EXAMINING THE JUDICIAL ATTITUDE TO DATA PROTECTION IN NIGERIA*

Abstract

In recent times, the subject of data privacy and data protection has become widely topical in Nigeria particularly amongst legal practitioners leading to an array of seminars, conferences, as well as researches with a view to developing the jurisprudence on the subject matter. Unlike several of its western and a few of its African counterparts, Nigeria just had its first comprehensive data protection law which came into effect on 12th day of June 2023. However, before the Nigeria Data Protection Act (NDPA) came into force, the courts have played a role towards data protection or at least, towards privacy protection. This article enquires into the attitude of Nigerian courts towards data protection prior to the enactment of the NDPA 2023. The study employed a doctrinal methodology and an analytic approach in its discourse. The paper reviewed ten cases on data protection and privacy related matters and found that the attitude of the courts is mainly positive towards data protection in Nigeria. It recommended inter alia, the continued adoption of a human rights-based approach towards data protection matters.

Keywords: Data Protection, Judicial Attitude, Case Law, Nigeria

1. Introduction

From time immemorial, humans have recognized and acknowledged the existence of the unique traits and characteristics which constitute the personhood of an individual. In other words, though there are core biological, physiological and physical identifiers which differentiate humans from animals on a broad spectrum, yet, there are unique traits and features which separate one human from the other. These traits otherwise known as data include personal details such as names, images or pictures, voice, facial features, private numbers and addresses (including phone, home or office) etc. On the basis of identity, every individual is entitled to a claim to his personhood and one should not be allowed to invade the private or personal space of another without invitation or permission. Indeed, it has been stated that personal information protection is an integral part of fundamental rights architecture.[1] Closely linked to this background of personal identity is the legal right to privacy officially recognised and protected by Constitutions and democracies all over the world. The right to privacy is deemed a fundamental right which should not be disregarded by governments, corporations and citizens alike. However, there have been violations of these rights particularly, in ways or forms which were uncommon in earlier times. The dawn of rapid technological advancements and the internet era have introduced digital ways of trumping the fundamental rights of citizens. Indeed, the concept of digital right owes its origins to the unprecedented technological incursion into almost every conceivable human endeavour including human rights.[2] It has been argued that contrary to the impression that digital rights are new sets of rights, they are rather, the replication of legal rights on the internet and digital platforms.[3]

Furthermore, the continuous emergence of intrusive technologies has posed a serious challenge to privacy rights. This has led to several data breaches on a huge scale. Several companies, including Uber and Facebook have been victims of cyber-attacks.[4] Another example is that of the Truecaller App which requested more information than necessary from users, including their geo-location, IP address, device ID, SIM card usage, applications installed on users' devices, screen resolution, device address book, browser, operating system, and more and gave these details to third parties.[5] See also the case of yahoo in 2016,[6] and Alibaba in 2018.[7] These recurrent data breaches call for enhanced legal mechanisms and judicial activism for data protection.

*By Ikenga K. E. ORAEGBUNAM, PhD (Law), PhD (Philosophy of Law), PhD (Religion and Society), PhD (Edu, in view), BL, Professor of Law and Applied Jurisprudence, and Formerly Head, Department of International Law and Jurisprudence, Faculty of Law, Nnamdi Azikiwe University Awka, Nigeria, Email: ikengaken@gmail.com; ik.oraegbunam@unizik.edu.ng. Tel: +2348034711211; and

Tega EDEMA, LLB, BL, LLM, PhD Candidate, Faculty of Law, Nnamdi Azikiwe University, Awka; Law Lecturer, Admiralty University of Nigeria, Ogwashi-Uku. Email: tegaedema342@gmail.com. Tel: 08133518440.

[1]Emeka Ekweozor, 'An Analysis of the Data Privacy and Protection Laws in Nigeria' *SSRN* <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3639129> accessed 5 November 2023

[2] Solomon Okedara, Olumide Babalola and Irene Chukwukelu , *Digital Rights in Nigeria through the Cases* (Luminate, Lagos, 2022) 9

[3]*ibid*, 9

[4] Techworld Staff, 'The most infamous data breaches', (2018) in DM Chika and ES Tochukwu, 'An Analysis of Data Protection and Compliance in Nigeria', *International Journal of Research and Innovation in Social Science (IJRISS)* 2020 4(5) 377

[5]Emmanuel Paul, 'NITDA Investigating Alleged Privacy Breach by Truecaller' *Techpoint Africa*, (25 September, 2019) <https://techpoint.africa/2019/09/25/nitda-truecaller-privacy-breach/> accessed 1 November 2023

[6] Robert Mcmillan ,'Yahoo Says Hackers Stole Data from 500 Million Accounts in 2014' *Wall Street Journal* (22 September, 2016) <https://www.wsj.com/articles/yahoo-says-information-on-at-least-500-million-user-accounts-is-stolen-1474569637> accessed 16 November 2023

[7]Micheal Hill and Dan Swinhoe, "The 15 biggest data breaches of the 21st Century", CSO (08 November 2022) in Francis Udeme Udoh, 'Privacy Rights in Nigeria: Prospects and Challenges in the Digital Era' [2022] *Lawsan Uniuyo Journal*

2. Conceptual Clarification

Data privacy

This is also referred to as information privacy. It is a strategic goal that seeks to guarantee the confidential and personally identifiable information stored on computer systems. It is also aimed at ensuring that data in transit and data at rest are always protected, while still allowing the flow of information.[8] Data privacy relates to keeping information confidential either through regulations, policies or initiatives by regulatory bodies or by the data subjects themselves deciding who should have access to such information and what such persons can do and not do with the information.[9] Generally, the right to data privacy emerged because of the need to protect individuals from risks associated with the automated or manual processing of their personal information.[10]

Data Protection

Data protection is said to have stemmed from the right to privacy and can be regarded as a tool through which the law protects an individual from abuse of his personal information by another person.[11] It involves implementing measures to safeguard data from unauthorized access, loss, alteration, or destruction. Etzoni[12] defines data protection as the protection of personal data of individuals and the free flow of personal data, in a manner that facilitates the promotion and protection of human rights in general and data privacy in particular.[13] The protection of personal data is primary to the exercise of the right to privacy and family life.

Distinction between Data Protection and Privacy

As noted by an author,[14] although sometimes used interchangeably, data privacy and data protection are distinct concepts. However, it is important to observe that whereas data protection (largely) ensures privacy, privacy does not ensure protection. It is then necessary to ensure the privacy of data by protecting same.[15] Data privacy is an aspect of data security and involves procedural and legal considerations, whereas data protection considers technical factors in ensuring privacy. Data privacy relates to keeping information/data confidential either through regulations, policies or initiatives by regulatory bodies or by the data subjects themselves deciding who should have access to such information about them and what such persons can do and not do with the information.[16] Data protection on the other hand appears to have been a derivative of privacy. Data protection, conversely, deals with the mechanism put in place by the recipients of data to ensure the 'protection' of the information or data. This deals with the aspect of ensuring the privacy of personal data rather than the privacy of the data itself.[17]

3. Judicial Response towards Data Protection in Nigeria: Case Law Review

Despite the fact that the Nation has had no comprehensive and specific data protection law, the Courts which is the arbiter of justice and fondly regarded as the last hope of the common man, has adjudicated on several cases relating to privacy and data protection as outlined below:

Digital Rights Lawyers Initiative (DRLI) v. National Identity Management Commission (NIMC)[18]

The Appellant challenged the Defendant's imposition of a N15, 000 levy on persons seeking rectification of their personal data in the national data base contending that rectification of personal data is a data subject's right under the

[8]Margaret Rouse, 'What is Data Privacy' in MA Ozekhome, 'Data Protection and Privacy in the Age of Digital Justice: Balancing Security and Individual Rights (paper presented at the Conference of West African Law Students Association, Abuja, on 4th September, 2023)

[9]Abraham Aigba, 'Protection of the Personal Data of Athletes in Sports', *Linkedin* <https://medium.com/@abrahamaigba/protection-of-the-personal-data-of-athletes-in-sports-ce39e638db4> accessed 18 November 2023

[10] Lukman Adebisi Abdurlrauf, 'The Legal Protection of Data Privacy in Nigeria: lessons from Canada and South Africa', (PhD Thesis of the Faculty of Law of the University of Pretoria, 2015)

[11] GVZH Advocates, 'Data Protection Vs. The Right to Privacy', <https://gvzh.mt/malta-law/data protection/vs-the-right-to-privacy/> in Abdullahi M. Abdulquadir, 'Regional Trade and the Challenges of Data Protection in West Africa' <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3770159> accessed 18 November 2023

[12] Amitai Etzioni, 'The Privacy Merchants: What is to Be Done', *University of Pennsylvania Journal of Constitutional Law* [2011] (14) 929 <https://doi.org/10.2139/ssrn.2146201> accessed 18 November 2023

[13]*ibid*

[14]Abraham Aigba, 'Protection of the Personal Data of Athletes in Sports', *Linkedin* <https://medium.com/@abrahamaigba/protection-of-the-personal-data-of-athletes-in-sports-ce39e638db4> accessed 18 November 2023

[15]ibid

[16]Abiodun Odusote, 'Data Misuse, Data Theft and Data Protection in Nigeria: A Call for a more Robust and more Effective Legislation', *Beijing Law Review* 2021 (12) 1284-1298

[17]Abraham Aigba, 'Protection of the Personal Data of Athletes in Sports', *Linkedin* <https://medium.com/@abrahamaigba/protection-of-the-personal-data-of-athletes-in-sports-ce39e638db4> accessed 18 November 2023

[18]Appeal Number CA/IB/291/2020

NDPR and payment should not ordinarily be made to enjoy a right. On the nature of data protection under section 37 of the 1999 Constitution, the court of Appeal held thus:

> But the meaning and scope of 'privacy of citizens' as guaranteed by the section has not received clear definition/interpretation in the constitution. The trial court had, in my view, rightly held that the right to 'privacy of citizens' as guaranteed under the section includes the right to protection of personal information and personal data.

On the objective of the NDPR, the Court, per Mohammed JCA, held that: 'As rightly observed in paragraph 26 of the Appellant's brief of argument, the preamble of the NDPR 2019 indicates that the NDPR was made as a result of concerns and contribution of stakeholders on the issue of privacy and protection of personal data'. On the nexus between NDPR and right to privacy under the constitution, the court expressly held that:

> it is pertinent for me to state that the CFRN 1999 makes provision in chapter IV guaranteeing the various fundamental rights of citizens. But as I stated earlier, the nature and scope of those rights and even their limitations are in most instances, furthered by other statutes, regulations or other legal instruments. It is in this instance that the NDPR must be construed as providing one of such legal instruments that protects or safeguards the right to privacy of citizens as it relates to the protection of their personal information or data which the trial court had rightly adjudged at page 89 of the record to be part of the right to privacy guaranteed by section 37 of the CFRN.

On the right of persons (individuals and corporate alike) to institute fundamental rights actions, the court held as follows:

> I need to add that no set of cases fosters public confidence in the judiciary as an adjudicatory system of redress than fundamental rights cases. This is primarily because most human rights enforcement cases are complaints by seemingly 'weak' individual members of the public against apparently 'powerful' state actors. For this reason, a narrow interpretation of Section 46 of the 1999 Constitution and the FREP Rules, 2009 that springs which restricts access in fundamental rights proceedings to only individuals will unduly retard the objective of ensuring the promotion and due observance by all, of the fundamental human rights so constitutionally guaranteed.

This Appellate court decision is highly commendable as the court expressly made clear pronouncements on key aspects of data protection matters including that data protection/privacy matters is a fundamental right issue which can be instituted under the Fundamental Rights Enforcement Procedure Rules, (FREP) 2009; the right or locus standi of any person, including NGOs to institute data protection matters in the interest of the public or any other person who ordinarily would not want to so do; data protection/privacy is a part of the right to privacy under Section 37 of the Constitution, 1999 (as amended). Okedara *et al*[19] notes that, 'this watershed decision has momentarily ended the debate on whether data protection is contemplated under privacy and this is good for the development of the subject pending the passage of a principal data protection legislation that would address the other procedural and substantive concerns omitted in the NDPR'.[20]

Incorporated Trustee of Digital Rights Lawyers Initiative (DRLI) v Central Bank of Nigeria (CBN)[21]

The CBN had stated that it will direct commercial banks to share their customers' data with financial technology (Fintech) companies. The Applicant approached the court challenging the directive as a likely interference with customers' right to privacy guaranteed under the Section 37 of the Constitution of the Federal Republic of Nigeria and relevant provisions of the Nigeria Data Protection Regulation. Even though the Court dismissed the suit of the Applicant, it made notable pronouncements in relation to data protection:

On whether the Respondent can validly make a directive to commercial banks to share data to third party without consent of data subject

> I find that a community reading of Regulation 2.2 (e) of Nigeria Data Protection Regulation 2019 and Section 2 (d) of the C.B.N. Act 2007 avails the Respondent/Applicant's directive, unless and until the Applicant/Respondent shows the contrary, which he has not done, due to his failure to expose that Respondent/Applicant's directive was not done in good faith, I hereby discountenance Applicant/ Respondent's issues one and two.

[19]Solomon Okedara, Olumide Babalola and Irene Chukwukelu , *Digital Rights in Nigeria through the Cases* (Luminate, Lagos, 2022)

[20]Olumide Babalola, 'The Court Of Appeal Settles The Debate On Whether Data Protection Is Now Subsumed Under Right To Privacy In Nigeria', <The Court Of Appeal Settles The Debate On Whether Data Protection Is Now Subsumed Under Right To Privacy In Nigeria - TheNigeriaLawyer> accessed 19 January 2024

[21]Unreported Suit No. FHC/AB/CS/76/2020

On what applicant must show to prove interference with data subject's rights

> More so, the deponent left in abeyance how the Respondent/Applicant's directive will interfere with his right to privacy guaranteed under the Nigeria Data Protection Regulation and section 37 of the Constitution. No doubt, this is a salient fact which ought to have been particularized. The case of Peak Merchant Bank Limited v. C.B.N. & Ors (2017) LPELR 42324 (CA) captures the importance of stating the facts of bad faith as follows; 'the elements and/or particulars that constituted the bad faith is not alleged clearly or definitely (positively) in the statement of claim.
>
> It was held by the Apex court in the case of N.D.I.C. V. C.B.N (supra) in pages 297 that '… in order that the court may have jurisdiction to entertain the type of action now in question, the Plaintiff/Respondent has to show or alleged bad faith in the way the revocation was done and indicate the elements that constitute bad faith… unless bad faith is positively alleged by way of its elements…an allegation without its elements cannot be regarded as positive.

Though the Court agreed that data protection is a fundamental right protected under the Constitution and litigable under the Fundamental Rights Enforcement Rules, yet, the Court in this instant case seemed to have misconstrued the provisions of the law regarding proof of bad faith as it relates to fundamental rights actions. Okedara et al's commentary on this case captures this criticism succinctly viz;

> It is my respectful submission here that……Since the Court of Appeal has ruled in another case that data protection and privacy as a fundamental right, then once fundamental rights are likely to be infringed and as such, it is expected that steps be taken to prevent the occurrence of the infringement, then a victim can approach the court for redress irrespective of whether or not the infringer has bad faith/intentions. However, where it affects public interest as in the case in view, the court should guide itself by balancing the effect of the likely harm against the proposed gains of 'not preventing' it. Proof of bad faith should not be a precondition in fundamental right cases, as such violates the intendment of the Constitution in protecting the right of its citizens which stands above all other rights. With respect to the court, the cases cited in support of the decision are not fundamental right cases and should not be applied as such.[22]

This author agrees with reasoning of the learned scholar as expressed above and suggests that going forward, Nigerian Courts should be wary of adopting such a narrow approach towards establishing infringement of fundamental right. The rule is that the slight apprehension that a fundamental right guaranteed under Chapter four of the Constitution is being or about to be infringed entitles an applicant to approach the courts for protection and it is expected that the Courts will intervene within the bounds of law.

Incorporated Trustees of Digital Right Lawyers Initiative v. L.T. Solutions & Multimedia Limited[23]

The Respondent through its Twitter handle tweeted that: 'over 200 million fresh Nigerian and international emails lists, sorted by age, state, LGA, city, industry etc send a dm or call 08139745545 to get yours'. The privacy policy published on the company's website showed that the Respondent collects personal data of citizens but it did not explain how data subject's consent were sought and obtained among other deficiencies. The Applicant filed an action claiming that data protection is guaranteed under the right to privacy in section 37 of the CFRN and the Respondent's processing of data of over 200 million Nigerians without legal basis violates the provisions of the NDPR and likely to interfere with their right to privacy.

On whether the right to privacy extends to protection of personal data, the court referred to the objective of the NDPR and held thus:

> In the light of the above, I thus also have no hesitation in holding that the right to privacy extends to protection of a citizen's personal data such [has] been alleged that the Respondent has violated or is threatening to violate as I now go on consider whether the Respondent has indeed violated the Applicant's right to privacy or threatens to violate it.

However, in a violent twist, the court went ahead to find that the Applicant did not depose to facts showing how the failure of the Respondent to publicize a privacy policy as well as obtain the consent of the Applicant before processing his data, infringed on the Applicant's right to privacy guaranteed under Section 37 of the constitution. The Court also held that since there is a penalty (for failure) to comply with the relevant provision of the NDPR and since the case before it was not a criminal or quasi criminal matter, the Court was deprived of jurisdiction to impose such fine even though it already found that the Respondent failed to comply with the NDPR. The Court also refused to grant damages or the reliefs sought by the Applicant. Firstly, it is submitted with the greatest respect, that the learned trial court failed to fully comprehend the nature of data protection matters. The requirement to publish a privacy notice is a stand-alone requirement and does not rest on the Applicant's duty to prove or show how this failure infringed on his right to

[22]Solomon Okedara, Olumide Babalola & Irene Chukwukelu, *Digital Rights in Nigeria through the Cases* (Luminate, Lagos, 2022)
[23]Suit No. HCT/262/2020

privacy. Both are distinct and separate subjects. Secondly, the Court completely missed the point when it failed to comprehend that the right to privacy being a fundamental right which is constitutionally protected, all that the Applicant is required by law to show is that the right has been, is being or is likely to be infringed upon. So even if the Respondent intended to carry out the activity being complained about, the Applicant need not show how the Respondent's prospective actions or failure to comply with the NDPR affected his right to privacy or caused him injuries. He only needs to show that there is likelihood of harm being done to his right of privacy by the prospective actions of the Respondent. However, this decision must be commended as the court took a rights-based approach towards addressing the issue of data protection. In that regard, the court held that data protection is a fundamental right protectable under the 1999 Constitution (as amended). This is a positive development.

Incorporated Trustees of Digital Rights Lawyers Initiative v Minister of Industry, Trade and Investment & 2 Ors[24]
In 2020, the Federal Government called for applications for a Micro Small and Medium Enterprise (MSME) Survival Fund/grant. Applicants were requested to divulge sensitive personal data (including Bank Verification Number (BVN) while applying online these data were processed. The 1st Respondent did not comply with the NDPR as they failed to publish a privacy policy or notice on the portal hosted online. Also, the Ministry of Trade, commerce and Industry neither appointed a data protection officer (DPO) nor developed any security measures to protect data, store data securely in the said online application portal. The Applicant approached the court on behalf of its members some of who were applicants for the fund, claiming that the Respondent had violated the provisions of the NDPR and interfered with the right to privacy of its members. The court held;

On when a Data Controller will be held liable for breach of data privacy of a data subject, the Court held as follows:

> The 1st Respondent did not deny the Applicant's case by providing any evidence to show that the obligations set out above as a data controller were complied with. The Applicant furnished the Court with Exh.3–6 which are photographs of the MSME Survival Fund Program online portal and in them. I see that neither of the obligations required of the 1st Respondent by the NDPR were complied with. The 1st Respondent beyond saying generally in Paragraph 9 and 10 of the counter afidavit that the portal was set up and being used with all security measures and statutory provisions regarding the privacy of data being collected, and that the operation of the survival fund were transparent and available to members of the public, it did not provide any details to demonstrate or prove compliance with the privacy protecting and securing measures outlined in the Regulations. All things considered, I hold that the failure of the Respondents, from taking measures towards protecting the data privacy of the citizens, taking into account the vital information required from the data subject such as the Bank Verification Number, names and addresses, poses a threat to the Applicant's members right to private and family life owing to the fact that the objectives of the NDPR as provided in Regulation 1.1 is to safeguard the rights of natural persons to data privacy.

This case emphasized the court's readiness to penalise any data controller who merely states that it has put in security checks without actually demonstrating how those security checks and measures work. This is a very laudable stance as this will put data controllers on their feet to ensure they put in measures such as data protection officer (DPO), publish privacy policies and state how data will be collected and used and for what purposes.

Incorporated Trustees of Digital Rights Lawyers Initiative v National Communications Commission[25]
In 2019, the National Communications Commission (NCC) introduced a (draft) Internet Industry Code of Practice which empowers the NCC to unilaterally issue a takedown order to Internet Service Providers (ISP) to shutdown certain websites without recourse to court order. The Applicant challenged the document in court seeking inter alia, a declaration that by Section 7.3 of the Respondent's establishment of Internet Industry Code of Practice on take down notice (the 'Draft Code') is likely to violate the Applicant's fundamental right to expression and the press guaranteed under Section 39 of the Constitution of the Federal Republic of Nigeria, 1999. The Court found that the Applicant had the locus standi to institute the action; however, the court held that the suit was speculative, frivolous and constituted an abuse of court process as the Applicant was challenging a Draft Code, which was not yet a substantive law. This decision is commendable in that the court recognised the right of the Applicant (an NGO) to institute the action in the interest of the public. The Court by so doing, also adopted a rights-based approach to this matter.

Incorporated Trustees of Digital Rights Lawyers Initiative & 2 Others v National Identity Management Commission[26]
In this case, the Applicant had sued the Defendant for infringement of the right to privacy of the 2nd Applicant who was requested by the Defendant to pay the sum of N15,000 for rectification of his date of birth in his national Identity Card. While dismissing the suit of the Applicant, the Court nonetheless pronounced on the relationship between privacy and data protection thus;

[24] Unreported Case Suit No. FHC/AWK/CS/116/2020
[25] Suit No. FHC/ABJ/CS/56/2019.
[26] Suit No. AB/83/2020

> The kernel of both the provision of section 37 of the constitution and these illuminating decisions is, to my mind, that privacy of a citizen of Nigeria shall not be violated. From these decisions, privacy to my mind can be said to mean the right to be free from public attention or the right not to have others intrude into one's private space uninvited or without one's approval. It means to be able to stay away or apart from others without observation or intrusion. It also includes the protection of personal information from others. This right to privacy is not limited to his home but extends to anything that is private and personal to his including communication and personal data.

Digital Rights Lawyers Initiative v National Youth Service Corps[27]

Sometime in 2020, the Respondent coerced Corps members to sign Data Subject Consent Forms on the eve of their passing out as a precondition for their final discharge from service. The personal data collected from the Corp members were subsequently published in magazines which bear the names, phone numbers, image photographs and other personal information of the Corp members. The Applicant challenged this action as a violation of the provisions of the NDPR and Section 37 of the Constitution which guarantees right to privacy. The court held that in so far as the Defendant also attached another form stating that Corps members could withdraw their consent and the manner in which they could do so, the Defendant had not infringed on the rights of the Corpers. In particular, the Court considered whether Section 20 of the NYSC Act divested the Court of jurisdiction to entertain an action for enforcement of fundamental rights of a Corp member. The court held in the negative and stated that it is not the intendment of the FREP Rules that the enforcement by a person of his fundamental right is to be subjected to the fulfilment of any condition precedent whatsoever, once the proceeding is initiated by due process.

On when a Controller may be held to have properly obtained Data subjects' consent under the NDPR

> A look at Exhibit 2 not only reveals a consent form, but it also contains leeway for the 2019 Batch B Stream 1 Corp members to waive their consent at any time, by use of DATA SUBJECT WITHDRAWAL FORM… (page 20) … In the instance of this case, I hold squarely that the Exhibit 2 is not an infringement of Applicant fundamental rights encapsulated in Section 37 of the Constitution of the Federal Republic of Nigeria 1999 (as amended), and the Exhibit 2 have not exposed at all that the applicant were railroaded into a straitjacket all for the sake of their graduation/passing out certificate.
>
> Pointedly I find that Exhibit 2 annexed to the Originating Summons have fully complied with the Nigeria Data Protection Regulation 2019. And crucial to set out is Article 2.3 (2) (c) to wit: –'Prior to giving consent, the Data subject shall be informed of his right and method to withdraw his consent at any given time. However, the withdrawal shall not affect the lawfulness of processing based on the consent before its withdrawal.

Incorporated Trustees of Digits Rights and Laws Initiative v Habeeb Olasunkanmi Rasaki[28]

The Appellant sued the Respondent for printing out various WhatsApp conversations of a certain named individual over a period of time. Due to the sensitive nature of the conversations, the Appellant approached the court to estop the Respondent from further processing (especially sharing and use) of the WhatsApp messages. The applicant sued and invited the court to interpret Article 1.1(a) and 4.8 of the Nigeria Data Protection Regulation (NDPR) 2019 whether the action of the Respondent was not an infringement of these legislations. The court dismissed the suit and held that the claim is not cognizable under the Fundamental Rights (Enforcement Procedure) Rule 2009 and the court had no jurisdiction to entertain it. This case presented a very fine opportunity for the court to decide on sensitive data however, it is sad that the court subtly stayed away from deciding the main issue in the case which is the issue of infringement of the right to privacy guaranteed by the constitution. The ratio of the court herein does not represent the correct position of the law on the status of the NDPR as an instrument that enforces the right to privacy as a fundamental right. The later decision of the Court of Appeal in *Incorporated Trustees of Digital Rights Lawyers Initiative & Ors v NIMC* (2021) LPELR–55623(CA) represents the current position of the law wherein the court recognized data protection under the NDPR rights as an extension of the right to privacy guaranteed by section 37 of the Constitution.[29]

Incorporated Trustees of Laws and Rights Awareness Initiative v. National Identity Management Commission[30]

In 2020, the National Identity Management Commission introduced digital identity cards on Google store. Upon the prompting of an official of the Federal Government of Nigeria advising people to download the identity cards (digital IDs) on the software application, several Nigerians within 24 hours of the announcement, complained about the porous security features of the digital IDs and data breaches that led to some people being given other citizens' information on their digital IDs. The Applicant on behalf of a named individual, approached the court seeking a declaration that the Respondent's processing of the digital identity cards via their software application (NIMC app) is likely to interfere with the right of privacy as guaranteed under article 1.1(a) of the NDPR 2019 and Section 37 of the Constitution. The Court held on a whether an action can be brought on behalf of a data subject for breach of the NDPR that, by regulation 4.2(6) of the NDPR, 'any breach of this Regulation shall be construed as a breach of the provisions of the National Information Technology

[27] Suit No. AB/207/2020
[28]Suit No. AB/207/2020
[29]Solomon Okedara, Olumide Babalola & Irene Chukwukelu, *Digital Rights in Nigeria through the Cases* (Luminate, Lagos, 2022)
[30]Suit No.: FHC/AB/79/2020

Development Agency (NITDA) Act of 2007. This provision takes it out of the purview of fundamental right action, therefore only a data subject can legally sue for breach of his data and that can only be done under the Nigeria Data Protection Regulation/NITDA Act, 2007'. It is submitted that even though the Court stated the right law, it failed to rightly and properly apply same hence it reached an erroneous conclusion that a breach of the NITDA provision takes the suit out of the scope of fundamental rights. It is submitted that the Court could have entertained the suit as a fundamental right action, had the court averted its mind to the fact that the NITDA and NDPR deals with data protection matters which have been adjudged to be a fundamental right matter in the case of *Digital Rights Lawyers Initiative (DRLI) v. National Identity Management Commission (NIMC).*[31]

Hillary Ogom Nwadei v Google Limited Liability Company & Anor[32]

The Applicant sought to enforce against the Respondent, his right to be forgotten as a data subject. The facts were that some time back, the Applicant, a Lawyer and a Priest was convicted of assault in the United Kingdom wherein he served an 8-month jail term. Several publications were written about the event which was frequently accessed on the Respondent's Google search engine. The Applicant found it difficult to get job years after the conviction and alleged that this was due to the fact that the offending articles were still findable on the Respondent's search engine. The Respondent argued that it had no control of what was published in its search engine as it was just a search engine. Moreover, that the Applicant's conviction made news in the United Kingdom and already forms part of the public records in the United Kingdom, hence, the Applicant had lost the right to be forgotten. The court dismissed the claims of the Applicant and held that the Applicant failed to place sufficient evidence before the court to show that the Respondent had something to do with the publication of the news or articles which the Applicant was complaining about. The Court did not really delve into the issue of the right of a data subject to be forgotten and whether same applies in this case. It is the humble submission of the authors that even if the court had considered the issue of the Applicant's right to be forgotten, same would not have availed the Applicant as what the Applicant sought to erase is public record which the public is entitled to know about or which the government ought to keep. The fact that privacy is a fundamental right does not mean that it is an alpha and omega right itself devoid of exceptions. One of the ways by which a data subject may lose his right to privacy is in the event of the commission of a crime. Criminal records being kept by the appropriate authorities do not and ought not to be erased under the guise of the right to be forgotten. These records exist and should be protected for the interest of the general public.

4. Conclusion and Recommendations

An examination of some of the cases on data protection and privacy as decided by the Nigerian courts reveal that the courts are more disposed to deciding that data protection is a fundamental right. At best, most of the Judges agree that data protection forms part and parcel of the constitutionally guaranteed right to private life. The Courts are also poised to hold that an individual or body corporate has *locus standi* to institute a case of breach of data protection rules or regulations. Therefore, the following are recommended for a more enhanced data protection regime in Nigeria:

1. Nigeria is on the right track by adopting a human right–based approach to data protection by holding in many of the cases that it is an off shoot of the right to privacy. However, it is suggested that the next step should be the creation of an entirely new fundamental right known as the fundamental right to data protection, distinct and independent of the right to privacy.[33]

2. In deserving cases, the right to privacy and data protection should not be used or seen as a shield to hide criminal records and other issues of public interest and public good. The right to erasure of data or to be forgotten cannot apply in all instances. For example, educational institutions typically store the data of students including past students of the institutions for several years. This is both safe for the institution and the students as it constitutes *prima facie* evidence that such individual attended the institution.

3. Data Controllers should ensure they set up necessary data security measures such as appointing a Data Protection Compliance Officer (DPCO), publishing privacy policies and stating how data will be collected, processed, and used as well as clearly indicating what purpose the data will be used for.

4. Legal practitioners and litigants in the area of data protection should be careful of how they litigate data protection cases, particularly in the manner the processes are drafted and the case conducted. Essentially, there is need to ensure that the material facts are pleaded and relevant evidence called and placed before the court to aid the court in arriving at a just decision of the case.

Hence, it can be said that the judicial attitude towards data protection cases so far is commendable and positive. It appears that quite a number of Judges are prepared to strictly enforce data protection if there is a clear breach of the provisions of well-articulated data protection legislation. With the existence of the NDPA 2023, it is hoped that in the coming days, more decisions protecting the data of individuals and corporate bodies alike will be made by the judiciary.

[31]Appeal Number CA/IB/291/2020
[32] Suit No. IKD/3191GCM/2019
[33](n.29)