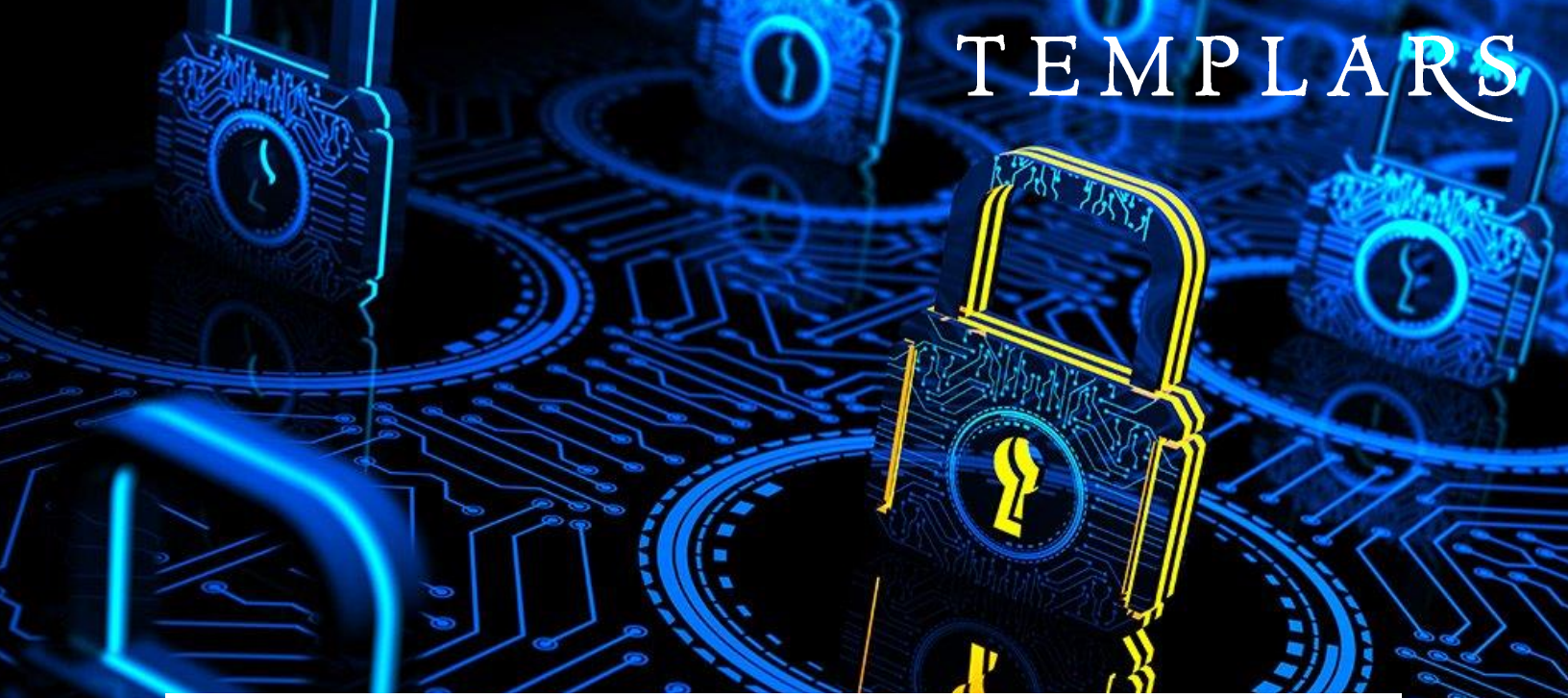

Enforcing Data Subject Rights Under Nigeria's Data Protection Regulation: **The Wrong Way (And The Right Way).**

In keeping with the drive towards data privacy and protection by different countries across the globe, Nigeria enacted the Data Protection Regulation (the "**NDPR**") in 2019[1], to regulate the collection and processing of Personal Data[2] of natural persons in Nigeria. The enactment of the NDPR was a step in the right direction in an era where personal data had become (and still is), the stock-in-trade of the Big Tech[3] and other domestic and multinational information technology corporations. There was an urgent need to regulate the collection and processing of Personal Data, and with this need in focus, provisions were made in the NDPR, among others, recognizing the rights of Data Subjects[4], and prescribing the obligations of Data Controllers[5] with respect to collected Personal Data.

[1] Nigeria Data Protection Regulation, 2019.
[2] Defined by Section 1.3(q) of the NDPR as any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person; It can be anything from a name, address, a photo, an email address, bank details, posts on social networking websites, medical information, and other unique identifier such as but not limited to MAC address, IP address, IMEI number, IMSI number, SIM and others.
[3] The largest and most dominant companies in the information technology industry, that is, Amazon, Apple, Google, and Facebook.
[4] Defined by Section 1.3(k) as an identifiable person; one who can be identified directly or indirectly by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity.
[5] Section 1.3(g) means a person who either alone, jointly with other persons or in common with other persons or as a statutory body determines the purposes for and the manner in which personal data is processed or is to be processed.

As the implementation of the NDPR gains traction, there has emerged a debate amongst privacy rights activists and data protection enthusiasts regarding the relationship that exists between the rights of a Data Subject under the NDPR and the privacy rights guaranteed under the Constitution of the Federal Republic of Nigeria, 1999 (as amended) (the "**Constitution**"). Specifically, the debate is whether the rights of the Data Subject under the NDPR may be subsumed under the right to privacy provided in the Constitution, such that the Data Subject, whose rights under the NDPR have been breached may enforce these rights by way of an action brought under the Fundamental Rights (Enforcement Procedure) Rules, 2009 (the "**FREP Rules**").

The extant FREP Rules were enacted on 1 December 2009[6] under the authority of Section 46(3)[7] of the Constitution and prescribes the procedure for the enforcement of fundamental rights enshrined in Chapter IV of the Constitution as well as the fundamental rights provided for under the African Charter on Human and People's Rights[8] (the "**African Charter**").

Our Objective

The purpose of this article is to review the divergent views or opinions regarding the procedure to be adopted by a Data Subject in enforcing the rights under the NDPR, and thus provide a guide or an appropriate direction that may be followed in enforcing those rights. The reason is that there seems to be the notion that the Data Subject's rights under the NDPR can be enforced the same way fundamental rights under the Constitution, may be enforced using the enforcement procedure provided by FREP Rules.

This notion, however, seems misplaced as shall be demonstrated in this article. It will also be shown that a Data Subject's rights under the NDPR may not necessarily enjoy the same status as the rights specifically guaranteed by the Constitution, and as such, the Data Subject's rights under the NDPR may not be enforced using the procedure prescribed by the FREP Rules.

The debate

Some data protection enthusiasts have argued that the rights of the Data Subject under the NDPR are analogous to the right to privacy under Section 37 of the Constitution and as such, those rights can be enforced in the same manner in which fundamental rights guaranteed under the Constitution may be enforced. The proponents of this view contend that the Data Subject's rights under the NDPR are a specie of the right to privacy under Section 37 of the Constitution and to that extent, those rights are enforceable the same way the privacy right may be enforced. This contention recently found support in the decision of the Ogun State High Court presided over by the Honourable Justice O. Ogunfowora, in **Incorporated Trustees of Digital Rights Lawyers Initiative and L.T Solutions & Multimedia Limited**[9] (***DRLI VS LTSM***) where it was held that a Data Subject's rights under the NDPR may be enforced the same way a Constitutional right is enforced under the FREP Rules. This decision will be discussed in detail in the following paragraphs.

The facts of DRLI VS LTSM

The facts of this suit occurred on the back of an alleged tweet by LTSM offering for sale, over 200 million Nigerian and international mailing lists. DRLI brought the suit under the FREP Rules and contended that LTSM does not have the right or legal basis to process Personal Data

[6] The FREP Rules replaced the Fundamental Rights (Enforcement Procedure) Rules, 1979 which formerly regulated proceedings for enforcement of fundamental human rights under the Constitution.
[7] Which enables the Chief Justice of Nigeria to make rules with respect to the practice and procedure for enforcement of fundamental rights under Chapter IV of the Constitution.
[8] which was ratified by Nigeria on 22 June 1983, and Domesticated by the African Charter on Human and Peoples' Rights (Ratification and Enforcement) Act, Cap. A9 Laws of the Federation of Nigeria, 2004
[9] Suit No. AB/83/2020 (Unreported)

in the manner that it purportedly did. The central issue was whether LTSM invaded or was likely to invade DRLI's rights to privacy provided under Section 37 of the Constitution and the NDPR. The court held that the right to privacy under Section 37 of the Constitution ought to be interpreted expansively to include protection of Personal Data under the NDPR and therefore, the suit was properly situated under the FREP Rules.

The approach adopted by the court in this case tends to suggest that a breach of a Data Subject's right under the NDPR may be remedied by an action brought under the FREP Rules *simpliciter*.

On the flip side, those opposed to this view, however, argue that a Data Subject's rights under the NDPR are neither constitutional rights nor fundamental human rights under the African Charter, and as such, cannot be enforced under the procedure provided in the FREP Rules.

This position received judicial approval in the recent judgment of the Federal High Court of Nigeria (the ***"FHCN"***) presided over by the Honourable Justice Ibrahim Watila delivered on 9 December 2020 in the case between the **Incorporated Trustees of Laws and Rights Awareness Initiative and The National Identity Management Commission**[10] **(*RAI vs NIMC*). I**t was held in the case that a breach of Data Subject's right under the NDPR is not necessarily a breach of the right to privacy under the Constitution, so that a claim for interpretation of the provisions of the NDPR is not a fundamental rights action falling within the purview of the FREP Rules. This seems to be the latest judicial decision on the subject and which for clarity sake, we have considered the facts in detail below.

The facts of RAI VS NIMC

The suit was filed in connection with the initiative of the Nigerian Government to establish a national identity database pursuant to the National Identity Management Commission (***"NIMC"***) Act enacted in 2007. NIMC is the public body established to, among others, maintain this database and issue National Identification Numbers to registered persons.

RAI, a public interest litigant purportedly suing for and on behalf of one Daniel John, claimed that the processing of Personal Data by NIMC is likely to interfere with Daniel John's right to privacy guaranteed under Section 1.1(a) of the NDPR and Section 37 of the Constitution. On the basis of this contention, RAI sought to injunct NIMC from further releasing digital identity cards pending an independent report of external cyber security experts on the safety and security of the Respondent's applications. The suit was brought under the FREP Rules.

One of the central issues that came up for consideration was whether the claim for breach, or rather, potential breach of the provisions of the NDPR was properly brought under the FREP Rules having been lumped together with a claim for breach, or potential breach of the right to privacy under Section 37 of the Constitution? The FHCN, after a careful review of the arguments on both sides, held that the suit was wrongly brought as a fundamental right enforcement action under the FREP Rules for the following reasons:

- by virtue of Section 3.2.2 of the NDPR[11], a breach of the NDPR is construed as a breach of the provisions of the National Information Technology Development Agency Act, 2007 (the "**NITDA Act**") and therefore, a Data Subject can only sue for breach of his rights under the NITDA Act; and

- before an action can be brought under the FREP Rules, the action must be premised on a breach of a fundamental right provided for under Chapter IV of the Constitution as the primary or principal claim. The court found that the principal

[10] Suit No. FHC/AB/CS/79/2020 (Unreported)

11 Provides as follows, *"Any breach of this Regulation [the NDPR] shall be construed as a breach of the provisions of the NITDA Act"*

claim in this suit was for breach of the provisions of the NDPR and the claim of breach, or potential breach, of the right to privacy under the Constitution was merely incidental or ancillary to the principal claim.

On the balance, the reasoning of the FHCN in **RAI vs NIMC** referenced above, seems plausible and persuasive. We say so for the following sundry reasons:

- first, while some rights of the Data Subject under the NDPR may be similar to the right to privacy under the Constitution, we believe that should not necessarily elevate the rights of a Data Subject under the NDPR to the status of rights specifically cognizable under the Constitution, to justify their enforcement under the FREP Rules.

- second, the NDPR derives its legitimacy from the NITDA Act and not the Constitution. The FREP Rules was enacted to regulate the enforcement of fundamental rights provided for under Chapter IV of the Constitution as well as the African Charter. Therefore, the FREP Rules ought not be deployed in a proceeding where the principal claim is for enforcement of a Data Subject's rights under the NDPR.

- also, in our opinion, the NDPR does not have any constitutional flavor necessary to bring it under the purview of the Constitution for the sake of enforcement by way of an action under the FREP Rules. And in any case, it must be noted that the FREP Rules were enacted for the very specific purpose of expeditiously hearing and determining proceedings for enforcement of fundamental rights under Chapter IV of the Constitution or under the African Charter.[12] By implication therefore, unless the right to be enforced is one specifically guaranteed and provided under Chapter IV or the African Charter, recourse to the procedure prescribed by the FREP Rules may not be validly had or deployed.

- furthermore, we believe that the approach adopted by the court in the ***DRLI VS LTSM*** case ignores the import of Section 3.2.2 of the NDPR which states that a breach of the provisions of the NDPR is to be construed as a breach of the NITDA Act, and thus and perhaps, more significantly, the rule that where the words or language used in a statute or law (such as the NDPR), is clear and unambiguous, it ought to be applied and given its ordinary grammatical meaning.[13]

- more so, as provided in the law, a breach of the NITDA Act may only be remedied or sanctioned in accordance with its provisions, and Section 18 thereof provides that a breach of the NITDA Act by a body corporate or person would upon conviction, attract a fine of N200,000 or imprisonment for a term of one year, or both for first offence; and for a second offence and subsequent offence, the breach would attract a fine of N500,000 or imprisonment for a term of three years, or both a fine and a term of imprisonment.

- it is equally instructive to note that Section 2.10 of the NDPR prescribes specialized penalties for breaches of the data privacy rights of any Data Subject, that is, in the case of a Data Controller dealing with more than 10,000 Data Subjects, payment of a fine of 2% of Annual Gross Revenue of the preceding year or payment of the sum of N10,000,000 whichever is greater; and in the case of a Data Controller dealing with less than 10,000 Data Subjects, payment of a fine of 1% of the Annual Gross revenue of

12 See the case of Enemuo & Another vs Ezeonyeka & Others (2016) LPELR-40171(CA) where it was held that, "*the Fundamental Rights (Enforcement Procedure) Rules 1979 were made specifically for a speedy determination of cases seeking the enforcement of the fundamental rights guaranteed by the Constitution of the Federal Republic of Nigeria*."

13 Virgin Nigeria Airways Ltd v. Roijien (2013) LPELR-22044(CA) "*where the language of the statute is clear and unambiguous, the Court should give the words their literal meaning*" We believe that to the extent that the language used in section 3.2.2 of the NDPR, is clear enough and should have been given its ordinary grammatical meaning.

the preceding year or payment of the sum of N2,000,000 whichever is greater.

- it is unlikely that the sanctions prescribed by Section 18 of the NITDA Act and Section 2.10 of the NDPR can be imposed or enforced against a respondent in proceedings initiated using the FREP Rules. This is because, in general, the proceedings envisioned under the NITDA Act and the NDPR are criminal or quasi-criminal in nature, while proceedings for enforcement of fundamental human rights under the FREP Rules are purely civil in nature, and in civil proceedings[14], there can hardly be any basis for a court to impose criminal sanctions on any of the parties.[15]

For the above reasons, it becomes prescient to say that the decision of the State High Court in the case of **DRLI VS LTSM** may have missed the point, when it held that the rights conferred under the NDPR may be enforced under the FREP Rules.

Our Take

Notwithstanding the foregoing, we believe that the issue is far from being settled because this is a decision of a court of first instance and as such, is at best, a persuasive precedent, not binding on courts of coordinate jurisdictions, such as the High Court of Ogun State.

That said, if we were to put the decision of Ogun State High Court in **DRLI VS LTSM** and that of the FHCN in the case of ***RAI vs NIMC*** on a scale, we would readily throw our weight behind the FHCN's decision. The reason is not far-fetched. The FHCN's reasoning that, a breach of a Data Subject's rights under the NDPR cannot be remedied by way of an action brought under the FREP Rules aligns with the basis for FREP Rules, as a specialized procedure reserved for enforcement of fundamental rights under Chapter IV of the Constitution or the African Charter.
And while conceding that the FHCN is a court of first instance, we reasonably believe that if the decision in ***RAI vs NIMC*** goes on appeal, there is a chance that same will withstand the rigors of the appeal process.

Even so, it is important to mention that this does not imply that a Data Subject whose rights under the NDPR have been breached does not have a recourse, because he does have. However, such a recourse, in addition to the administrative remedies available under the NITDA Act, could possibly be for the Data Subject to bring a regular action to enforce such breaches.[16] Similarly, while breaches of the rights under NDPR may not be properly introduced in proceedings for enforcement of fundamental human rights, they may however be introduced as ancillary claims or reliefs. In other words, a claim for a breach of the provisions of Chapter IV of the Constitution or the African Charter must form the principal or substantive claim, while the claim for breach of the provisions of the NDPR must only be the ancillary claim. In this regard, it has been held many times that to sustain a fundamental rights enforcement action, the substance of the suit must be hinged on an alleged breach of a fundamental rights cognizable and justiciable under Chapter IV of the Constitution or the African Charter[17].

Therefore, where an alleged breach of a right under Chapter IV is made ancillary to a substantive claim of breach of the NDPR, the action would be incompetent if brought under the FREP Rules. This position was confirmed by the Supreme Court in the case of **Tukur v. Government Taraba State**[18] where it succinctly restated that:

14 Save where specifically stated in the relevant law, though this is uncommon.
15 The reason is that for the sanctions to be imposed, the guilty party must have been tried by the court and found guilty. But this would usually happen in a criminal proceeding as opposed to civil proceedings.
16 Where it is the case that the Data Subject can bring a civil claim to enforce his rights under the NDPR, separate from the administrative criminal or quasi-criminal remedies provided.
17 Tukur v. Government Taraba State [1997] 6 NWLR (Pt. 510) 549
18 [1997] 6 NWLR (Pt. 510) 549

"…when an application is brought under the Fundamental Rights (Enforcement Procedure) Rules, 1979, a condition precedent to the exercise of the court's jurisdiction is that the enforcement of fundamental right or the securing of the enforcement thereof should be the main claim and not an accessory claim. Enforcement of fundamental right or securing the enforcement thereof should, from the applicant's claim as presented, be the principal or fundamental claim, and not an accessory claim…"

Conclusion

In light of the foregoing backdrop, it may not be out of place to adjust the FREP Rules in a way that would make the Rules readily amenable and flexible to accommodate emerging rights, such as the Data Subject's rights in the NDPR, that are similar to the rights of citizens specifically provided for in the Constitution. But until such an adjustment, it may be important that originating processes with the reliefs sought in an action brought under the FREP Rules, are carefully couched to avoid being thrown out of court at a preliminary stage of the proceedings. The substantive or principal claim must be in relation to a breach of a fundamental right as contained in Chapter IV of the Constitution or African Charter, while the ancillary claim may be a breach of the provisions of the NDPR. Better still, and perhaps, a better approach, would be to make a claim for breach of the NDPR and NITDA Act a stand-alone proceeding, rather than lumping it together with a fundamental right enforcement action under the FREP Rules. That way, any unnecessary controversy with its attendant risks, can be avoided.

Contacts:

Sadiku Ilegieuno
Partner
sadiku.ilegieuno@templars-law.com

Cyriacus C Orlu
Managing Counsel
cyriacus.orlu@templars-law.com

Funso Tinuoye
Associate
funso.tinuoye@templars-law.com

Francis Jarigo
Associate
francis.jarigo@templars-law.com