Journal of Law, Policy and Globalization
ISSN 2224-3240 (Paper) ISSN 2224-3259 (Online)
Vol.121, No.2 2022

Challenges to the Implementation and Enforcement of Data Protection in Nigeria

IBRAHIM SHEHU[1]
AND
SANI RABIU BELLO[2]

Abstract
Data protection is an important tool to the development of any country. The purpose of this research is to discuss on the challenges to implementation and enforcement of electronic data protection with a view to highlighting the challenges and identify some of the remedial measures that need to be adopted in addressing the challenges. There have been threat to data protection in developing countries and such threats are evident in developed countries, for instance the laws on data protection and privacy which are not specific to the target, like the Constitution of the Federal Republic of Nigeria, 1999 (as amended) and the Nigeria Data Protection Regulation 2019. Other challenges to data protection as identified in this paper include dearth of judicial decisions on data privacy violations, unethical computer users in the office, computer system mal-function, hardware failure, power blackouts and power failures, lack of data protection practitioners in Nigeria, issue of consent to data collection. Doctrinal method of research is adopted for writing this paper. Certain remedies are discussed which includes internet regulation for users and internet service providers, computer ethics education and training among users, cross-border harmonization of laws on data protection and enforcement procedures, response to and preparing for power blackouts/power failures, response to system and hardware failures and introduction of national youth development forums and self-employment initiatives. Data protection is a vital tool to the development of any country.
Keywords: Enforcement, Data Protection, Nigeria
DOI: 10.7176/JLPG/121-2-07
Publication date: May 31st 2022

INTRODUCTION

Up until January 25, 2019, Nigeria did not have any dedicated general legislation on data privacy and protection apart from the 1999 Constitution (as amended) which has not been particularly useful for this purpose especially when considering our courts' somewhat restrictive approach to the interpretation of the relevant section on privacy.Currently, as our laws stand, for the enforcement of data protection and privacy in Nigeria, we now have section 37 of the Constitution of the Federal Republic of Nigeria, 1999 (as amended) and the Nigeria Data Protection Regulation 2019 which may be used correlatively to achieve a common purpose. This resulted in bringing some challenges to the implementation of data protection in Nigeria.
Section 37 of the 1999 Constitution provides that:
"The privacy of citizens, their homes, correspondence, telephone conversations and telegraphic communications is hereby guaranteed and protected."

Although the provision above does not specifically mention "data", it is arguable that information on homes, correspondences and telephone conversations are captured in the definition of personal data, hence, the above provision can be used to safeguard such breach.[3]

The Nigerian Data Protection Regulation (NDPR) was introduced by the National Information Technology Development Agency (NITDA) on 25th January 2019 signaled the gradual institutionalisation of a culture of data privacy and protection in Nigeria. A deeper awareness and appreciation of relevant issues around data privacy and protection has begun to take root. Before the NDPR came into force, Nigeria's regime of data privacy and protection existed in multiple legislations that sought to protect subject-specific data and information from unlawful use. These ultimately proved inadequate in addressing the concerns of owners, users and regulators of data, thus giving birth to the NDPR. The NDPR is currently Nigeria's singular most comprehensive body of rules that govern data privacy and protection.[4]
The NITDA guidelines define personal Data as

[1] Senior Lecturer, Faculty of Law, Usmanu Danfodio University, Sokoto.
[2] Lecturer 1, Faculty of Law, Bayero University, Kano.
[3] Olumide Babalola: DATA PROTECTION AND PRIVACY CHALLENGES IN NIGERIA (LEGAL ISSUES), 09 March 2020, Available at https://www.mondaq.com/nigeria/data-protection/901494/data-protection-and-privacy-challenges-in-nigeria-legal-issues-. Accessed on March 4, 2021.
[4] UCHE VAL OBI: DATA PRIVACY AND PROTECTION REGULATIONS IN NIGERIA, 02.12.2020, Available at https://inplp.com/latest-news/article/challenges-confronting-implementation-of-data-privacy-and-protection-regulations-in-nigeria/. Accessed on March 2, 2021.

"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, Personal Identifiable Information (PII) and others."[1]

CHALLENGES ON ENFORCEMENT OF ELECTRONIC DATA PROTECTION

There are myriads of problems or challenges on enforcement of data protection in Nigeria. These challenges include:

1. **INADEQUACY OF DATA PRIVACY AND PROTECTION LEGISLATION:**
   Even in spite of NITDA's commendable issuance of NDPR in January 2019, it still does not completely solve data privacy concerns. The NDPR is, sadly, limited to electronic data thereby leaving paper-based data violations without remedies or protection. Recourse may however be had to section 37 of the Constitution but reliance thereon is not without its own nuances especially when faced with a narrow-minder court as we have seen in the past, where clear cases on infringement of privacy have been struck out because the court concerned preferred to deal with them as tort of nuisance. Worthy of mention, is the effort of Paradigm Initiative at sponsoring the Digital Rights Protection Bill which was however rejected by the President. Its passage would have eased the inadequacies of section 37 and the NDPR on data protection issues.
2. **TECHNOLOGICAL ADVANCEMENT IN INFORMATION AND COMMUNICATION TECHNOLOGY**
   A lot of progress has been made in discovering new knowledge in the field of information and communication technology. Some of the new knowledge and advancements have been used destructively. For instance, hackers use their high-tech skills to change, intrude or interfere with computer networks with an intention of destroying information or making some money out of it.[2] Bullesbach[3] notes that, development and application of new ICT lead to challenges of data protection. Though new technologies in developing countries are a positive step of development, proper planning is necessary before applying new knowledge. Hackers use principles of new technologies. It should be noted that hackers may indeed be consultants in the particular firms they are working for. It means that such crimes may go undetected or can be detected after a long time. The reason is that the consultant (hacker) occupies a position of trust and nobody would suspect any ill motives in his operations. After all, he is a consultant. Capron explains that, most computer crimes are discovered by accident. He identifies a case in which employees of a certain city welfare department created a fictitious workforce and programmed the computer to issue pay cheques, which the employees would intercept and cash.
   Spamming is a crime that is also linked to technological advancement in the field of ICT. The current explosion of mobile phone communication and cheap email services has attracted a lot of spamming activities.[4]
3. **COMPUTER ETHICS EDUCATION AND TRAINING AMONG USERS**
   Ethical practices in the work environment form the basis of success for any business venture. Boulton (ud) observes that, employees in small business firms are likely to pirate software, a practice that is seemingly endorsed by the management for purposes of business survival. The main challenge here is piracy within the office/business atmosphere where the superiors may not regulate their users. Otherwise, there may not be clear guidelines on ethical practice in the office.[5]
   Piracy of data is practiced by experts with the necessary technical knowledge. For example, IT (Information Technology) consultants may use pirated software to complete certain projects. Developing countries experience this problem because of the increasing unemployment trends, where people survive by using illegal business practices to make a living. Illegal transactions can be carried over a network without being noticed. Bynum explains that, there are always problems in the application of computer ethics because there are no clear policies of how computer technologies should be used.[6]

[1] Section 1(3) (a) of NITDA Regulation.
[2] Muli David Tovi, Mutua Nicholas Muthama: ADDRESSING THE CHALLENGES OF DATA PROTECTION IN DEVELOPING COUNTRIES, European Journal of Computer Science and Information Technology, Vol.1, No. 1, pp.1- 9, September 2013.
[3] 2004.
[4] Muli David Tovi, Mutua Nicholas Muthama: (n6).
[5] Muli David Tovi, Mutua Nicholas Muthama: (n 6).
[6] Ibid.

4. **COMPUTER SYSTEM MAL-FUNCTION AND HARDWARE FAILURE**
   Data should not only be protected from people (users) but also from computer systems that either not functioning well or hard ware that fails to function appropriately. System operations are related to the software used. System failure, according to Meadowcroft (2005) may result from the complexity of the software used. Developing countries are using modern software which is complex and efficient in operation. If there is improper coding of software, the system is likely to fail. Data held in such a system is also likely to vanish if the system malfunctions. System failure can result from the user e.g. when the user gives the computer inaccurate instructions. This may lead to loss of files and indeed data held in these files, hardware such as diskettes are vulnerable to conditions such as extreme temperatures, scratching, pressure and presence of magnetic fields. [1]
5. **DEARTH OF JUDICIAL DECISIONS ON DATA PRIVACY VIOLATIONS**
   The Nigerian judiciary, like its counterpart elsewhere, thrives on judicial precedents, especially when the lower courts are confronted with somewhat novel cases. Our case law is however replete with straight jacketed privacy cases which relate to invasion of homes and offices as opposed to invasion of data privacy stricto sensu.
   Apart from the decision in **Emerging Market v Eneye** (supra), there is no other appellate court decision on invasion of telephone (data) privacy. Hence, it is increasingly difficult for practitioners and judges to find authorities on which they can rely on while granting reprieve to data violation victims.[2]
6. **LACK OF DATA PROTECTION PRACTITIONERS IN NIGERIA**
   Yet another pertinent challenge facing the industry in Nigeria has to do with the role that a credible professional body could play in ensuring strict adherence to a regulatory framework by all practitioners and stakeholders within both the private and public sectors of the economy. This body may also be charged with the responsibility of monitoring developments in regulatory governance and technology to keep abreast with international standards and best practices. [3]
7. **ISSUE OF CONSENT TO DATA COLLECTION**
   Another important issue is the requirement to secure the consent of a Data Subject before personal data may be sourced and utilised for any purpose. Consent implies that valid consent must be obtained before the collection of data, especially through clear stipulation of the purpose of data collection and indication of the need for additional consent where personal data might be shared with third parties. Furthermore, a Data Controller is required to take and keep a record of the consent of individuals, and there must be provision for withdrawal of consent by such Data Subject at any time (European Data Protection Board, 2016). Regrettably, in Nigeria, both government agencies and private firms have consistently failed to comply with these aspects of the NDPR by their actions, thus causing untold embarrassment and hardship to affected persons. In Nigeria, it is not uncommon to experience data about one being generated and captured by companies and agencies without knowledge of its owner or first seeking and securing consent.[4]

REMEDIES TO THE CHALLENGES

The following are regarded as attempts to remedy the challenges of data protection. However, these are not, by any means exhaustive.

1. **Internet Regulations for both Users and Internet Service Providers**
   New technologies contribute to the national development of developing countries. However, challenges due to the technological advancement retard the growth of some sectors of the economy. Internet access is one of the main issues. Developing countries need to initiate self regulation mechanisms. Bullesbach (2004) observes that, adequate data protection is effective when countries initiate data protection by means of self regulation. This is an important aspect for developing countries because of the different cultural diversities of their people. Self regulation mechanisms would cater for all diverse cultures different from the western countries. Developing countries should embrace a self regulatory approach by encouraging their internet service providers to regulate their customers by establishing regulatory mechanisms internal to their businesses. This would cultivate ethics among customers in using the internet. Spamming can also be controlled by using combined efforts between law enforcement

[1] Ibid at page 4.
[2] Olumide Babalola: DATA PROTECTION AND PRIVACY CHALLENGES IN NIGERIA (LEGAL ISSUES), 09 March 2020, page 9, Available at https://www.mondaq.com/nigeria/data-protection/901494/data-protection-and-privacy-challenges-in-nigeria-legal-issues-. Accessed on March 4, 2021.
[3] UCHE VAL OBI: DATA PRIVACY AND PROTECTION REGULATIONS IN NIGERIA, 02.12.2020, Available at https://inplp.com/latest-news/article/challenges-confronting-implementation-of-data-privacy-and-protection-regulations-in-nigeria/. Accessed on March 2, 2021.
[4] Ibid.

agencies and internet service providers.[1]

2. **Computer Ethics Education and Training among Users**
   Ethical practices are an important component of any professional field. In this era of ICT, a lot of data relating to people, governments and business organizations is being handled by computing professionals. As a result a high level of ethical practice is essential. Ethical practices can be imparted to computing professionals during their course of study or being given in-service training. Ethical practices in developing countries should serve a central role in alleviating data crimes. Computer users in these countries should be trained on ethical issues related to data protection. There is a need for refresher courses on emerging issues such as internet pornography, spamming, hacking and other forms of cybercrime. All these issues are as result of the advancement in ICT. The main remedy is therefore a code of practice for all computing professionals and service providers in ICT. Not all computer-related infringements are noticed. This is why all computing professionals should regulate their practices in an ethical point of view. Personal data should also be protected from unauthorized access.[2]
3. **Cross-border Harmonization of Laws On Data Protection and Enforcement Procedures**
   Data protection requires concerted efforts which must involve harmonization of new or existing legislation. These laws must have an international setting and applicable to all states regardless of whether a country is developed or not. Conflicting or no laws at all hampers the fight against illegal data access and cyber crimes. Developing countries need to establish common laws that can be uniformly applied in different countries for the same crime. Relevant stake holders in developing countries should therefore hold common forums within which certain laws can be harmonized[3]
4. **Response to System Failure, Hardware Failure and Power Blackouts** Data needs to be protected against physical factors such as system failure, hardware failure and power blackouts. System failure may depend on the users and this is why users have a central role to play to avoid system failure. The best practices for avoiding system failure, according to Phillips (2004), include user manuals that provide system specifications and also testing the code.[4]
5. **National Youth Development Forums And Self Employment Initiatives**
   Developing countries should view youth unemployment as the major source of the numerous economic crimes including data piracy. The youth should play an important role in data protection. Governments in developing countries should initiate forums that are aimed at educating the youth on self employment and also organizing workshops for educated but unemployed youth. They should establish youth groups whose main objective is to eradicate data crimes.[5]

CONCLUSION

It can be concluded in this study that the challenges of Data Protection will continue to manifest in developing countries and this is because there has been technological changes and advancement in Information communication Technology, therefore developing Countries need to review their existing Laws or establish new laws, review the enforcement procedures and they should also review existing curricula for computer professionals.

It is recommended that data privacy and protection should be given adequate Legislation and Judicial consideration and with this approach, the challenges to the implementation and enforcement of electronic data protection will be reduced if not eliminated.

[1] Muli David Tovi, Mutua Nicholas Muthama: (n 6)
[2] Ibid at page 5.
[3] Ibid at page 6.
[4] Ibid at page 6.
[5] Ibid at page 7.