A CURSORY LOOK AT THE RIGHTS OF DATA SUBJECTS UNDER THE NDPR 2019

BY TIMOTHY OPURUM[1]

Introduction

Data Protection in Nigeria is fairly a novel regime in the nation's legal jurisprudence. The need to regulate this aspect of our national life becomes inevitable following the high rise in the global advancement of information technology. Countries and their governments are becoming more concerned about what happens to the information of their nationals on cyberspace. This is particularly so where such information is directly or indirectly connected to the identity of an individual national.

The internet space is a world of its own governed by data relating to diverse issues that are connected to human existence. It is popularly regarded as the new world aided by digital technology that has disrupted the analogue or manual system of processing information, and are essentially written in digital codes. This new world, regardless of its sophistication, easier accessibility and open usage, is not unlikely to be immune from attendant negative consequences. For instance, cybercrimes are crimes aided by the digital technology. Statistics reveals that some victims of abduction and assassination had their information sourced from the internet, particularly the social media platforms. Also, some serial murder, terrorism, genocidal acts etc. are directly or indirectly inspired by digital technology. The collection of people's personal information by business owners for economic benefits like sending customized business promotional messages, transferring of the information to a third party for pecuniary benefits and all sorts, without the consent of the individuals are made possible by digital technology. Hacking into private information and personal data is made possible by digital technology. As a result of the foregoing consequences attributed to the digital age, various governments of the world are now making concerted efforts to promulgate regulatory frameworks calculated at data protection, and Nigeria is not exempted.

[1] Timothy Opurum is a legal practitioner in Lagos. His areas of legal practice include Data Privacy and Protection, Litigation, Corporate and Property Law. You can contact him on opurumtimothy@gmail.com

The Legal Framework

The National Information Technology Development Agency (NITDA) is an Agency of the Federal Government of Nigeria established in 2007 by the NITDA Act of 2007 and saddled with the statutory responsibilities to, among other functions, regulate data processing in Nigeria. It is in fulfillment of its obligations that the Agency, in 2019, issued the Nigeria Data Protection Regulations (NDPR) with its objectives as specified in Reg. 1.0 of the Regulation. And it provides thus:

> *"The objectives of this Regulation are as follows:*
>
> *a) to safeguard the rights of natural persons to data privacy;*
> *b) to foster safe conduct of transactions involving the exchange of personal data;*
> *c) to prevent the manipulation of personal data, and*
> *d) to ensure that Nigerian businesses remain competitive in international trade; through the safeguards afforded by a just and equitable legal regulatory framework on data protection and which regulatory framework is in tune with global best practices."*

Interestingly, Reg. 1.3(d) defines data as thus:

> *"Characters, symbols and binary on which operations are performed by a computer, which may be stored or transmitted in the form of electronic signals is stored in any format or any device."*

In a loose interpretation, data simply means information leading to the identification of any person, place or thing, while personal data deals with any personal information that identifies an individual.

Issue 06 of the European Digital Rights (EDRi) Papers defines Personal Data as thus:

> *"Any kind of information (a single piece of information or a set of information) that can personally identify an individual or single them out as an individual."*

In a similar vein, Reg. 1.3(9) describes personal data thus:

> *"Any information relating to an identified or identifiable natural person ('data subject').*

The Regulation went further to define an identifiable natural person as

> *"One who can be identified, directly or indirectly, in particular reference to an identifier…"*

A Data Subject, by the Regulation, is an identifiable person; one who can be identified directly or indirectly, in particular reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural (and religious) or social identity.

In other words, my bank details, social status, height etc. are my personal data capable of enjoying protection against unauthorized or unlawful usage. If you walk into a supermarket and at the end of your transactions in there, your information - your name, phone number, email address, gender, date of birth etc. – are collected from you with your consent in a bid of contacting you subsequently for more business deals, those details collected of you are regarded as your personal data. They are personal to you and they reveal your identity.

So, are there rights that accrue to a Data Subject that can be legally enforced? Are Data Controllers liable for some breaches of these rights? What are these rights? Are they even enforceable? These are some of the issues to be considered in this article.

Rights of Data Subjects

By virtue of the provision of the NDPR 2019, a data subject enjoys certain rights over his personal data. These rights are summarized as follows.

1. Right to knowledge of Data Controller: It is the data subject's right to know who or what agency, known as Data Controller, is collecting his or her personal data. Failure of the Controller to disclose its identity will entitle the data subject to refuse the grant of such personal data as is being requested. On the other hand, where the personal data of the data subject is already obtained and the data subject wishes to know who the controller is, the data subject is entitled to be furnished with such details by the Controller. Where this is not done, the data subject can withdraw his consent and further demand that his personal data be deleted by the controller,

and where that is still not satisfied, the data subject reserves a further right of action in a competent court for redress.

2. Right to the contact of the Data Protection Officer (DPO): By virtue of the provision of the NDPR, each Data Controller is mandated to have a DPO. A DPO is a data compliance officer specifically employed to ensure that an organization which has something to do with data processing complies with the provision of the Regulation. A data subject has the right to the contact details of such DPO.

3. Right to Knowledge of the Purpose for which the Personal Data is being processed: It is not enough that a Controller is interested in processing personal data of a data subject, the Controller, in clear terms, must specify the purpose for which the personal data is being processed. Part of this is also to disclose the duration of time for which the personal data will be processed. Importantly, the Controller is expected to divulge the legal basis for processing such personal data. A Controller will not be allowed to use in perpetuity personal data of a data subject; there must be a purpose and time frame within which it will be legally valid to continue the use of that personal data. Also, the period for which the personal data will be stored, or if that is not possible, the criteria used to determine that period has to be disclosed.

4. Right to know whether personal data will be transferred to a third party: It is part of the data subject's right to know who his data will be shared with. The controller is under an obligation to disclose if it will be sharing such personal data with other interested parties. Apart from disclosing this fact, the Controller is equally mandated to disclose the potential recipient of the said personal data. In other words, the names of the recipients of the shared personal data must be disclosed to the data subject before his consent can be obtained.

5. Right to request from the Controller access to and rectification or erasure of personal data or restriction of processing concerning the data subject or to object to the processing as well as the right to data portability: A data subject has the right to demand a rectification from the Controller where he perceives there is an error in his data. He can also demand an erasure of his personal data or even restrict or object the processing or manner of processing of same and its portability or transferability.

6. Right to withdrawal of consent: One of the basic obligations of a Controller is to ensure that the consent of the Data Subject is first sought and obtained before

proceeding to process his persona data. Importantly, the Regulation expects that such consent so obtained must be free from force or coercion, duress or undue influence of whatever kind. The data subject must give such consent based on his own freewill. Where consent is obtained otherwise and personal data is obtained, the data subject will be entitled to a redress. However, the data subject can decide to withdraw his consent any time, particularly whenever he feels his personal data is not being used for the purpose he gave his consent, or where his personal data has been transferred to a third party without his prior consent.

7. A data subject also enjoys the right to lodge a complaint with the regulatory body where necessary.

Seeking redress

Where any of the rights of the data subject has been breached or being breached, he can maintain an action in a court of competent jurisdiction. He is also entitled to lodge a complaint with the Agency which is mandated to set up an Administrative Redress Panel to look into the issues raised in the complaint.

Conclusion

The National Information Technology Development Agency (NITDA), being the regulatory agency saddled with the protection of personal data of Nigerians, has a lot to do to ensure that individual persons are properly enlightened about how they can protect their data and what to do when such personal data have been breached. Only a few people are aware of the existence of this legal regime.