THE PROBLEMS OF THE DEFICIENCY OF DATA PROTECTION LAW IN NIGERIA*

Abstract

Data protection is an approach created to provide security and protection over information that are personal to individuals and are capable of identifying or leading towards the identification of individuals. This brief study examines the problems of lack of data protection law in Nigeria. It looks at how data protection legislation will advance the right to privacy in the use of internet and information technology. The study recommends an urgent enactment of data protection law, which will not only be in the interest of citizens but also for national protection and development.

Keywords: Data protection, Law, Deficiency, Problems, Nigeria

1. Introduction

The pertinence of Data Protection cannot be overemphasized in a state especially where the citizens of said state have a knack for abusing and infringing on a person's right to privacy; which although has been provided for in the Constitution has been made an incessant subject of breach. Over the time, the onrush of technology and the expansive use of the internet have made it intensely compelling for a state no matter its level of development to have an all encompassing and profound Data Protection Law; this is to say underdevelopment is not a defence. A state without this law is exactly like the proverbial blind leading the blind, the end is of course disastrous.

2. Findings and Discussion

Coming home, Nigeria till date can be easily cited as one of the states without a definite Data Protection law; at best it can only boast of a bill which is birthed from the shameless act of our legislators duplicating the GDPR[1] of European States. This deficiency has proven perilous as the Judiciary has nothing to predicate upon when faced with cases having breach of data privacy as a subject matter; and it is a known fact in law that one cannot place something on nothing and expect it to stand – '*ex nihilo nihil fit'*.[2]

There have been plethora of cases where the judiciary tried their hands on some of these related scenarios and albeit the difficulties, gave sound judgement which can serve as a yardstick and as a trail our legislators could follow in drafting a definite Data Protection Law in Nigeria. The principle of Judicial Activism has been saving the day and has filled this huge vacuum to a reasonable extent; this however does not pardon the lackadaisical act of the draftsmen.

In the popular case of *Godfrey Nya Eneye v MTN Nigeria Communication Ltd*,[3] the court held that the unauthorized disclosure of the Claimant's mobile phone number by his telecommunications service provider i.e. the defendant, and subsequent unsolicited text messages received from unknown third parties were violation of his constitutional right to privacy. This is to say that in Nigeria, a person is entitled to enjoy his right to privacy with no interference whatsoever from any person. In other words, service providers even in the course of their duty, have a certain limit which the principle of Purpose Limitation covers at length.

Before delving into these cases, it should be borne in mind that any Data protection Law has in it Principles which must be adhered to, to ensure the safety of all and sundry. A close perusal of the Data Protection Law of our counterparts disclosed some principles like the Principle of Fairness, Principle of Data Minimization, Principle of Purpose Limitation, Principle of Accuracy and what have they. So supposing Nigeria has its definite and unadulterated Law, it is expected to have these principles or related ones. In the Nigerian case of *Habib Nigeria Bank Limited v. Fathudeen Syed M. Koya*[4] which involved an alleged disclosure by a bank of a customer's transactional information, the Court of Appeal held that it is elementary knowledge that the bank owed its customer a duty of care and secrecy. This breach came into place because there was an excess of information required in the first place, which was outside the major purpose of the data subject.

It should be known that what Nigeria has at best is a bill, which can be challenged because it lacks definition and strong statutory back up, in other words an already made law trumps it and can have it dismissed at any stage.

***By Chinaza Shalom AJAEGBU, LLB, ChMC,** Nigerian Law School, Phone No: 07039643740.

[1] General Data Protection Regulations

[2] *UAC v Macfoy* 1962 AC 150.

[3] CA/A/689/2013.

[4] [1990 - 1993] 5 NBLR p. 368 at 387.

This is not the kind of loose laws we need in Nigeria. The Data Protection Bill 2015 is merely a bill, which has not been law; and as such there would be some inherent limitations even in it. A judicious analysis of the said Bill exposes a lot of restraints found in it. The Data Protection Bill originated in the House of Representatives in 2015 and was transmitted to the Senate in 2017; currently it is at its third stage. The Bill does not include key provisions which are in consonance with international best practice; such as mandatory consent of a data subject to processing, regulation of processing by third parties, appointment of data protection officers by organisations and fundamental considerations in permitting cross border transfer of data/the yardstick for determining adequate level of protection in foreign countries/territories to which data is transferred. Simply put, the Bill does not provide for security measures to safeguard data and prevent breach. So at the end of the day, you see Nigeria has Zero Data Protection Law and there is nothing graceful about the aftermath.

It is undeniable that the lack of comprehensive data protection legislation leaves a vacuum in the Nigerian data protection system which raises national security issues stemming from the daily processing of personal data of Nigerians by both public and private institutions and even third parties. The protection of the fundamental rights of Nigerians, especially the right to data protection in light of the technological advancements should be a major source of concern and motivation for all citizens and government alike. Data breaches in Nigeria are highly prevalent and almost conventional. Unsolicited phone calls and messages are received by Nigerian citizens on a frequent basis. A very good example of this occurred during the general elections in 2019. A legion of citizens received phone calls from some unknown persons campaigning for the ruling party, All Progressives' Congress (APC). Upon investigation, it was discovered that the phone numbers and location, which amount to personal data, were obtained from the Independent National Electoral Commission (INEC), the body responsible for conducting the elections from the data it had collected and processed to enable it register people for the elections.[5] Nigeria as it is today is no man's land as it is filled with unruly and lawless individuals, including our leaders who are topping the corruption chart. To not have a Data Protection Law in addition to the on-going madness in the state would be an invitation to the Devil's treat. Technological advancement is good but on the other arm, there are underlying threats which not curbed would leave room for doom and an horrendous aftermath. Young people are careless and too lax; today people's data are stolen from data controllers and made subjects of blackmail to extort from the vulnerable victims of this breach. Everyone has an innate need to feel safe in his environment, both in the virtual and offline environs. The Legislators can make this a dream come true by awakening the giants in them.

3. Recommendation

It is therefore proposed that our National Assembly work at passing a comprehensive data protection law sooner than later. At the very least, this inherent limitation in Nigeria's judicial system will be cured; people will be safe in this nation, and everyone wins. It is a win-win.

[5]O. Adanikin, 2019 Election: How APC may have benefited from NCC, INEC breach of voters' privacy, International Centre for Investigative Reporting published 01/02/2019 available at https://www.icirnigeria.org/2019-election-how-apc-may-have-benefited-from-ncc-inec-breach-of-voters-privacy/ accessed on 06/03/2020.