Scientific Research Publishing

Beijing Law Review, 2021, 12, 1284-1298
https://www.scirp.org/journal/blr
ISSN Online: 2159-4635
ISSN Print: 2159-4627

Data Misuse, Data Theft and Data Protection in Nigeria: A Call for a More Robust and More Effective Legislation

Abiodun Odusote

University of Lagos, Akoka-Yaba, Nigeria
Email: aodusote@unilag.edu.ng

How to cite this paper: Odusote, A. (2021). Data Misuse, Data Theft and Data Protection in Nigeria: A Call for a More Robust and More Effective Legislation. *Beijing Law Review, 12,* 1284-1298.
https://doi.org/10.4236/blr.2021.124066

Received: November 15, 2021
Accepted: December 26, 2021
Published: December 29, 2021

Abstract

The concept of life as we know it has changed dramatically in the 21st century. The shift of the world from the industrial era to the information era has highlighted the value of data, its influence on global systems and economies, and the harm that may arise from its abuse. This makes data protection laws important to protect the privacy data subjects all over the world, which is a fundamental human right under article 12 of the Universal Declaration of Human Rights (UDHR, 1948), and other globally recognized legislative instruments. As vulnerable stakeholders in the system, data subjects should have the power to decide what information to share with third parties and how this information is used. However, technological advances (such as the internet) have made the preservation of this freedom tricky. Therefore, States must enforce protection through legislative action. This paper examines the issue of data misuse and theft in the light of data privacy protection from a legal perspective, by reviewing the efforts that have been made in its development in Nigeria, the inadequacies of the current system and providing recommendations that can be implemented towards a more digital future.

Keywords

Digital Information, Personal Information, Data Privacy, Data Subjects and Data Protection

1. Introduction

It is generally agreed that globally businesses have moved from analogue to electronic. In the past, business is significantly conducted in the traditional local markets or on the High Streets, bank accounts are kept in the form of ledgers, and hard copies of records are kept. Times have changed now. Significantly,

businesses have moved online and electronic copies of records and information are kept. The concept of life and living has drastically changed. The rise of the internet from obscurity to prevalence in a few decades has had a profound effect on societal interactions and individual relationships across the globe (Wright & Chatfield, 2012). With the complexities of emerging technology in modern times, the right to privacy has become somewhat fragile, leaving sensitive data in the hands of data controllers who may or may not have due regard for this fundamental right. These custodians of data may not be so informed as to the dangers of poor and ineffective handling of data, especially as it concerns millions of people.

There has been an informed need for data privacy in Nigeria, as new developments arise. Just recently, Lagos State commissioned its first state-owned DNA forensic centre (Olasunkanmi, 2019), which has the potential of harnessing the most sensitive information of the human being: his DNA. As commendable as this action is, it is sad to note that there are no effective legislative measures to ensure that the data to be collected from this centre is protected. Especially where precedents have shown the lack of seeming regard the government has for the protection of the data of its people. For example, in 2015, the Nigerian Government contacted Mastercard, an American debit card company to process the biometric data of her citizens to produce National ID Cards (Ekott, 2014). If such data was hacked or misused by the company, there would have been no legal consequences or adequate compensation for the victim of the data misuse. There are no measures put in place to ensure that this did not happen. These are the issues that are brought to light in the discussion on data misuse, theft and protection in Nigeria. This necessitates the adoption of the doctrinal method and the comparative legal research method. These methodologies help to understand the provisions of the different data protection approaches in other jurisdictions and best practices across the globe.

Digital information unlike any other resource has been extracted, refined, valued, bought and sold in different ways (Ekott, 2014). With an estimated 4.66 billion active internet users worldwide, social media has become the greatest mechanism through which personal data is collected and these data could be exploited illegally to harm users. In Nigeria, over 101.7 million people use smartphones (Ceci, 2021) a testament to the reach the digitalized world has on a country that boasts of 200 million people. It is therefore pertinent to protect data and regulate its usage.

Under section 37 of the 1999 Constitution of the Federal Republic of Nigeria (CFRN), the privacy of citizens, their homes, correspondence, telephone conversations and telegraphic communications is guaranteed and protected. However, the right to privacy does not seem to include individual data or consider the internet and its complexities, which has brought to prominence the importance of this provision. Thus, this omission has created a vacuum left to be filled by new and existing laws, particularly those of other jurisdictions. The only

available regulatory framework in Nigeria is the Nigeria Data Protection Regulation (NDPR) issued by the National Information Technology Development Agency (NITDA) in 2019.

2. Definition of Key Terms

Data has been described as the oil of the digital era (Economist, 2021). Individual facts, statistics, or pieces of information that are gathered by observation are referred to as data. The Merriam Webster Dictionary defines it as actual information (such as measurements or statistics) used as a basis for reasoning, discussion, or calculation. But also, as information in digital form that can be transmitted or processed (Hacker, 2011). Data is a valued resource across online platforms, be it social media, online shopping websites, other e-commerce platforms, online educational platforms, etc. With people constantly uploading a lot of information ranging from their contact details and photos to sensitive details like their credit/debit card details, such data is put at risk in the hands of processors in ways which these individuals enjoying those services are unlikely to consider.

Data misuse is the use of information in ways in which it is not intended (Sham, 2020). Generally, the use of data is governed by agreements, policies, laws and regulations and where such data is used outside the scope of these laws, data misuse occurs. This could be exemplified by improper data handling practices like copying company confidential information to personal devices, thereby leaving them open for others to see and steal; improper filing systems, which could lead to collecting the wrong data from customers, or loss of data; and using data outside the given scope of authority. A scenario that typifies data misuse is when in 2017 workers in Uber, an international transportation company, deployed a device to track the whereabouts of celebrities, politicians and journalists, despite the company's privacy policy that forbade them from viewing customer ride histories (Lecher, 2016). Since then, the company has had to undergo regular third-party auditing processes to ensure that the privacy of its users is not being compromised. Another example closer to home involved Truecaller, a popular caller identity app that in 2019 was investigated by the NITDA for breaching the NDPR (Paul, 2019). Article 1.1 of Truecaller's privacy policy, allowed Truecaller to give user information to third parties, contravening Article 2.1(b) and Article 1.2 (iii) of the NDPR. The app was also asking for more information than necessary, 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. This was in actual violation of Article 2.3 (2)(d) of the NDPR, a testament to the company's flagrant misuse of user data.

On the other hand, data theft is the act of stealing information from databases, devices and servers. It usually entails a cyberattack or the collection of the data without the owner's consent and could present terrible repercussions to the

business, and the reputation of not only the owner but stakeholders to the business, which in many circumstances includes millions of users. Data theft could result from having ineffective passwords, unsecured servers, faulty networks, the use of publicly available information, terrible practices like creating fake websites and compromised wifi servers or links. With the internet growing in complexity, so also has the diversification of theft measures. In 2016, Yahoo! revealed that the data of 500 million users had been compromised in a breach that had occurred in 2014 (Volz, 2016). They claimed that this breach occurred through third-party forging cookies that were once accepted by the company's users, granting the Russian hackers' access to their accounts without the use of passwords.

As inferred from the above examples, the breach of data could have terrible consequences on affected parties. Therefore, to prevent the misuse and theft of data, the concept of data protection comes into play. Data protection is a set of strategies and processes used to secure the privacy, availability, and integrity of data (McCandlish, 2002). It is vital for any organization that collects, handles or stores sensitive data, and can help prevent misuse, loss and theft of data. It has been defined 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 (Etzioni, 2011). Such data may include the date of birth, sexual orientation, credit/debit details, inter alia. Separately, such information might not be harmful, but when collected and collated, may be used to gain more insight on the individual, and possibly predict his actions and access his financial details. The world's most valuable companies include tech giants such as Google, Apple, Amazon etc. whose subscribers are routinely required to provide their data to facilitate access to their services (Obi, 2020). Artificial intelligence through algorithms has become so smart, that it can review contracts, conduct legal research and mediation, predict exposure to disease and determine when a machine needs servicing (Ponkin & Redkina, 2018). Hence, data protection is paramount (Pang, 2021). The data industry has demonstrated such exponential growth that certain multinationals now position themselves as data purveyors and merchants (Gay, 2009). This just shows the subject of data protection is in the global context, and in developing economies like Nigeria.

3. Data Protection Regime in Nigeria

Data privacy protection entails the regulation of the use and dissemination of information. The concept of data privacy is recognized globally (Jin, 2022). Many states in the international community recognize data privacy as a right. According to the United Nations Conference on Trade and Development (UNCTAD), over 128 countries in the world have set in place data protection and privacy legislation to ensure that their citizens' data are safe (UNCTAD, 2020). This list includes Nigeria.

Being the most populated country in Africa, with industries that are developing to accommodate the rapidly evolving digital world, it is expedient that the data protection laws in Nigeria are detailed enough to protect the information of the country's people. To this effect, the following legislative framework discussed below exists.

3.1. Current Legislative Framework

Prior to the advent of the NDPR, several data protection frameworks were already in place. The CFRN is the grundnorm of the Nigerian legislative sphere and Section 37 provides for the right to privacy. It states that "the privacy of citizens, their homes, correspondence, telephone conversations and telegraphic communications is hereby guaranteed and protected." While this provision does not specifically mention data, it is arguable that that information on homes, correspondences and telephone conversations are captured in the definition of personal data and therefore, this provision could be interpreted to particularly safeguard data privacy under the canopy of the generic right to privacy. To attest to this, before the establishment of the NDPR, most data privacy cases were instituted under this section. This happened in *Emerging Market Telecommunication Services* v. *Barr Godfrey Nya Eneye* (2018) LPELR-46193, where the claimant, a legal practitioner sued the operators of Etisalat mobile line for exposing his phone number to persons/companies that sent him unsolicited text messages in violation of section 37. He was awarded damages by the Federal High Court, and on appeal, the Court of Appeal upheld this decision. See also, *Ezugwu Emmanuel Anene* v. *Airtel Nigeria Ltd*, Suit No: FCT/HC/CV/545/2015 (Unreported); *Godfrey Nya Eneye* v. *MTN Nigeria Communication Ltd* Appeal No: CA/A/689/2013 (unreported).

However, this provision is not adequate for data privacy protection given its restrictive scope. For one, it is analogous and does not consider the internet driven world we live in. Secondly, it creates room for contentions on what type of information may fall within its scope, which could lengthen judicial processes. Thirdly, the scope is already so limited, that the legislature is under the obligation to not pass any law or take any action that would unreasonably restrict it further. Instead, the right to privacy imposes an obligation on the legislature to enact a law to protect the privacy of personal data, thereby widening its scope. And so, the need for additional data protection laws is made clear by the nature of the right to privacy in the constitution which has led to its being referred to as "probably one of the most under-researched, under-litigated and under-developed rights in the Nigerian Constitution."

The Cybercrimes (Prohibition, Prevention, etc.) Act 2015 (the Cybercrimes Act) also protects certain aspects of the rights of data and privacy. The Cybercrimes Act's explanatory memorandum specifically states that the Act provides a wholesome framework for the curbing of cybercrimes in Nigeria as well as the protection of critical national information infrastructure, and the promotion of

cybersecurity, intellectual property and privacy rights.

The National Identity Management Commission Act 2007 can also be classified as falling under some of the frameworks guaranteeing data protection in Nigeria. This body is charged with the responsibility of ensuring the protection of Nigeria's national database and preventing the misuse of this information for fraudulent activities. Also, the recently published National Cybersecurity Policy and Strategy 2021 provides a framework for ensuring risk-mitigated cyberspace while ensuring cyber security optimization. In addition to the above-stated laws, sector-specific laws such as the Freedom of Information Act 2011, the Child Rights Act 2003, the Nigerian Communications Commission (Registration of Telephone Subscribers) Regulation 2011 also exist to ensure data protection in Nigeria. Section 9 of the regulation states that the subscriber's information shall be held on a strict confidentiality basis and no person or entity shall be allowed access to any subscriber's information that is on the Central Database except as prescribed by the Regulation. However, despite the presence of all these legislative documents, an all-encompassing data protection framework was still being clamoured to shed more light on grey areas in Nigeria's data protection regime.

3.2. The Nigeria Data Protection Regulation (NDPR)

The presence of comprehensive protection of data privacy in Nigeria was foreign until 2019 when efforts were made by the National Information Technology Development Agency Act 2007 (NITDA) to put an end to this menace by issuing the NDPR. This Regulation sought to sufficiently regulate data privacy, which was not covered by the existing data protection frameworks available in Nigeria at that time. The NDPR was issued in January 2019 pursuant to Section 6 (a) and (c) of the NITDA Act 2007. The Regulation is the current national law on data protection in Nigeria that applies to public and private sector processing of personal data within and outside Nigeria. This Regulation was also established to protect the right to privacy, create the right environment for digital transactions as well as create jobs and improve information management practices in Nigeria.

The NDPR provides definitions for important terms necessary for the protection and use of data in its definition section, Order 1.3. For instance, personal data is defined as any information relating to an identified or identifiable natural person technically described as a Data Subject. The Data Subject may be a human being or a non-living object but must be identifiable. Evidently, this definition goes a step ahead of previous legislations in giving defining "data" and establishing a foundation for the protection of data against misuse and theft. The NDPR is similar to and gets inspiration from the European Union General Data Protection Regulation (GDPR), with provisions on the principles of data processing, duties of data controllers towards users, need for consent of data subjects, requirements for transferring data, and requirements of data compliance officers. The regulation also includes penalty provisions for failure to comply with the regulation, Order 2.10.

To aid with its implementation, the NDPR Implementation Framework (NDPRIF) was enacted in 2019 to ensure that the NDPR was properly implemented and to prevent docility. One of the key features of the implementation framework is the provision that the NDPR's company-mandated audit be conducted by Data Protection Compliance Organizations (DPCOs) that are licensed and published by NITDA. See Nigeria Data Protection Regulation 2019: Implementation Framework, article 2 (Compliance and Enforcement).

There is no doubt that the world is now a digital one and the rate at which online users are prone to data security risks using the internet has been on the rise in Nigeria. In most instances, many companies and institutions do not take the care to put in place measures to manage and secure the personal data provided by their users. They also do not specify clearly the nature in which or the purpose for which the data would be used (Pang, 2021). The provisions of how the user's data would be used are usually included in print form and most people, especially those who are uneducated, easily miss them. Thus, the data either end up getting stolen or used inconsistently with the users' rights of privacy.

The NDPR indeed plays a significant role in protecting data privacy and protection in Nigeria, evident in its provisions ensuring that personal data collected are used for the purposes they are collected. However, these regulatory provisions only cover natural persons and not artificial or legal persons (Omoniyi, 2021). This is a massive setback as these legal entities are made up of natural persons, and a breach of their privacy as a legal entity may amount to a breach of their personal data individually (Scott & Eke, 2020). Furthermore, the NPDR merely provides that a breach of its provisions amounts to a breach of the NITDA Act. It fails to provide explicit and specific punishments for non-compliance. The fact that the NPDR is only a Regulation and not an Act enacted by the National Assembly also contributes to its limitations in scope and application.

4. Challenges of Data Protection in Nigeria

As inferred above, Nigeria's data protection scene is hampered by obstacles that constantly lead to the infringement of the rights of users. These issues are comprised of but are not limited to the following:

4.1. Inadequacy of the NDPR and Other Legislations

Despite the NITDA's admirable efforts with the issuance of the Nigeria Data Protection Regulation (NDPR) 2019, data privacy concerns remain an issue, because the regulation remains restrictive in scope. For instance, Paragraph 1.0 (a) of NDPR restricts the safeguard/protection offered under the regulation to, rights of only natural persons. Therefore institutions/businesses that may fall victim to a data privacy breach, misuse or theft may not have recourse under the regulation if a plain judicial interpretation is implemented by the court. The act also only protects electronic data, not taking into consideration that data could be

physical (in form of letters, surveys, cheques, etc.). These shortcomings fall counterproductive to the intention of the act which was to widen the scope of Section 37 in protecting the data of the individuals. And so, these restrictions fall short of iconic when viewed in this light and may create room for the creation of legislation that widens the scope, yet again, thereby posturing to the NDPR's impending redundancy.

With regards to the definitions used, while they go a step ahead of the constitution, they are also inadequate when compared to foreign laws on the same subject. Data is defined under the regulation as "characters, symbols and binary which operations are performed by a computer which may be stored by transmitted in the form of electronic signals is stored in any format or any device." The word computer here is limiting and connotes that the NDPR may not protect information that is not stored outside the use of ICT systems. The GDPR does not define data, but it defines "personal data" as information relating to identified or identifiable natural persons. See 4(1) And the Black's Law Dictionary (Garner & Black, 1999) also doesn't define data but defines a "database" as a "compilation of information arranged in a systemic way." These definitions capture the essence of data, which is "information." The non-use of words that could restrict the meaning of data is evident here also, an element that the NDPR lacks.

Furthermore, while regulation 2.10 of the NDPR imposes a penalty for violating data privacy rights, the rights are not explicitly stated anywhere in the regulation. Instead, one must improvise by turning to regulation 2.13's "Rights of a Data Subject" provision. And even though while the regulation outlines the consequences of non-compliance, it is vague on the remedies available to victims of data-privacy breaches. The punishments outlined therein would simply serve to enrich the Government at the cost of the actual victims of data breaches. This is a glaring oversight and defies the age-long principle of *ubi jus ubi remedium*, "where there is a right, there is a remedy."

And while recourse can still be found under Section 37 of the Constitution of the Federal Republic of Nigeria (CFRN) 1999, it does not come without its hitches. Since this provision does not explicitly refer to "data," it is subject to debate whether or not information on homes, correspondences and telephone conversations stated in the law, connote personal data. Therefore, it is moot whether section 37 can be invoked to defend data breach.

Proponents of this position argue that the right of the subject of a data breach to legal recourse is an offshoot of the right to privacy under Section 37 of the CFRN and the NITDA Act 2007. This was given credence by the decision of Ogun State's High Court *in Incorporated Trustees of Digital Rights Lawyers Initiative* v. *L.T Solutions & Multimedia Limited* (*DRLI v. LTSM*) Suit No. AB/83/2020 (unreported). Here, the court held that a data subject's rights under the NDPR may be enforced as a constitutional right under the Fundamental Rights Enforcement Procedure 2009 (FREP) Rules. However, on the other side

of the argument, the position is that a data subject's rights under the NDPR are neither constitutional rights nor fundamental under the bill of rights, hence, they should not be enforced as such. This argument is premised on the absence of the word data in section 37. But it loses weight where certain specific laws and regulations provide specific protections as detailed above. Notwithstanding, this lack of constitutional presence has given room for loopholes in the enforcement of data protection in Nigeria.

4.2. Systematic Inadequacies

Inadequacies in the system can be seen from several angles. First, there is a lack of synchrony between existing Nigerian data protection legislation and the problems meant to be solved. A practical example can be seen in the case of trespassing and hacking into a computer network. While both offences appear to be similar, the penalty for trespass does not apply to hacking private data. And so, there are no relevant provisions in Nigerian law that cater to hacking private data (Muli & Mutua, 2013). This is a situation in which there are no applicable laws against hacking. Also, even with existing regulations, sufficient protection of personal data is lacking especially as regards to data collection, processing and control which is not up to par with international standards set by the GDPR.

In a 2019 Business Day interview, the Chief Data Officer of Sterling Bank, Fatai Tella, said that there was a lack of synergy among stakeholders in the data protection industry and that it was necessary to sit down and discuss the data breaches that should necessitate a policy (Eleanya, 2019). Issues like this have given rise to the NDPR being described as sketchy in comparison to the GDPR and other international laws (even though the NDPR borrows a lot of its fundamental principles from the GDPR) due to the incongruencies and loose ends presented in the regulation that has prevented its smooth application, thereby making it appear to be an act that exists for the sake of existing.

Education is also an issue, rife within the system. One that ties in with the ignorance many subjects of data breaches have as regards their rights to privacy and data protection, and the dangers that the internet and other data collectors (like telecommunication companies and organizations) poses to their safety and their privacy. Valid consent must be sought before data collection, particularly by a clear statement of the data collection objective and notice of the need for extra consent where personal data may be shared with third parties. However, this is usually not the case in Nigeria. As both private and public entities have consistently failed in upholding these ethical rules and guidelines, and a lot of people who fall victim are unaware that either they have fallen victim, or that they recourse under the law.

Furthermore, due to the aforementioned statutory issues, the lack of uniformity in judicial opinion with relation to data privacy poses a barrier to data protection in Nigeria. While some courts view data privacy as a basic right of the data subject, others see it as a right to be safeguarded by regulatory control, even if the data was provided to a firm for the purpose of providing services. This lack of uniformity in

judicial opinion on data control is a significant concern because it exposes individuals and organizations to data breaches and may prevent them from seeking redress. To make matters worse, there is a huge lacuna when it comes to cases on data privacy, data theft and misuse within the country which is bad news for a system of law that is built upon judicial precedents. From all the aforementioned, it appears as though the data privacy scene is undergoing a battle.

4.3. Lack of Technical Knowledge on Data

As Nigeria develops, it is worth mentioning that we still have a long way to go. Many companies in a bid to keep up with the times are becoming digitalized, to expand their reach and get a foothold in the global market sphere. The question is whether going digital and having digital systems is more than just an aesthetic. And if adequate thought is given into cybersecurity, which could look like employing the right personnel to oversee company information systems and imbibing data privacy into the company culture. It has been seen that is not so. Several cases have exposed the propensity for Nigerian companies (Eleanya, 2019) (especially within the telecommunication industry) to take advantage of the data belonging to their clients for extraneous purposes and to sometimes sell these to third parties. Even with individual data users, a great majority do not understand the concept of sensitive information and how it becomes currency when used on the internet.

4.4. Lack of Reporting/Recording of Data Breaches

Despite the establishment of the NDPR, several data breaches are unreported and undocumented. This is due to a variety of factors, including a delay in notifying the data subject of the breach and reporting the incident to the relevant authority (Salau, 2016). This is in direct conflict with article 33 of the EU General Data Protection Regulation (GDPR), which requires Controllers/Processors to report data breaches within 72 hours to the appropriate authority and the affected parties if the breach poses an implementation difficulty. In the case of a data breach, African data protection regimes must include notification procedures. In *Habib Nigeria Bank Limited* v. *Fathudeen Syed M. Koya*' a case involving an alleged disclosure of a customer's transactional information by a bank, the Court of Appeal held it to be basic knowledge that the bank owed its customer a duty of care and secrecy.

As already mentioned, in most cases in Nigeria, the data subjects are ignorant of their rights to data protection. Data collectors/administrators may equally be unaware of their duty to protect and respect the privacy of data in their care. A handful of civil societies advocating and monitoring data protection have emerged in recent times to this effect (Madbuike, 2018).

4.5. Non-Compliance and Enforcement of Existing Legislation

It is an issue of concern whether the provisions of the data protection regulation

are disregarded by most agencies and parastatals. For example, the NDPR act, slated to be launched on the 25th day of January 2019, was meant to take effect from 25th April 2019, pending the distribution of protection policies by data collectors as required by section 2.5 of NDPR. However, the due date has passed, and the data collectors are yet to publish their privacy policies (Obi, 2020). To make matters worse, the NITDA has failed to penalize them as required in section 2.10 of the NDPR, hence, the compliance with the NDPR is off to a rocky start. Other provisions for prompt and constant compliance, like section 4.1(2) which requires every data controller to designate data protection officers have also been grossly ignored.

Recently, the Nigeria Immigration Service posted the international passport data page of a Nigerian resident in the UK on their social media page without his consent; a gross violation of the subject's right to privacy. However, nothing has been done about this by the enforcement agency of the NDPRIF, whose duty is to ensure compliance. Its existence remains a mirage to any actual show of interest in ensuring that the ideals of the regulation are upheld. And as we all know; laws are only useful when they are implemented.

5. Recommendations

The following recommendations are hereby proposed to ensure that the problem of data protection in Nigeria becomes a thing of the past:

Uniformity in law is the first important step. As seen above, while Nigeria has several legislative documents that mention data privacy, and the NDPR was enacted also to this effect, the NDPR is inadequate in substance and being. A proper law protecting the right to privacy is required, not a regulation. And its contents should portray adequate definitions to encompass the ever-changing reality we live in. Adequate penalties and remedies for data breach and misuse should be stipulated by the act, and it should cover the data privacy of bodies both real and constructive.

Presently, a bill has been presented before the National Assembly "Data Protection Bill 2020" with the objective of improving upon the NDPR. This Act aims to protect personal data, minimise the harmful effect of personal data misuse and establish a functional regulatory organ and ensure that personal data is protected in a transparent, fair and lawful manner (Scott & Eke, 2020). However, like the NDPR, it does not accord any protection for corporations or institutions which might fall victim to data misuse or theft. Nevertheless, this Bill promises to solve some of the issues raised above. For the uniformity in data protection laws, part 1(a) of the Bill stipulates that it aims to promote a code of practice that ensures the privacy and protection of data subject's data without unduly undermining the legitimate interests of commercial organisations and government security agencies for such personal data. And as regards the compensation of victims, the Bill makes provision for a court of law to grant orders for the compensation of victims of offences by convicted persons, an element that is missing in the NDPR among other improvements.

Education is important on several levels. Users should be taught the importance of their data, their rights under existing laws, and the best ways to ensure they are protected from misuse. This education should also be prioritized in companies. Practising professionals should be adequately trained on the content of the laws, how to apply them, and the ethics of responsibility. Companies should ensure that systems of checks and balances are in place, as seen in the Uber case stated above. And routine previews are done on their clouds to ensure that the privacy of their information and those of their clients are safe. Privacy ethics should also be taught to employees as part of company policy.

A constitutional amendment is required to ensure that data privacy is enshrined in the country's most essential legislative document. This is the first step in ensuring that the State has made advancements towards prioritizing the protection of personal data. The NDPR could be reviewed to address some of the issues that have hindered its efficient implementation. Efforts should be made to ensure that the document stays up to date with whatever new challenges may arise as the data protection scene expands to accommodate modern reality.

Finally, all these efforts will be useless without sufficient plans for implementation. In the wake of a revised act, the NITDA could award incentives and sanctions for cooperation or the lack thereof to public and private bodies involved. They could also implement a body that ensures that companies are conducting ethical practices with the data they collect from others, and issue guidelines as to the level of cyber protection they should meet in exchange for certifications that improve their goodwill before the country. This way, the motivation to take data protection and privacy more seriously would be encouraged.

6. Conclusion

Data Protection in Nigeria has come a long way, from a lack of legislative backing to a regulatory instrument that though imperfect, has served as a placeholder in ensuring that individuals have a resource they can rely on to safeguard their privacy and to protect them from data misuse and theft. However, as seen from the above developments, a lot of work still needs to be done in ensuring that the data protection scene remains up to date with the ever-changing digitalized world. The NDPR is inadequate in substance and implementation and there is an acute lacuna in the understanding of data privacy by users and data controllers. With adequate revisions, the road to data protection in Nigeria will become paved.

Notes

A data controller is a public or private individual or legal entity, body or association, who alone or jointly with others, decides to collect and process personal data and determine the purposes for which such data are processed.

Conflicts of Interest

The author declares no conflicts of interest regarding the publication of this paper.

References

Babalola, O. (2020, March 9). *Data Protection and Privacy Challenges in Nigeria (Legal Issues).* Mondaq. https://www.mondaq.com/nigeria/dataprotection/901494/data-protection-and-privacy-challenges-innigeria-legal-issues

Ceci, 2021.

Child Rights Act 2003.

Constitution of the Federal Republic of Nigeria (CFRN), 1999.

Cybercrimes (Prohibition, Prevention, etc.) Act 2015.

Data Protection Bill 2020.

Digital Rights Lawyers Initiative v. L.T Solutions & Multimedia Limited (DRLI v. LTSM) Suit No. AB/83/2020 (Unreported).

Economist (2017, May 6). Data Is Giving Rise to a New Economy. *The Economist.* https://www.economist.com/briefing/2017/05/06/data-is-giving-rise-to-a-new-economy

Ekott, I. (2014, August 29). Scandalous: Outrage in Nigeria as Government Brands National ID Card with MasterCard's Logo. *Premium Times.* https://www.premiumtimesng.com/news/headlines/167479-scandalous-outrage-in-nigeria-as-government-brands-national-id-card-with-mastercards-logo.html

Eleanya, F. (2019, Nov. 6). The NDPR Isn't Perfect But It's a Step to Data Protection for Nigeria. *Business Day.* https://businessday.ng/technology/article/the-ndpr-isnt-perfect-but-its-a-step-to-data-protection-for-nigeria

Emerging Market Telecommunication Services v. Barr Godfrey Nya Eneye (2018) *LPELR-46193.*

Etzioni, A. (2011). The Privacy Merchants: What Is to Be Done. *University of Pennsylvania Journal of Constitutional Law, 14,* 929. https://doi.org/10.2139/ssrn.2146201

EU (2016). *General Data Protection Regulation (GDPR): Regulation* (p. 679). European Union.

European General Data Protection Regulation (GDPR).

Ezugwu Emmanuel Anene v. Airtel Nigeria Ltd, Suit No: FCT/HC/CV/545/2015 (Unreported).

Freedom of Information Act 2011.

Fundamental Rights Enforcement Procedure 2009 (FREP).

Garner, B. A., & Black, H. C. (1999). *Black's Law Dictionary.*

Gay, S. (2009). The Lamp-Oil Merchants of Iwashimizu Shrine: Transregional Commerce in Medieval Japan. *Monumenta Nipponica, 64,* 1-51. https://doi.org/10.1353/mni.0.0057

Godfrey Nya Eneye v. MTN Nigeria Communication Ltd Appeal No: CA/A/689/2013 (Unreported).

Habib Nigeria Bank Limited v. Fathudeen Syed M. Koya.

Hacker (2011). In *Merriam-Webster.com.*

Jin, C. (2022). The Civil Law Protection of Citizens' Personal Information in the Context of Big Data. In *International Conference on Cognitive Based Information Processing and Applications (CIPA 2021)* (pp. 313-320). Springer.

https://doi.org/10.1007/978-981-16-5854-9_39

Lecher, C. (2016, December 12). *Uber Employees Secretly Tracked Politicians and Celebrities, Lawsuit Claims*. The Verge. https://www.theverge.com/2016/12/12/13920258/uber-employees-tracking-celebrities-security-lawsuit

Madbuike, E. (2018, May 31). *GDPR: 7 Types of Nigerian Companies That Should Comply*. Techpoint Africa. https://techpoint.africa/2018/05/31/gdpr-compliance-nigeria

McCandlish, 2002.

Muli and Mutua, 2013.

National Cybersecurity Policy and Strategy 2021.

National Identity Management Commission Act 2007.

National Information Technology Development Agency Act 2007.

Nigeria Data Protection Regulation (NDPR) 2019.

Nigerian Communications Commission (Registration of Telephone Subscribers) Regulation 2011.

Obi, U. V. (2020, September 9). *An Extensive Article on Data Privacy and Data Protection Law in Nigeria*. International Network of Privacy Law Professionals. https://inplp.com/latest-news/article/an-extensive-article-on-data-privacy-and-data-protection-law-in-nigeria

Olasunkanmi (2019, February 22). *Lagos DNA Forensic Centre Receives International Accreditation*. Lagos State Government Official Web Portal. https://lagosstate.gov.ng/blog/2019/02/22/lagos-dna-forensic-centre-receives-international-accreditation

Omoniyi (2021). *Actions: Beyond the Nigerian Data Protection Regulations (NPDR) 2019*. Le Law. https://www.lexology.com/library/detail.aspx?g=6a860952-efec-4624-a6d8-f6d58970f25f

Pang, X. (2021). Civil Law Protection of Personal Information in the Era of Big Data. *Open Access Library Journal, 8,* 1-12. https://doi.org/10.4236/oalib.1108016

Paul, E. (2019, September 25). *NITDA Investigating Alleged Privacy Breach by Truecaller*. Techpoint Africa. https://techpoint.africa/2019/09/25/nitda-truecaller-privacy-breach

Ponkin, I. V., & Redkina, A. I. (2018). Artificial Intelligence from the Point of View of Law. *RUDN Journal of Law, 22,* 91-109. https://doi.org/10.22363/2313-2337-2018-22-1-91-109

Salau, A. O. (2016, February 22/23). Data Protection in an Emerging Digital Economy: The Case of Nigerian Communications Commission: Regulation without Predictability? In M. Bottis, & T. Alexandropoulou (Eds.), *Broadening the Horizons of Information Law and Ethics: A Time for Inclusion* (pp. 1-486). University of Macedonia Press. http://icil.gr/download.php?fen=years/2016/downloads/documents/icil_2016_proceedings_book.pdf

Scott, B., & Eke, S. (2020, July 3). *Nigeria: NDPR and the Protection of Personal Data of Legal Entities in Nigeria*. Mondaq. https://www.mondaq.com/nigeria/privacy-protection/961432/ndpr-and-the-protection-of-personal-data-of-legal-entities-in-nigeria

Sham, S. (2020, June 25). *What Is Data Misuse*? Okta. https://www.okta.com/blog/2020/06/data-misuse

UNCTAD (2020, April 2). *Data Protection and Privacy Legislation Worldwide*. UNCTAD. https://unctad.org/page/data-protection-and-privacy-legislation-worldwide

Universal Declaration of Human Rights (UDHR) 1948.

Volz, D. (2016, September 22). *Yahoo Says Hackers Stole Data from 500 Million Accounts in 2014*. Reuters. https://www.reuters.com/article/us-yahoo-cyber-idUSKCN11S16P

Wright, J., & Chatfield, T. (2012, March 3). As Google Acts, the Question Is: Have We Lost Our Privacy to the Internet? *The Guardian*. http://www.guardian.co.uk/technology/2012/mar/03/internet-privacy