom of expression online and the expression of opinion online,[139] the right to peaceful assembly and association online,[140] freedom of information online,[141] and the freedom to learn.[142] However, it also entrenches students' privacy regardless of where learning occurs[143] and the right to create public knowledge.[144]

However, it is essential to note that there are conflicts between some provisions of the Bill and other laws. For example, while the Bill permits anonymous access to the internet except where it threatens the public interest, the Cybercrimes Act, 2015 makes it an offence to use any device to avoid detection or prevent identification where there is an intention to commit a crime. Also, the provision of the Bill that allows disclosure of personal data with a warrant by a court of law after the individual has been notified may be whittled down by the Mutual Assistance in Criminal Matters Act, 2016, which allows the interception of telecommunications, share stored communication or other types of electronic data with

130 Digital Rights and Freedom Bill 2019, Section 1
131 Digital Rights and Freedom Bill 2019, Section 2
132 Digital Rights and Freedom Bill, 2019, Section 3
133 Digital Rights and Freedom Bill, 2019, Section 3(7)
134 Digital Rights and Freedom Bill, 2019, Section 3(8)
135 Digital Rights and Freedom Bill, 2019, Section 3
136 Digital Rights and Freedom Bill, 2019, Section 3(1)
137 Digital Rights and Freedom Bill, 2019, Section 3(10)
138 Digital Rights and Freedom Bill, 2019, Section 4
139 Digital Rights and Freedom Bill, 2019, Section 5 & 6
140 Digital Rights and Freedom Bill, 2019, Section 8
141 Digital Rights and Freedom Bill, 2019, Section 7
142 Digital Rights and Freedom Bill, 2019, Section 9
143 Digital Rights and Freedom Bill, 2019, Section 10
144 Digital Rights and Freedom Bill, 2019, Section 11

third party states as part of a mutual legal assistance arrangement. Finally, the exceptions to the right to anonymity under the Bill provides an opportunity for misinterpretation and may create loopholes.

2.2.10 Data Protection Bill 2016

The Data Protection Bill 2016 (HB. 02) was introduced in the 7th National Assembly by House member Honourable Yakubu Dogara and was yet another legislative attempt towards data protection in Nigeria.[145] The Bill seeks to make provision for the Regulation of the processing of information relating to individuals.

Under Section 1, data subjects have the right to access personal information being processed by or on behalf of a data controller. However, the Bill provides that a data controller shall not be obliged to comply with a request to supply any data unless adequate information is available. For example, the controller may reasonably require identifying the person making the request and locating the information that the person seeks.[146]

The Bill recognises the rights of data subjects to object to direct marketing and automated decision-making.[147] The principles guiding data processing are provided in the Bill. The Bill makes an offence, the unlawful access to personal data.[148] In seeking to protect personal data, the Bill guarantees the right of an individual whose data resides in the custody of the data controller to seek redress in a court of law.[149] However, the Bill is silent on which court should be the court of the first instance. Furthermore, the Bill does not provide for establishing the office of a data protection authority to enforce its provisions, nor does it impose an obligation on the data controller to appoint a data protection officer. In addition, the Bill omitted many safeguards that are found in modern data protection laws.

2.2.11 Data Protection Bill 2017

This Bill is sponsored by Senator Ahmad Ibrahim Lawan and makes provisions for regulating information relating to individuals.[150] The Bill provides that personal data shall be:

[145] https://placbillstrack.org/8th/view.php?getid=1130
[146] Data Protection Bill 2016, Section 2
[147] Data Protection Bill 2016, Sections 6 & 7
[148] Data Protection Bill 2016, Section 10
[149] Data Protection Bill 2016, Section 4
[150] Data Protection Bill 2017, Section 1.

processed fairly and lawfully; obtained for only for one or more specified purposes, and shall not be further processed in any manner incompatible with that purpose or those purposes; adequate, relevant, and not excessive concerning the purpose or purposes for which they are processed; accurate and where necessary kept up to date;[151] processed following the rights of the data subject; and shall not be kept longer than is necessary. In addition, appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and accidental loss or destruction of, or damage to, personal data.

The Bill provides that personal data shall not be transferred to another country or territory unless that country or territory ensures an adequate level of protection for the rights and freedom of data subjects concerning the processing of personal data.[152] It also grants to the data subject certain rights concerning the processing of personal data.[153] However, the Bill does not provide for creating a data protection authority to enforce its provisions, nor does it impose an obligation on the data controller to appoint a data protection officer to ensure compliance with the Bill. In addition, the Bill lacks legal and internal safeguards that are found in modern data protection laws.

2.2.12 National Data Protection Guidelines 2017

The Guidelines were issued by the National Information Technology Agency (NITDA). The Guidelines were made under Section 6 of the NITDA Act.[154] Under Section 6, the NITDA Act articulates the functions of the Agency, including the power to develop guidelines.

According to the NITDA, the Guidelines acts as a guide for organisations and persons that control, collect, and store the personal data of Nigerian residents and citizens within and outside the country.[155] The Guidelines define personal data as "any information relating to an identified or identifiable natural person ("data subject"); information relating to an individual, whether it relates to their private, professional or public life. It provides 11

[151] Data Protection Bill 2017, Section 1 (1) (d).

[152] Data Protection Bill 2017, Section 1 (2) (3) (4).

[153] Data Protection Bill 2017, Section 2.

[154] https://nitda.gov.ng/wp-content/uploads/2020/11/NITDA-ACT-2007-2019-Edition1.pdf

[155] 'Whiter the NITDA Data Protection Guidelines 2017?' (African Academic Network on Internet Policy - AANoIP, 21 October 2018) <https://aanoip.org/whiter-the-nitda-data-protection-guidelines-2017/> accessed 20 September 2021

principles that should guide data processing.[156] Under the Guidelines, the processing of sensitive personal information is only acceptable in certain instances.[157]

The Guidelines provide the factors that will determine the adequate level of protection to be put in place by another country.[158] This level of protection shall be assessed in light of all the circumstances surrounding a data transfer operation or set of data transfer operations. The circumstances include consideration of the nature of the data, the purpose and duration of the proposed processing operation or operations, the rules of law, both general and sectorial, in force in the receiving country, and the professional rules and security measures that are complied with within the country. These rules and measures must not be lower than what is provided in the Guidelines.

The Guidelines provide that relevant authorities shall enforce its provisions like NITDA or any other statutory authority. The lack of specificity on what "any other statutory authority" means leaves room for wide interpretation.[159]Also, NITDA is an executive agency with a narrow statutory scope. The Agency's powers are limited to the powers granted under the NITDA Act. Thus, the designation of NITDA as an authority does not replace the need for an independent data protection authority.

Furthermore, the Guidelines do not provide an enforceable right of redress for data subjects or the means to obtain redress. Moreover, the Guidelines are silent on the compensation for data subjects and sanctions where the Guidelines are violated. Finally, like the 2013 Guidelines, Section 6 of the NITDA Act, where the Agency purportedly derives the power to make the 2017 Guidelines, is questionable and raises doubt as to the capacity of the Agency to do so.

2.2.13 Data Protection Bill 2018

Following the public hearing of the Senate Committee on Judiciary, Human Rights and Legal Matters, the Committee mandated a review of the Data Protection Bills of 2016 and 2017 to propose a harmonised Data Protection and Privacy Bill.[160] Further to this recommendation, the Federal Ministry of Justice, with the support of the GLACY+ Project of the Council of Europe and the European Union, the Cybercrime Advisory Council and the

[156] Data Protection Guidelines 2017, Section 6-12, 15-17 and 27

[157] Data Protection Guidelines 2017, Section 14

[158] Data Protection Guidelines 2017, Section 28

[159] Data Protection Guidelines 2017, Section 33

[160] Request for comments and observations on draft data protection and privacy bill, 2018 and invitation to 1-day validation workshop <draft_dataProtection_ privacyBill.pdf (nimc.gov.ng)> accessed 26 August 2021

Experts Group of the Senate Committee on ICT and Cybersecurity, held a Data Protection Legislative drafting workshop in September 2018.[161] Participants reviewed the drafts according to international standards and best practices at the workshop and produced a Data Protection Bill 2018. The Data Protection Bill, 2018, emanated from several recapitulations going back to 2014, namely, the Personal Information and Data Protection Bill 2014, the Data Protection Bill 2015, and the Protection of Personal Information Bill 2016.

The objective of the Bill was to protect the rights of data subjects and prevent abuse and misuse of data.[162] The Bill applies to public and private entities processing personal data either by automated or non-automated means within Nigeria.[163] The Bill contains the established principles of data processing[164] and the legal bases for data processing.[165] In addition, the Bill introduced privacy by design and default,[166] prescribed obligations for both data controllers and processors,[167] increased the rights of data subjects[168] and allowed notification of both data subjects and the Supervisory Authority in the event of a data breach.[169] Also, the Bill imposes a fine of five million Naira where the personal data is obtained unlawfully without the controller's consent.[170]

The Bill establishes a Data Protection Commission to act as the Supervisory Authority to implement and enforce the law.[171] However, under Section 8, the management structure of the Commission comprises some government agencies. The implication is that the Commission will, arguably, have no independence to carry out its functions. This contradicts the ECOWAS Act,[172] Malabo Convention and Declaration of Principles on

[161] Ibid
[162] Data Protection Bill 2018, Section 1
[163] Data Protection Bill 2018, Section 2(1) & (2)
[164] Data Protection Bill 2018, Section 3 (1) (a-f)
[165] Data Protection Bill 2018, Section 4(1) and (2)(a-e)
[166] Data Protection Bill 2018, Section 31, 33 and 34
[167] Data Protection Bill 2018, Section 17-26
[168] Data Protection Bill 2018, Section 35
[169] Data Protection Bill 2018, Section 32
[170] Data Protection Bill 2018, Section 48(1)(c)
[171] Data Protection Bill 2018, Section 7
[172] ECOWAS Supplementary Act, Article 14(2)

Freedom of Expression and Access to Information in Africa, requiring the Data Protection Authority to be an independent administrative authority. Furthermore, the ECOWAS Act[173] and the Malabo Convention[174] provide that members of the data protection authority shall be incompatible with government membership.

Similarly, Article 15(5) of the Modernised Convention 108[175] also provides that the data protection supervisory authorities exercise their functions with complete independence without instructions from any other entity. These provisions are tailored towards ensuring the independence of the authority from government influence and control. However, the Constitution of the Commission under the Data Protection Bill, 2018 contradicts this.

The Data Protection Bill provided some commendable provisions and made it through all the legislative stages. However, in May 2019, when the National Assembly forwarded the Bill to the President for assent, the President refused its assent, and no reason was found for the refusal.

2.2.14. Data Protection Bills 2019

In 2019, two Data Protection Bills were presented before the House of Representatives, a Data Protection Bill 2019 (HB 504) sponsored by Hon. Nduidi Godwin Elemelu and a Data Protection Bill 2019 (HB 564) sponsored by Hon. Yakubu Dogara. Both Bills have not progressed beyond the first reading. At the Senate, a Protection of Personal Information Bill, 2019, sponsored by Senator Stella Oduah, is also currently stuck at its first reading.

2.2.15. Data Protection Bill, 2020

The Data Protection Bill 2020[176] is currently the most recent and most comprehensive data protection initiative in Nigeria. Hence, the need to discuss the provisions of the Bill under this section. The Federal Government introduced the Bill through the Legal and Regulatory Reform Working Group (LWG), constituted in March 2020. This was in furtherance of the

[173] ECOWAS Supplementary Act, Article 16

[174] African Union Convention, Article 11(6)

[175] Modernised Convention for the Protection of Individuals with Regard to the Processing of Personal Data 2018 <https://search.coe.int/cm/Pages/result_details.aspx?ObjectId=09000016807c65bf > accessed 26 August 2021

[176] Data Protection Bill 2020 <https://www.ncc.gov.ng/documents/911-data-protection-bill-draft-2020/file> accessed 23 July 2021

Federal Government's implementation of the Nigeria Digital Identification for Development (ID4D) Project.[177]

The objectives of the Bill are primarily to establish an effective regulatory framework for the protection of personal data, regulate the processing of information concerning data subjects and safeguard their fundamental rights and freedoms guaranteed under the 1999 Nigerian Constitution.[178] It aims to promote the code of practice that ensures privacy and data protection without undermining the interest of commercial organisations and government agencies in respect of such data.[179] In addition, the Bill seeks to minimise the effects of misuse and abuse of personal data, establish an impartial regulatory authority and ensure personal data is processed fairly and lawfully.[180]

The Bill applies to the processing and use of personal data of both Nigerian citizens and persons residing in Nigeria by automated or non-automated means.[181] This means that the Bill also extends to the processing of both electronic and non-electronic data. The Bill extends to personal data processed by private and public organisations resident in Nigeria.[182] It applies to data controllers and processors of personal data where they are both established in Nigeria and the personal data of the data subjects processed within whether the data subject resides in or outside Nigeria.[183] Other instances where the Bill applies is where a data controller is not established in Nigeria but uses equipment or a data processor in Nigeria to process data of subjects resident within or outside Nigeria; or where processing is carried out in respect of data of subjects that reside in or outside Nigeria and such data originates partly or wholly from Nigeria.[184] However, the Bill does not apply to

[177] 'A Review of The Nigerian Data Protection Bill 2020 - Privacy - Nigeria' <https://www.mondaq.com/nigeria/privacy-protection/983116/a-review-of-the-nigerian-data-protection-bill-2020> accessed 9 October 2021
[178] Data Protection Bill 2020, Section 1
[179] Data Protection Bill 2020, Section 1(a)
[180] Data Protection Bill 2020, Section 1(b)-(d)
[181] Data Protection Bill 2020, Section 2(1) (a)
[182] Data Protection Bill 2020, Section 2(1) (b)
[183] Data Protection Bill 2020, Section 2(1) (c) (ii & iii)
[184] Data Protection Bill 2020, Section 2(1) (c) (iv)

the processing of personal data carried out by a data subject while performing a purely personal or household activity.[185]

2.2.15.1: Key Provisions of the Bill

(a) Basic Principles and Lawful Basis for Processing Personal Data

The Bill provides the basic principles and legal basis for processing personal data by a data controller or processor. Personal data must be processed for a specific, explicit, and legitimate purpose and in a lawful, fair, and transparent manner.[186] Other bases include contract, compliance with a legal obligation, protection of vital interests of a data subject or another person, or a prevailing legitimate interest pursued by the data controller or a third party.[187] The provisions are the same as the ones provided by NDPR, except that it includes legitimate interest.

(b) Establishment of a Regulator

The Bill established a Regulator with powers and defined mandate better than what is obtainable under the NDPR. It created the office of the Data Protection Commission and a governing body for the Commission.[188] The governing board is made of stakeholders in the data protection community and government agencies.[189] However, the governing body's constitution with Ministries and government agencies considered part of the executive is contrary to principles under international instruments on the constitution of an independent agency. For example, Article 16 of the ECOWAS Data Protection Implementation Act provides that members of a data protection authority are incompatible with government membership.[190] The Bill empowers the Commission to implement and monitor compliance with the provisions of the Bill, make administrative arrangements which it believes are appropriate to discharge its duties, investigate complaints based on the Bill, make regulations, apply to the court for a warrant, impose fines and penalties and generally

[185] Data Protection Bill 2020, Section 2(2)
[186] Data Protection Bill 2020, Section 3(1) (a-h)
[187] Data Protection Bill 2020, Section 4(1)(2) (a-e)
[188] Data Protection Bill 2020, Section 7 and 8
[189] Data Protection Bill 2020, Section 8(a-f)
[190] See Article 11(6) of African Union Convention on Cybersecurity and Persona Data Protection

perform its responsibilities with the aid of enforcement agencies.[191] In addition, the Commission is required to make regulations for the licensing and certification of data protection compliance officers and organisations.[192] Thus, the Commission will replace the role that NITDA has played to date in terms of data protection regulation.

(c) Rights of the Data Subjects

The Bill provides for the rights of data subjects similar to those contained in the NDPR except that the Bill introduces the right regarding automated processing, a judicial remedy, the right to notification, and the right to have data processing suspended.[193] The Bill States that these rights may only be limited by the provisions of Section 38, which empowers data subjects to request an assessment from the Commission to determine whether processing complies with the Act.[194]

(d) Processing of Sensitive Data

The Bill includes the personal data of children among sensitive data and prohibits the processing of sensitive data except certain conditions are met.[195] These conditions include consent (in the case of a child under parental control, prior consent of the parent or guardian is required before processing) or where processing is necessary.[196] Section 26 (3–7) of the Bill provides instances where processing may be necessary. In addition, it provides that sensitive data relating to race or ethnic origin should not be processed except where it is necessary to identify and eliminate discriminatory practices and with appropriate safeguards for the rights and freedoms of the data subject.[197]

Furthermore, religious organisations founded on religious or philosophical principles are allowed to process sensitive personal data if it relates to their members, employees, or

[191] Data Protection Bill 2020, Section 10
[192] Data Protection Bill 2020, Section 9(j)
[193] Data Protection Bill 2020, Section 18 - 25
[194] Data Protection Bill 2020, Section 17(1) and (2)
[195] Data Protection Bill 2020, Section 26(1) (a-b)
[196] Data Protection Bill 2020, Section 26(2) (a-b)
[197] Data Protection Bill 2020, Section 26 (7)

other persons belonging to the organisations; where it is consistent with the objects of the institutions; and where it is necessary to achieve the aims and objectives of such institutions.[198] Under Section 29, the Bill further provides compensation for the data subject where they suffer harm arising from an infringement by the data controller or where processing is contrary to the provisions of the Bill. For the data controller or processor, proof that they took reasonable care in all cases to comply with the requirement of the Bill suffices as a defence.

(e) Duties of Data Controllers and Data Processors

The Bill sets out the duties of data controllers and processors under Section 30(1). Where a data controller engages a processor, the controller will be vicariously liable.[199] There must, however, be a legally binding contract between both parties. A data controller is required to employ only a data processor who provides sufficient guarantees to implement appropriate technical and organisational measures, considers the data controller's obligations, and ensures the protection of the rights and fundamental freedoms of the data subject.[200] Data Controllers are required to appoint a Data Protection Officer responsible for ensuring adherence to the Bill. However, this is subject to the Regulation made by the Commission.

(f) Administration and Enforcement

Section 36 of the Bill introduces the concept of an Enforcement Notice and vests in the Commission the power to issue such notices to data controllers or processors, where they have contravened or reasonable belief of likely contravention of the data protection principles under the proposed Act. The notice is issued to restrain a data controller or processor from processing the person's data described in the notice.

(g) Trans-Border Flow of Personal Data

[198] Data Protection Bill 2020, Section 27(1)(a)
[199] Data Protection Bill 2020, Section 31(3)
[200] Data Protection Bill 2020, Section 31(2)

According to the Bill, the transborder transfer of personal data may only occur where an adequate level of protection based on the Bill is secured in the recipient State or international organisation. The transborder transfer of personal data may also happen where the data subject has given explicit, specific and free consent, after being informed of risks arising in the absence of appropriate safeguards, where the data subject's interests require it; and for prevailing legitimate interests. The aim is to eliminate the bottlenecks that may arise in fulfilling the international transfer of data.

(i) Offences and Penalties

The Bill criminalises the unauthorised collection, disclosure, and retention of personal data, sale of personal data, and negligence in protecting data. It imposes a fine of 5 million Naira and imprisonment for a year for unlawful collection, disclosure, and retention of personal data.[201] In addition, the Bill imposes a penalty of one million Naira for the illegal sale of personal data or imprisonment for five years to run concurrently.[202] In the case of unlawful advertisement of personal data, a fine of N500,000 Naira per record or imprisonment of five years is imposed to run concurrently.[203] It further criminalises situations where a breach is caused by the negligence of the data controller or processors by imposing a fine of 10 million Naira for every year of default or imprisonment of not less than one year.[204] In addition to imposing sentences, the court may give an order to the convicted person to forfeit its asset, money and equipment used to or intended to be used to commit the offence to the Federal Government.[205] The Bill also provides a Court of law to grant orders to compensate victims of violations by convicted persons.[206]

2.2.15.2 Inadequacies of the Bill

(a) Derogation of Data Protection on Ground of Public Policy

[201] Data Protection Bill 2020, Section 44
[202] Data Protection Bill 2020, Section 44(3)
[203] Data Protection Bill 2020, Section 44(4)
[204] Data Protection Bill 2020, Section 45(1)
[205] Data Protection Bill 2020, Section 49(1)
[206] Data Protection Bill 2020, Section 50(2)

It has been argued that the negation of data protection on the grounds of public policy is too broad and may grant the government enough freedom to trample on the principle of data protection to the detriment of data subjects.

(b) Clarity on Duties of DPO and DPCO

The Proposed Bill did not give detailed information about the roles of DPO and DPCO. A more description of their role will help enthrone clarity on the significance of such entities. In addition, section 30 (e) creates the obligation to conduct a data protection impact assessment but fails to specify the situations that will trigger the assessment.

(c) Journalistic, Literary or Artistic Expression

The Bill did not make copious provisions exempting the application of the Regulation to journalistic, literary or artistic expression. The use of "legitimate interests" in Section 23 is loose and does not include the interest of journalists or news agencies to report freely. Also, Section 25 does not define "public interest" to include the interests of journalists or news agencies. A review is important to ensure that freedom of expression is not stampeded. The absence of journalistic exceptions will deny journalists the opportunity to report on news of public benefit for fear of infringing the data protection law.

(d) International Transfer of Data

Section 43(1) of the Bill provides that data can move outside Nigeria to another country with adequate protection but fails to specify how the adequacy decision will be determined.

(e) Stringent Conditions for Processing

Section 26(4)(c) requires the swearing to an affidavit to process sensitive personal data. In emergencies, this could be dangerous, especially if there is a vital interest of the data subject. The lawful basis for processing sensitive personal data under Section 26 are limited and omit scenarios where the data subject has made the data manifestly public, public interest in the area of public health or emergency and preventive and occupational medicine.

(f) Notification for Data Breach

The Bill only specifies the obligation to notify the data subject within 48 hours of discovery after informing the Commission. There is a need to clarify the timeline to notify the Data Protection Commission when a breach can result in high risk and danger to the data subjects.

3.0: Examination of Existing Framework

3.1: Nigerian Data Protection Regulation (NDPR) 2019

The National Information Technology Development Agency (NITDA) on 25 January 2019 issued Nigeria Data Protection Regulation as the primary legislation guiding data protection in Nigeria. NITDA claims its power over data protection on its authority under Section 6 of the NITDA Act.[207] Under this Section, NITDA is vested with the power to develop guidelines. Particularly, Section 6(c) provides its power to issue guidelines for electronic governance and monitor the use of electronic data interchange and other forms of electronic communication transactions where electronic communication may improve the exchange of data and information.

The objective of the NDPR is to protect the rights of natural persons, among other things.[208] In November 2020, NITDA released the Data Protection Implementation Framework (DPIF)[209] as an addendum to the NDPR, mainly to clarify the provisions of the NDPR[210] and promote a shared understanding of the NDPR to promote voluntary compliance.[211] Therefore, the framework should be read in conjunction with the NDPR and relevant laws applicable to it and do not supersede the NDPR.[212]

The NDPR applies to every transaction involving the processing of personal data by automated or non-automated means regarding natural persons in Nigeria and Nigerian citizens residing outside Nigeria.[213] The Regulation does not apply to:

a) The use of personal data in furtherance of national security, public health, safety, and order by agencies of the Federal, State, or Local government or those they expressly appoint to carry out such duties on their behalf;

[207] NITDA Website. <https://nitda.gov.ng/wp-content/uploads/2020/11/NigeriaDataProtectionRegulation11.pdf> accessed 26 August 2021
[208] Nigeria Data Protection Regulation 2019, Section 1.1
[209] NITDA Website. <https://nitda.gov.ng/wp-content/uploads/2021/01/NDPR-Implementation-Framework.pdf> accessed 26 August 2021
[210] Implementation Framework 2020, Article 2 & 1.1
[211] Implementation Framework 2020, Article 1.2
[212] Implementation Framework 2020, Article 2
[213] Nigeria Data Protection Regulation 2019,Article 1.2 (a) (b)

b) The investigation of criminal and tax offences;

c) The collection and processing of anonymised data; and

d) Personal or household activities with no connection to a professional or commercial activity.[214]

It is important to note that NDPR does not directly provide for these exceptions, but Article 2.1 of the Implementation Framework expressly states the exceptions to give meaning to the provision of NDPR.

Noteworthy is that in 2020, NITDA issued Guidelines for the Management of Personal Data for Public Institutions in Nigeria.[215] The Guidelines govern the roles and responsibilities of public officers and public institutions regarding the processing and managing personal data in compliance with the Nigeria Data Protection Regulation.

3.1.1: Key Provisions of the Regulation

Some provisions of the Regulation are discussed below:

(a) Principles of Data Processing

Article 2.1 of the Regulation sets out guiding principles for the lawful processing of personal data. Data controllers are responsible for complying with the principles in the Regulation. These principles are lawfulness, purpose limitation, data minimisation, accuracy, storage limitation, integrity, and confidentiality. However, data processing principles like fairness, transparency, and accountability are not specifically provided under the NDPR.

(b) Lawful Bases for Processing

The Regulation provides under Article 2.2 that processing of personal data shall be unlawful unless there is a legal basis for such processing. Article 2.2(a–e) of the NDPR provides five lawful bases: consent, contract performance, vital interest, the performance of a public task, and legal obligation.

The Regulation does not include legitimate interest as a lawful basis. Thus, it may seem that a data controller or processor in Nigeria cannot rely on legitimate interest as a lawful

[214] Implementation Framework 2019, Article 2.1

[215] NITDA Website. <https://nitda.gov.ng/wp-content/uploads/2020/11/GuidelinesForImplementationOfNDPR InPublicInstitutionsFinal11.pdf> accessed 26 August 2021

basis for processing the personal data of data subjects. On the other hand, though, Article 16 of the Implementation Framework provides that provisions of GDPR and other international laws can be persuasive where there is a gap in the provision of NDPR. This tends to weaken the Regulation and leave its interpretation open to conjectures.

(c) Data Transfers to a Foreign Country

Article 2.11 provides that transborder transfer of personal data outside Nigeria may occur where the recipient country has adequate data protection law. The Regulation empowers the Agency to determine the adequacy of data protection of the recipient country.[216] However, Article 2.12 provides exceptions where personal data can be transferred if the recipient country does not have adequate data protection law. These include:

1. Where data subject gives explicit consent to the proposed transfer, after having been informed of the possible risks of such transfers;
2. where a transfer is necessary for the performance of a contract between the Data Subject and the controller or the implementation of pre-contractual measures taken at the Data Subject's request;
3. where a transfer is necessary for the conclusion or performance of a contract concluded in the interest of the Data Subject between the controller and another natural or legal person;
4. where a transfer is necessary for important reasons of public interest;
5. where a transfer is necessary for the establishment, exercise or defence of legal claims; and
6. where a transfer is necessary to protect the Data Subject's vital interests or of other persons, where the Data Subject is physically or legally incapable of giving consent.

In all these circumstances, the Data Subject must be made to understand the specific principle(s) of data protection that is likely to be violated in the event of transfer to a third country. However, this proviso does not apply where the data subject is required to initiate or defend a legal claim, whether civil or criminal, in a third country.[217]

(d) Data Subjects Rights

The Regulation under Article 3.1 provides for the rights of data subjects, and they include the right to access, portability, restriction of processing, rectification, erasure, lodge complaint, object to a decision made solely on automated processing.

[216] Nigeria Data Protection Regulation 2019, Article 2.11(a)
[217] Nigeria Data Protection Regulation 2019, Article2.12 (a-f)

(e) Data Protection Compliance Organization (DPCO)

The Regulation created the Data Protection Compliance Organisation (DPCO), licensed entities responsible for supporting organisations with compliance to the NDPR.[218]This provision is novel and introduces a new player into the institutional framework of the data protection ecosystem.

(f) Obligation to Appoint Data Protection Officer (DPO)

The Regulation under Article 4.1(2) mandates every data controller to appoint a DPO. Despite this, Article 3.4.1 of the Implementation Framework lists when a controller is expected to appoint a DPO. The DPO is responsible for managing the privacy program and ensuring the organisation is complying with the NDPR. The DPO should possess the professional expert and requisite knowledge and understanding of the applicable data protection law to carry out the duties. A DPO shall not be liable for the organisation's non-compliance with applicable data protection laws.[219]

(g) Data Controller and Processor's Obligation

Article 3.2 of the Implementation Framework made copious provisions of the obligations of data controller and processor. It mandates them to conduct a data protection audit where the controller processes more than 2000 personal data, process data only on a legally justifiable cause, and ensure appropriate technical and organisational measures to protect the rights of data subjects as provided in Article 2.2 of the NDPR.

(h) Sanction and Enforcement

Article 2.10 of the Regulation provides sanctions when someone breaches the "data privacy rights" of any data subject, in addition to any other criminal liability. The Regulation in Article 4.2 empowers the Agency to administer and enforce the Regulation. Accordingly, the Agency may impose a fine of up to ₦10,000,000 or 2% of annual turnover where the Controller processes more than 10,000 personal data. A fine of ₦2,000,000 or 1% of yearly turnover may also be imposed if the controller processes less than 10,000 personal data.

[218] Nigeria Data Protection Regulation 2019, Article 1.3(iii)

[219] Implementation Framework 2019, Article 3.6

The Agency may decide to go with whichever is greater.[220] In issuing monetary sanctions, the Agency shall follow an administrative process that complies with the principles of fair hearing and judicial safeguards. Relying on their power, NITDA has so far, within two years, sanctioned three institutions that are found to have breached data subjects' rights.[221]

(i) Criminal Prosecution

NITDA has determined that a party violates the NDPR, especially where such breach affects national security, sovereignty, and cohesion. Accordingly, it may seek to prosecute officers of the organisation as provided for in section 17(1) (3) of the NITDA Act 2007.

In addition to the obligations above, the DPIF introduced new obligations to conduct a data protection impact assessment for specific processing activities, rules on cookies, introducing new bases for the international transfer of data, all, which are not contained under the NDPR.

3.1.2: Inadequacies of the Regulation

Despite the safeguards contained in the Regulation, some of its provisions fall short of the international standard on data protection. The territorial scope of the Regulation is problematic and will be difficult to enforce. The Regulation applies to Nigerians outside Nigeria. It appears muddled the concept of extraterritorial applicability of laws. Some of these include:

(a) Subsidiary legislation

The NDPR is subsidiary legislation and not an Act of a legislative house and cannot substitute for a data protection law. However, the authors have stated earlier in this report that the provision of the law NITDA leans on to issue previous Guidelines and the NDPR is not so clear. Hence, it may be responsible for the revision under the proposed amendment to the Act establishing NITDA.

(b) Independence of Regulator

[220] Nigeria Data Protection Regulation 2019, Article 2.10(a)(b)

[221] The latest being the ₦10 000,000 (Ten Million Naira) fine on Soko Lending Company Limited. 'NITDA Sanctions SokoLoan for Privacy Invasion – NITDA' <https://nitda.gov.ng/nitda-sanctions-soko-loan-for-privacy-invasion/> accessed 9 October 2021

The Agency is not established as an independent data protection supervisory authority, as is the case under international instruments such as Article 11 and 12 of Malabo Convention, Article 1(3) and 14 of the ECOWAS Supplementary Act and Principle 42 of the Declaration of Principles on Freedom of Expression and Access to Information in Africa. Similarly, NITDA's board is made up of executive members, and the membership of the executive arm of the government is incompatible with the independence of the authority.

(c) Absence of Legitimate Interest

The Regulation surprisingly omitted legitimate interest as one of the lawful bases for processing. Legitimate interest is an important legal basis. It is flexible and can apply in wide circumstances, especially where other lawful bases are not appropriate. The omission will create hardship for controllers and operationalisation problems. Things like fraud prevention, network and information security or some business to business contact will typically leverage legitimate interest, and the other lawful bases are not appropriate.

In a contrasting move, the Agency introduced a new lawful basis, the legitimate interest of the data subject under Guidelines on the Use of Personal Data by Public Institutions.[222] However, aside from the failure to define what this means or how it is meant to work, it may be difficult to establish a possible scenario where a public authority can solely decide what amounts to the legitimate interest of a data subject.

(d) Controller Obsessed

The Regulation tends to be obsessed with the controller. However, many of the duties, including those supposed to be left for or done by the processor, were still assigned to the controller. There is no distinction in the controller's responsibilities from the processors as contained in Article 3.2 of the Implementation Framework.

(e) Inconsistency in the Use of terminology

The Regulation uses both personal data and personal identifiable information interchangeably. Thus, it is unclear which of the terms the NDPR intended to use. This is because the concept of personal data is wider and includes personal information capable of identifying an individual indirectly. Also, the Regulation uses administrator and processor in both the Regulation and the Implementation Framework inconsistently.

(f) International Transfer of Data Conundrum

[222] Article 2.2 (f) Guidelines on the Use of Personal Data by Public Institutions

Article 2.11 of NDPR, Article 7.1 of the DPIF requires the Agency to list countries with adequate data protection law available. According to this provision, the Agency published a whitelist of countries considered to have an adequate law.[223] However, the drawing up of the safelist does not comply with the requirement stated in Article 2.11 of the NDPR. This Article provides that NITDA must consider the legal system, the recognition of fundamental rights, enforcement procedure, judicial system, and international collaborations before placing it under the whitelist. Rather, the Agency provided a list of countries without considering the requirement under Article 2.11.

For example, Namibia is mentioned on the list, yet it does not have a data protection law. Similarly, the list also includes all signatories to the Malabo Convention – for example, Comoros is a signatory but has yet to enact a data protection law. Moreover, both countries are yet to set up their supervisory authority in a sense conceived under Article 2.11 (d) of the NDPR.[224]Another example is Togo and Algeria, which has laws but have yet to establish their authorities. A non–profit initiative is currently challenging the flawed whitelist.[225] Further, it is surprising that NITDA favoured the signatories of the Convention over the countries that ratified.

In addition, the DPIF introduced Binding Corporate Rules (BCR) and Standard Contractual Clauses (SCC) for transfer within a group of entities.[226] First, there is no basis for these mechanisms when they are not specifically mentioned under the NDPR. Second, the nature of SCC was misconceived as it can be used to transfer data outside a group of companies.

(g) Cookies consent rule

Though the NDPR did not specifically say anything about cookies, the Implementation Framework specified that only consent could be used as a lawful basis to instal cookies on a user device.[227] Though the Implementation Framework did not make a distinction between strictly necessary cookies and other types of cookies. The Implementation Framework suggests that the continuous use of the website constitutes valid consent, which

[223] Data Protection Implementation Framework 2020, Annexure 3

[224] 'Highlight of the NDPR Implementation Framework' <https://www.linkedin.com/pulse/highlight-ndpr-implementation-framework-ridwan-oloyede-> accessed 9 October 2021

[225] 'Nigeria International Transfer of Data Framework - A Call for Reassessment' (*ikigaination.org*, 21 September 2021) <https://ikigaination.org/nigeria-international-transfer-of-data-framework-a-call-for-reassessment/> accessed 22 October 2021.

[226] Article 7.3 DPIF

[227] Article 5.6 DPIF

is contrary to the conditions for valid consent under Article 2.3 of NDPR and Article 5.1 of DPIF. Consent of a user cannot be implied.[228]

(h) Absence of Journalistic Exception

The NDPR and its accompanying DPIF did not include journalistic exceptions as one of the derogations. This omission will make it difficult for media and the press to report on news content beneficial in the public's interest for fear of violation of data protection law. In addition, the absence could suppress the expression of freedom of expression online and offline and press freedom.[229]

(i) Rule of Imposition of Sanction

Article 2.10 of NDPR specifies that violation of a data subject "data privacy" right will incur the financial sanction under the Regulation. It is unclear if a violation of the NDPR that does not impact the "data privacy" right of the data subject is punishable. For example, failure to file an audit report has nothing to do with data subject rights. In addition, the provision used the numerical threshold of data subjects affected to determine the severity of the sanction. While the number of people affected by the Regulation violation is one of the factors, it is not the only metric. For example, a far lesser number of data subjects whose genetic data is impacted will be considered more severe compared to a loss of names. When imposing fines, the Regulator should consider other factors. For example, the nature, gravity and duration of the infringement; the purpose of the processing; the number of the data subject concerned; level of damage and damage mitigation measures implemented; intent or negligence; degree of cooperation with the Commission; and categories of personal data.

(j) Insufficient Protection of Sensitive Personal Data

---

[228] Cookies, Consent, Contradictions, and the Implementation Framework (*African Academic Network on Internet Policy* - 2021) <https://aanoip.org/cookies-consent-contradictions-and-the-implementation-framework/> accessed November 25, 2021.

[229] The intersection of the right to freedom of expression online and protection of personal information in Botswana, Ethiopia, Kenya, and Nigeria. < https://techhiveadvisory.org.ng/wp-content/uploads/2021/09/Africa-ReportFoEDP.pdf> accessed 25 November 2021

The NDPr defined sensitive personal data under Article 1.3 (xxv) but did not make any specific provision for its protection. However, the DPIF specifies consent as the only lawful basis for processing sensitive personal data.[230] The apparent restriction on the use of consent for all situations requiring sensitive personal data will make operationalisation of the law difficult when a different lawful basis would have been sufficient.

3.1.3 Two Years of the NDPR: A Review

Aside from the inadequacies of the Regulation, it has recorded some success, even if these achievements are not monumental. For example, NITDA has expended a lot of time and resources in ensuring compliance with the NDPR by enforcing requirements such as the data protection compliance audits filing (with a database of at least 635 entities that have filed their statutory audit reports).[231] The Agency is also doing a remarkable job of raising awareness through organising events and partnering with organisations.

The Agency also announced it commenced active investigations into cases of alleged non-compliance and data breaches by public and private entities. According to the NDPR Performance Report, 15 violations have been investigated.[232] First, in September 2019, NITDA commenced a probe into the call-filtering service, Truecaller, for alleged breach of Nigerian users' data protection rights. Then, in December 2019, NITDA began investigating the Lagos State Internal Revenue Service for suspected violation of taxpayers' data in the state and eventually imposed a punitive fine of NGN 1 million (approx. €2,180).[233]

According to the 2020 NDPR Performance Report,[234] the Agency had issued about 230 compliance and enforcement notices. As a result, it released the Guidelines on the Use of Personal Data by Public Institutions. The Guidelines provide how public institutions should

[230] Article 5.3.1 (b) DPIF

[231] NITDA Performance Report 2020. <https://nitda.gov.ng/wp-content/uploads/2021/03/NDPR-Lite-Performance-Report-2O19-2O2O.pdf> accessed 20 August 2021

[232] Ibid

[233] 'NITDA to Investigate Breach of Data Protection Regulation by Lagos State Internal Revenue Service' (The Guardian Nigeria News - Nigeria and World News, 28 December 2019) <https://guardian.ng/news/nitda-to-investigate-breach-of-data-protection-regulation-by-lagos-state-internal-revenue-service/> accessed 9 October 2021

[234] Ibid

process personal data. It mandates every public institution to appoint a data protection officer and conduct data protection impact assessment assessments (DPIA), among other things, for every significant data processing project.

The publication of the performance report is a laudable one on the part of the Regulator as it presents them as being transparent. Recently, NITDA fined Electronic Settlement Limited, a Fintech company, five million Naira (₦5 000,000.00) for the data breach.[235] Also, Sokoloan has been fined the sum of Ten million (₦10,000,000) for the data breach, and the company has been placed under a six–month information technology oversight.[236]

Nonetheless, amidst the progress highlighted in the preceding paragraphs, there are also instances where the Regulator did not conclude an investigation. For example, in July 2019, after the Nigeria Immigration Service posted the biodata page of a citizen on its Twitter handle, NITDA was quick to issue a statement about investigating the violation.[237] However, two years and a few months on, NITDA is yet to issue the outcome of its investigation. Similarly, the Agency appears not to act when the violation concerns another federal government agency. For example, the Economic and Financial Crimes Commission (EFCC) was alleged to have violated the NDPR. EFCC, in July 2019, launched a crime–fighting mobile application (App) that will allow people to report suspected crime by sharing pictures of a property suspected to be acquired illegally or a suspect with the EFCC through the App.[238] The App lacked a privacy notice, and it is also embedded with advertisement trackers monitoring the behaviour of users and sharing with advertisers. The App has over

[235] Punch.ng, 'NITDA Imposes N5m Fine on Fintech for Data Breach',16 March 2021: https://punchng.com/nitda-imposes-n5m-fine-on-fintech-for-data-breach/ accessed 23 July 2021

[236] NITDA, 'NITDA Sanctions Soko Loan for Privacy Invasion' <https://nitda.gov.ng/nitda-sanctions-soko-loan-for-privacy-invasion/> accessed 23 July 2021

[237] "NITDA Commences Investigation on Alleged Breach of NDPR" (*Vanguard News*July 12, 2019) <https://www.vanguardngr.com/2019/07/nitda-commences-investigation-on-alleged-breach-of-ndpr/> accessed November 25, 2021.

[238] "EFCC Launches 'Crime-Fighting' Mobile App" (*Channels Television*January 3, 2015) <https://www.channelstv.com/2021/07/14/efcc-launches-eagle-eye-mobile-app/> accessed November 25, 2021.

10,000 downloads at the time of this report. NITDA is yet to issue a public statement or a sanction despite a report filed in September 2021.[239]

3.3: Other Laws and Regulations Impacting Data Protection

Aside from the Nigeria Data Protection Regulation, which specifically addresses data protection in Nigeria, there are other sector-specific interventions that contain provisions addressing data protection in Nigeria.[240] Furthermore, Guidelines, Regulations and Frameworks have also been made under certain principal Acts like the National Identity Management Commission Act 2007, the Nigerian Commissions Act 2003 and the Nigeria Data Protection Regulation 2019.[241]

3.4 Other developments

The absence of a comprehensive data protection law enacted by the federal legislature has led some states to consider regulating the protection of personal information. In October 2021,[242] the Lagos State government Data Protection Bill passed the second reading stage and a public hearing was held in November 2021.[243] However, the proposed law has a wide territorial scope that will bring organisations not located in Lagos within its regulatory purview, creating operationalisation problems for organisations and potential conflict with existing NDPR. In addition, the Bill includes the obligation to register with the State

---

[239] "Eagle Eye: A Violation of the Right to Privacy - Ikigaination.org" (*ikigaination.org*September 21, 2021) <https://ikigaination.org/eagle-eye-a-violation-of-the-right-to-privacy/> accessed November 25, 2021.

[240] They include the Freedom of Information Act 2011, the Cybercrimes (Prohibition, Prevention, etc.) Act 2015, the National Child Rights Act 2003, the HIV and AIDS (Anti-Discrimination) Act 2014, the Credit Reporting Act 2017, the National Health Act (NHA) 2014 , the Wireless Telegraphy Act 1998, the Nigerian Commissions Act 2003, the National Identity Management Commission Act 2007, the Nigeria Police Act, 2020, the Federal Competition and Consumer Protection Act (FCCPA) 2018, the Companies and Allied Matters Act 2020, Labour Act, National Minimum Wage Act 2019, Employees Compensation Act 2010, Personal Income Tax (Amendment) Act 2011, Trafficking of Persons (Prohibition) Enforcement and Administration Act 2015, Violence Against Persons Prohibition Act 2015, and the Money Laundering (Prohibition) Act 2003.

[241] Consumer Code of Practice Regulations 2007, the Central Bank of Nigeria Consumer Protection Framework 2016, the Nigeria Communications Commission (Registration of Telephone Subscribers) Regulations 2011, the Data Protection Implementation Framework 2019, the Guidelines for Provision of Internet Services for Internet Service Providers, the Lawful Interception of Communications Regulation 2019, the National Cybersecurity Policy 2021, Guidelines for the management of personal data by Public Institutions 2020, and Guidelines for Nigerian Content Development in Information and Communication Technology (ICT).

[242] Lagos Data Protection Bill Scales Second Reading (*Premium Times Nigeria* October 25, 2021) <https://www.premiumtimesng.com/regional/ssouth-west/491701-lagos-data-protection-bill-scales-second-reading.html> accessed November 25, 2021.

[243] Akinwunmi King. Lagos Assembly Meets Experts, Stakeholders over Data Protection Commission Bil (*Independent Newspaper Nigeria*November 18, 2021) <https://independent.ng/lagos-assembly-meets-experts-stakeholders-over-data-protection-commission-bill/> accessed November 25, 2021.

Regulator and renew annually. More significantly, the new rules on the international transfer of data could create chaos and conflict with existing national rules. For example, the authorisation of the State Regulator is required to transfer data outside Nigeria.[244]

In addition, in 2018, the Central Bank of Nigeria (CBN) requested a draft Data Protection Regulation contribution. Unfortunately, much has not been heard from the effort, but it may be brought back to life considering the antecedent of the CBN to introduce secondary regulatory instruments. Ogun State has a similar legislative proposal from the executive to enact a law on privacy, but at the time of this report, it is yet to be presented before the State legislature. Nevertheless, the approach could be a trend, and more states governments and regulators may consider enacting their laws.

Finally, in November 2021, a publication concerning a request for a proposal was made to draft a new data protection law and subsidiary legislation for Nigeria. The advert suggests a departure from the Data Protection Bill 2020.[245]

[244] "Ikigai Innovation Initiative Contributes Its Quota to the Lagos State Data Protection Bill 2021 - Ikigaination.org" (*ikigaination.org*November 22, 2021) <https://ikigaination.org/ikigai-innovation-initiative-contributes-its-quota-to-the-lagos-state-data-protection-bill-2021/> accessed November 25, 2021.

[245] Tosin Omoniyi, "Data Protection: Indignation as FG Abandons Draft Bill, Seeks 'Consultants' for Fresh Process" (*Premium Times Nigeria*November 17, 2021) <https://www.premiumtimesng.com/news/top-news/495768-data-protection-indignation-as-fg-abandons-draft-bill-seeks-consultants-for-fresh-process.html> accessed November 25, 2021.

4.0: Major Highlights

- Nigeria has had a long and plaid history in its attempt to enact data protection legislation. Evidence of attempts to pass a comprehensive regulation started as far back as 2005. However, findings reveal that the journey is still ongoing with the draft Data Protection Bill 2020. While the various attempts are a step in the right direction, the push of the Nigerian government towards comprehensive legislation is slow. It also shows that policymakers do not view data protection as a priority issue that should be given serious attention.
- Nigeria is yet to ratify any of the international instruments, and they both currently have no force of law in the country.
- While the NDPR, though subsidiary legislation, contains some data protection provisions, the Regulation's review shows that it has some challenging provisions that might negatively impact data protection. Similarly, the draft Data Protection Bill 2020 possesses inherent lapses that must be addressed to enable Nigeria's robust data protection regime.
- The Nigerian government is embarking on a new endeavour to draft a new data protection Bill from scratch, which will reverse the seeming progress made and delay the country's comprehensive data protection law.
- State governments and regulators are making an effort at enacting or introducing their data protection laws or regulations. However, the multiplicity of effort will create conflict and operational difficulty due to a lack of common standards.

5.0: Recommendations

The following embody recommendations from this report on key steps that need to be taken by state actors, policymakers and legislators, and non-state actors like civil society organisations and activists, researchers, and academia, towards promoting data privacy protection in Nigeria.

For Government

- There should be a concerted effort and collaboration between experts and relevant stakeholders for a comprehensive legal framework for personal data protection in Nigeria.
- Experts and stakeholders should ensure that a legal framework for personal data protection is informed and tailored towards tackling the emerging challenges of a data-driven society Nigeria is fast becoming.
- There is a need for judicial activism and proactiveness by the Nigerian judiciary towards data protection. Also, expertise and knowledge through training should be available for the judges to enforce and uphold existing law.
- The executive should ensure the data protection authority that will be established is independent in funding, control and there should be no interference with their activities. In addition, knowledgeable and competent individuals should be appointed to the independent authority.

For Policymakers and Legislators

- There is a need to establish an independent Data Protection Authority to oversee the enforcement and implementation of data protection. However, for the body to carry out its duty, it must function independently and impartially.
- There should be a provision for a review mechanism and the stated period when a review should be carried out in data protection laws. This review should be aimed at addressing the advances in technology and the changes in data protection issues.
- The legislature should be made aware of the importance of data protection to the whole mandate of human rights protection and should ensure the combined efforts of all stakeholders towards a timely production of comprehensive legislation.
- There have been various uncoordinated attempts, as can be gleaned from this report. Thus, there is a need for coherent and unified policies and initiatives geared towards data protection.

- The policymakers should diligently consider the comments and opinions of interested persons on the lapses and improvements that should be made to the Data Protection Bill, 2020.
- Legitimate interest should be included as a lawful basis for processing personal data.
- Journalistic, artistic and literary exceptions should be included to preserve the freedom of expression.
- Words, phrases and terminologies should be adequately defined and used consistently,

For Civil Society Organisations and Activists

- There should be investment by civil societies and activists in cutting-edge research that will promote the understanding of data protection in Nigeria.
- Civil societies and activists should collaborate with relevant stakeholders to ensure the production of data protection legislation that provides comprehensive human rights provisions.
- There should be a deployment of public sensitisation and various legal and advocacy tools on the importance of enacting comprehensive data protection legislation and its timely delivery.
- There should be strategic litigations to challenge government excesses and the provisions of certain laws that restrict or derogate from international human rights principles.

For Researchers, Academia and Philanthropy Organisations

- It is recommended that they carry out more contextually relevant research on the need for comprehensive legislation.

  Research should be conducted to highlight the gaps in the Regulation and the operationalisation of the law. Research should also be conducted to understand the extent of violation of the right and their impact on people.

6.0: Conclusion

This report reviewed and analysed Nigeria's legislative and regulatory journey towards a comprehensive data protection regulation. A review of this nature is critical in Nigeria's history, considering the increasing importance attached to personal data in a digital age and the risks its unregulated processing poses to individuals. Therefore, the report reflected on the development of data protection within the international, regional and domestic contexts. In keeping with the objective of the report, we reviewed and analysed Nigeria's legislative and regulatory attempts towards data protection, fundamental provisions, improvements, and shortcomings. Our review of the legal regime of data protection in Nigeria concluded that the existing framework does not cater to Nigeria's growing data protection issues considering the rapid advances in information technology and the digital economy. This report noted that current regulations are weak and lacking may not stand the test of time given the sophistication of Nigeria digital space. Furthermore, we identified and analysed some of the provisions that should inform comprehensive data protection reforms. Finally, recommendations were made to different stakeholders.