KAMPALA INTERNATIONAL UNIVERSITY

LAW JOURNAL

KIULJ Vol.4 Issue 1,2022

KAMPALA INTERNATIONAL UNIVERSITY

LAW JOURNAL

(KIULJ)

KIULJ. VOL 4, ISSUE 1, 2022

KAMPALA INTERNATIONAL UNIVERSITY LAW JOURNAL (KIULJ)

Journal of School of Law, Kampala International University, Kampala, Uganda

ISSN: 2519-9501(Print)

ISSN: 2519-9528(Electronic)

Published by:
School of Law
Kampala International University
P.O. Box 20000 Kampala
Kampala
Uganda

ABOUT THE JOURNAL

KAMPALA INTERNATIONAL UNIVERSITY LAW JOURNAL is the official journal of the School of Law, Kampala International University. It is a peer-reviewed journal providing distinctive and insightful analysis of legal concepts, operation of legal institutions and relationships between law and other concepts. It is guided in the true academic spirit of objectivity and critical investigation of topical and contemporary issues resulting from the interface between law and society. The result is a high-quality account of in-depth assessment of the strengths and weaknesses of particular legal regimes with the view to introducing reforms. In furtherance of the requirements of advanced academic scholarship, the Journal places high premium on originality and contribution to knowledge, plain and conventional language, and full acknowledgment of sources of information among other things. It is superintended by a Board of respected academics, lawyers, and other legal professionals.

The Journal offers useful reference material to legal practitioners, international organisations, non-governmental organisations and the academia. It also provides multipurpose policy guide for the government.

The Journal is a biannual publication. Calls for articles and submission datelines are determined by the editorial board.

All correspondences are addressed to:

The Editor-in-Chief
Kampala International University Law Journal,
School of Law,
Kampala International University,
P.O. Box 20000 Kampala,
Uganda.
valentine.mbeli@kiu.ac.ug
Tel: (+256) 0706970595
Website:www.kiulj.kiu.ac.ug

Scope

Kampala International University Law Journal (KIULJ) is the official Journal of the School of Law, Kampala International University, Uganda. It is a peer-reviewed Journal providing an objective and industry focused analysis of national and international legal, policy and ethical issues. The Journal publishes well researched articles that are in sync with sound academic interrogation and professional experience on topical, legal, business, financial, investment, economic and policy issues and other sectors.

Citation

This Journal may be cited as ***KIULJ Vol 4, Issue 1, 2022.***

Disclaimer

Statements of fact and opinion contained in the *Kampala International University Law Journal* are those of the respective authors and contributors and are not necessarily those of the School of Law, Kampala International University, the editors or the institutions with which the authors are affiliated. Accordingly, the authors and contributors are responsible for the integrity and accuracy of the respective material contents and references. The School of Law, Kampala International University, does not make any representation, express or implied, with regard to the accuracy of the materials in the Kampala International University Law Journal and wishes to unequivocally disclaim any responsibility or liability for such materials.

FROM THE EDITORIAL SUITE

The primary objective of the **KAMPALA INTERNATIONAL UNIVERSITY LAW JOURNAL (KIULJ*)*** is to provide a platform for a robust intellectual discourse, through the publication of incisive and insightful articles and other contributions from a variety of scholars, jurists and practitioners across jurisdictions. The desire to accomplish this objective guides the choice of the materials being presented to the reading public in every edition. The peer review and editing processes of the papers that are finally selected for publication are equally influenced largely by the pursuit of this goal.

To this end, articles from seasoned scholars and practitioners in each edition address a wide spectrum of issues from different branches of the law, such as, International Criminal Law, Law of International Institutions, Environmental Law, Human Rights Law, Medical Law, Oil and Gas Law, Constitutional Law, Corporate Governance to mention but a few. You will, no doubt, find these scholarly works a worthy contribution to knowledge in their respective fields.

On behalf of the Editorial Board, I wish to appreciate all our reviewers, internal and external, for their constructive criticisms, comments and suggestions. These go a long way to enrich the quality of the papers published in this Journal. The various contributors who painstakingly addressed the observations and suggestions of the reviewers, thus facilitating the achievement of the purpose of the review process also deserve our commendation.

We also, with a grateful heart, acknowledge the interest our teeming readers have continued to show in the succeeding editions of the journal just as we assure them of our readiness to give them the best always. We equally thank our editorial consultants for their useful advice and comments that have contributed to the continuous improvement of the quality of the journal. Legal practitioners and scholars are hereby informed that contributions to our journal are received on a rolling basis. They should feel free to send in their manuscripts and ensure they comply with the submission guidelines as spelt out in the Call for Papers obtainable from the journal's website (www.kiulj.kiu.ac.ug). All contributions should be addressed to the Editor-in-Chief and forwarded to the email addresses supplied in this edition.

VALENTINE T. MBELI (Ph.D)

Editor-in-Chief.

e-mail:valentine.mbeli@kiu.ac.ug

TABLE OF CONTENTS

OBSERVING CORPORATE GOVERNANCE ETHICAL BEST PRACTICES OF PRIVACY AND DATA PROTECTION IN THE COVID-19 ERA IN NIGERIA

OLARIYIKE D AKINTOYE, Ph.D[*]

Abstract

Most data protection regulations recognize the need for balance between the rights of individuals and the justifiable interference with these rights. The Nigeria Information Technology Development Agency (NITDA) issued the Nigerian Data Protection Regulation (NDPR) to create a regulatory framework that conforms to international standards and good corporate governance practices. This paper attempts to address the question of how well the personal data collected during the pandemic could be safeguarded from breaches. The paper used the doctrinal research methodology with recourse made to the primary and secondary sources of gathering information. It recommends that good corporate governance practices in the area of data and privacy protection should be adopted by public and private institutions. It further suggests that the collection of data should be guided by an extant law, while adopting the principle of necessity, and transparency. The study concludes that in as much as data collection is important to combat the spread of Covid -19, this should be done while respecting ethical best practices.

Keywords: Privacy, Data Protection, Covid-19 Pandemic, Corporate governance, Nigeria.

Introduction

Privacy is a fundamental human right, recognised by Section 37 of the Nigerian 1999 Constitution. It is also recognised in the Universal Declaration of Human Rights, the International Covenant on Civil and Political Rights, and in many other international and regional human rights conventions. The July 2015 appointment of the first UN Special Rapporteur on the Right to Privacy in the Digital Age reflects the rising importance of privacy in global and national digital policy. Privacy is central to our enjoyment of personal dignity and autonomy, it empowers the individual against the state and is necessary for securing other human rights, such as the right to freedom of expression and opinion.[1]

[*] Senior Lecturer, Department of Business and Private Law, Faculty of Law, Kwara State University, Malete, Nigeria. Email: olariyike.akintore@kwasu.edu.ng ; riyikeakintoye@yahoo.com Mobile: +2348055830014

[1]NZ Human Rights, 'A new legal framework for privacy, data and technology, Available on https://www.hrc.co.nz/our-work/privacy-data-and-technology/new-legal-framework-privacy-data-and-technology/ accessed on 30 July, 2020.

Data protection on the other hand, is a legal mechanism that ensures privacy. Privacy and data protection are therefore two interrelated internet governance issues. Data Privacy describes the practices which ensure that the data shared by customers is only used for its intended purpose, and the right of a citizen to have control over how personal information is collected and used.[2]

The processing of personal data in Nigeria falls within the purview of a rapidly developing Privacy Framework strengthened by the coming into force of the Nigerian Data Protection Regulation (NDPR) in 2019.This regulation, which became a Bill[3] has now been abandoned. The Federal government is now planning to engage the services of consultants to draft a new document.[4] The Bill before it was abandoned was seen by many as a modest attempt to raise the Nigerian data protection framework to global standards and was inspired by its European counterpart, the General Data Protection Regulation of May 2018 (GDPR).[5]

In a bid to effectively combat the Covid-19 Pandemic, various governments have resorted to location data analytics, surveillance of its citizens, facial recognition technology and biometrics, thermal cameras and disclosure of health and travel records. Also, a lot of personal information are obtained and processed on the internet at a much higher rate and frequency than the pre-pandemic era. Governments are thus forced to overlook several data privacy concerns in the name of fighting COVID-19.[6]

The questions to be answered are; is the Nigerian government and its agencies adhering to the rules of good corporate governance and best practices as relates to privacy and data protection in the Covid-19 era? How is the personal data collected during the pandemic safeguarded from privacy breaches and what happens to the gathered data after the pandemic is over? This paper is an attempt to contribute to the discourse on good corporate governance practices as it relates to privacy and data Protection in the country.

Keeping User Data Private as a Good Corporate Governance Practice

Protecting user data and sensitive information is a first step to keeping user data private.[7] In 2014, Forbes reported that 46% of organizations suffered damage to

[2]Data Privacy definition, Available on https://www.emotiv.com/glossary/data-privacy/ accessed on July 14, 2020
[3]Nigeria Data Protection Bill, 2020
[4]The Federal Government spent funds in 2020 to gather stakeholders across the country to draft a document it planned to pass to the National Assembly to serve as precursor to legislation protecting the sensitive data of Nigerians. The government has abandoned this document and is now planning to engage a consultant to draft a new document.
[5]Temitayo Ogunmokun, 'Covid-19, Privacy and Data Protection in Nigeria: Matters Arising' available on https://aanoip.org/covid-19-privacy-and-data-protection-in-nigeria-matters-arising/ accessed on 18 July, 2020.
[6]Francis Ololuo, 'Nigeria: COVID-19 Pandemic And The Data Privacy Implications' 08 May 2020 available on https://www.mondaq.com/nigeria/privacy-protection/929530/covid-19-pandemic-and-the-data-privacy-implications
[7]Data Privacy definition, Available on https://www.emotiv.com/glossary/data-privacy/ accessed on July 14, 2020

their reputation and brand value as a result of a privacy breach[8]. Data protection is the process of safeguarding important information from corruption, compromise or loss.[9]Privacy is usually defined as the right of any individual to control his own personal information and to decide whether or not to disclose it to third parties. Nigeria and other jurisdictions realising the benefits of complying with data privacy laws are passing their own data protection regulations like their European counterparts.

Data Protection in the United Kingdom and the United Nations

In the United Kingdom, there is the Data Protection Act of 1998, a revision of the Act of 1984 which stated rules for data users and defined individuals' rights in regard to data that is directly related to them. The Act became effective on March 1, 2000. The law itself strives to balance the individual rights to privacy and the ability of more public organizations to use this data in the process of conducting business. The Act gives guidelines, and principles, which a data controller must observe when handling personal data in the course of doing business. These principles go along the lines of having been obtained fairly, lawfully and transparently.[10]

The United Nations through the United Nations Development Group (UNDG) had established Guidance for the universal operation of data for the purpose of safeguarding its privacy and protection. The Guidance Note on Data Privacy, Ethics and Protection[11] sets out general guidance on data privacy, data protection and data ethics for the UNDG concerning the use of big data, collected in real time by private sector entities as part of their business offerings, and shared with UNDG members for the purposes of strengthening operational implementation of their programmes to support the achievement of the 2030 Agenda.[12]

The right to privacy had previously been largely neglected within the UN human rights monitoring mechanisms, despite being upheld as a fundamental human right in the Universal Declaration of Human Rights and the International Covenant on Civil and Political Rights (ICCPR). [13]While the United Nations (UN) pioneered and recognised the impact of modern technological developments on (data) privacy as far back as 1968, little has so far been achieved in terms of introducing a truly global data privacy framework beyond the ICCPR General Comment No.16: Article 17 (Right to Privacy) in 1988 and the 2010 report of the UN Special Rapporteur on

[8]Forbes Insight, 'Reputational Impact of IT Risk' Available on https://images.forbes.com/forbesinsights/StudyPDFs/IBM_Reputational_IT_Risk_REPORT.pdf accessed July 15, 2020.
[9]Definition of Data Protection, available on https://searchdatabackup.techtarget.com/definition/data-protection accessed July 15, 2020.
[10]www.gov.uk> data-protection, accessed may 26, 2021
[11]*Guidance Note on Data Privacy, Ethics and Protection* https://undg.un.org/resources/data-privacy-ethics-and protection-guidance-note-big-data-acheivements-2030-agenda.accessed July 15, 2020
[12]Global Pulse, 'Data Privacy, Ethics and Protection Principles' available on https://www.unglobalpulse.org/policy/privacy-and-data-protection-principles/ accessed on 30 July, 2020.
[13]http://www.ohchr.org/en/professionalinterest/pages/ccpr.aspx

the promotion and protection of human rights and fundamental freedoms while countering terrorism, the right to privacy was hardly referenced within the UN human rights mechanisms. This lack of attention changed in 2013, due to the Snowden revelations, which created significant political momentum to address the practices of mass surveillance facilitated by modern communications technologies.[14]

Corporate Governance and an Overview of Data Protection laws in Africa

Data protection law has been gaining ground in Africa over the past 20 years. Today, out of 54 countries, 25 have passed data protection laws, the latest countries being Uganda, and Egypt. Other countries, for example Nigeria have introduced data protection bills which are under discussion or waiting to be on the legislative agenda.[15]

African Regional legislative framework

In 2010, the Economic Community of West African States (ECOWAS), adopted a Supplementary Act on Personal Data Protection, followed a year later, by a Supplementary Act on Cybercrime. So far, two thirds of the ECOWAS member states now have in place data protection regulations, except Togo, the Gambia, Guinea Bissau, Sierra Leone and Liberia.[16]

In 2013, the Southern African Development Community (SADC) published a Model Data Protection Act. Since then, only two countries have enacted data protection laws. Counting the five SADC member states which already had privacy laws in place, seven out of 16 member states have a data protection legal framework today.[17]

The African Union in 2014 adopted the Convention on Cyber Security and Personal Data Protection (the Malabo Convention), which is a comprehensive document covering electronic transactions, privacy and cyber security. To date, the Malabo Convention has been signed by 14 states and ratified by five countries out of 55 member states[18] (Western Sahara being part of the African Union).

Need for a harmonised legal framework

Harmonising the data protection statutory and regulatory framework in Africa is still on the agenda of regional organisations and some states. In addition to protecting citizens' privacy, having a harmonised or, at best, a uniform framework is seen as an opportunity to promote the continent's development by allowing free

[14]Privacy International (GB),'United Nations Recognition of Privacy' available on https://privacyinternational.org/impact/united-nations-recognition-privacy accessed on 30 July, 2020.
[15]Lexology, 'Overview of data protection laws in Africa' available on https://www.lexology.com/library/detail.aspx?g=82196d1c-2faa-43c2-983b-be3b0f1747f2 accessed on 30 July, 2020.
[16]Ibid
[17]ibid
[18] Ibid

flow of data within Africa, encouraging data transfers from other continents to Africa and thus boosting the use of African-based data centres, outsourcing services, block chain technology, e-government and fintech services.[19]

Privacy and data protection is still an emerging topic in Africa and more legislation are expected in the near future.[20]On the African continent, ECOWAS appears to be one of the most active regional organisations in the area of cyber security. In 2010, the community adopted the Supplementary Act on Personal Data Protection within ECOWAS. This legally binding Act, seen as being strongly influenced by the EU Data Protection Directive (95/46/EC), specifies the required content of data privacy laws and obligates member states to establish a data protection authority.[21]

In 2015, ECOWAS signed a Memorandum of Understanding with the International Telecommunication Union (ITU) to facilitate the interaction between the two organizations. In 2017, ECOWAS co-organized the regional conference on harmonization of legislation on cybercrime and electronic evidence with the Council of Europe and since 2017 it has supported the Council of Europe-led judicial training for judges and prosecutors of its member states in this field.[22] In 2018, together with other African regional organisations, ECOWAS participated in the First African Forum on Cybercrime organized by the African Union with a focus on cybercrime policies and national legislation, international cooperation, and capacity building. Similarly, ECOWAS has cooperated with the United States on developing its Member States' cyber security strategies.[23]

Comparing African Data Privacy Laws with their European Union Counterpart

Since 2001, 32 of the 55 African countries have enacted data privacy laws. Of great importance is the 2014 adoption of the African Union Convention on Cyber-security and Personal Data Protection ('Malabo Convention'), but it has only yet received a third of the required ratifications.

Of more practical effect have been data privacy agreements and model laws in Regional Economic Communities (RECs). The most mature development as yet, and the earliest, has been from ECOWAS, which has had eleven out of fifteen member enact legislation in compliance with its 2010 Supplementary Act. Africa's only binding data protection agreement yet in force, and was influenced strongly by

[19]Lexology, 'Overview of data protection laws in Africa' available on https://www.lexology.com/library/detail.aspx?g=82196d1c-2faa-43c2-983b-be3b0f1747f2 accessed on 30 July, 2020.
[20]Ibid
[21] CCDCOE, 'Economic Community of West African States' Available on https://ccdcoe.org/organisations/ecowas/ accessed on 30 July, 2020
(Greenleaf, Graham, 'The Influence of European Data Privacy Standards Outside Europe: Implications for Globalisation of Convention 108 (October 19, 2011),'' International Data Privacy Law, Vol.2, Issue 2, 2012; UNSW Law Research Paper No.2011-39; Edinburgh School of Law Research Paper No. 2012/12
[22]http://www.coe.int/en/web/cybercrime/glacyplusactivities accessed,30 July, 2020.
[23]Ibid

the EU Data Protection Directive (DPD) (1995). The three main African instruments, (AU Convention, ECOWAS Act, SADC Model Law) are compared with the European instruments typifying the 'three generations' of development of data privacy laws (Convention 108, 1980; EU DPD, 1995; and EU GDPR, 2016). Conclusions are drawn on the extent to which the three African instruments require, on average, that national laws should include the standards of each of these three generations of international instruments.[24]

Although a continent-wide convention on Cyber Security and Personal Data Protection was adopted by the African Union back in 2014,[25] some of the proposed and existing national laws fall short of comprehensively protecting data and privacy. For instance, Uganda's Data Protection Bill, 2015 and Ghana's Data Protection Act, 2012 lack succinct clauses on key areas such as notification of breach and data portability, and also have limitations on the right to access, among others.[26]

Despite this, mass collection of personal data continues across the continent, leaving the majority of Africans vulnerable to the violation of their data privacy. This contrasting state of affairs formed part of the discussions at a July 2017 convening of lawyers, government officials, civil society representatives, academics, and students at the Institute for Information Law ,University of Amsterdam for a five-day training course on issues pertaining to privacy and data protection law in relation to the internet and electronic communications.[27]

For about seven decades, the European Convention on Human Rights, 1950, has functioned as the framework to guarantee Data protection. The General Data Protection Regulation (GDPR) came into force in the European Union (EU) in May 2016. The 28 EU member states, have until May 2018, to apply the Regulation to existing national laws to ensure the protection of citizens with regard to the processing of personal data and its transfer within the EU and beyond, the right of privacy, for private and family life. More recently, the European Charter of Fundamental Rights, 2020 has reinforced this right. These instruments are the basis of the robust protections provided for under the GDPR.

In Africa similar frameworks which address privacy are less than two decades, such as the Declaration of Principles on Freedom of Expression in Africa (2002) (Part V), the Resolution on the Rights to Freedom of Information and Expression on the Internet of Africa, and the civil society led African Declaration on Internet Rights and Freedoms.[28]

[24]Greenleaf, Graham and Cottier, Bertil, 'Comparing African Data Privacy Laws: International, African and Regional Commitments' (April 22, 2020), available at https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3582478 accessed on 31 July, 2020.

[25]Edrine Wanyama, 'What African Countries Can Learn from European Privacy Laws and Policies, July 27, 2017, available at https://cipesa.org/2017/07/ Accessed on 31 July 2020.

[26]Ibid.

[27]http://www.echr.coe.int/documents/convention_eng.pdf accessed July 14, 2020

[28]http://www.unesco.org/fileadmin/multimedia/hq/ci/ci/pdf/events/netconference_march2015_submissions/reference_from_africaninternetrights_org,pdf

However, whereas European instruments have been largely endorsed and supported by member states, many African instruments still struggle to gain similar recognition by member states. As in the EU, African countries need to uphold the principles laid down in these instruments towards the recognition and enforcement of citizens' right to privacy and data protection.[29]

An Overview of Data Privacy Protection Legislation in Nigeria

There has been no comprehensive legislation that set out to protect the data of Nigerian citizens except for Section 37 of the Constitution,[30] which provides that "...the privacy of citizens, their homes, correspondence, telephone conversations, and telegraphic communications is hereby guaranteed and protected..." Apart from the Constitution, there is the Nigeria Data Protection Regulation (NDPR) 2019 a subsidiary legislation aimed at addressing data privacy and protection in Nigeria. There are also some sector-specific data protection regulations such as;

i. **The Nigeria Consumer Code of Practice Regulations (NCC), 2007**, which deals generally with the protection of consumers' data in the telecommunications sector. It requires all licensees to take reasonable steps to protect the information of their customers against improper or accidental disclosures.[31]

ii**. The NCC Registration of Telephone Subscribers Regulation 2011,** deals with the data privacy and protection of subscribers, it provides for confidentiality of personal information of subscribers stored in the central database or a licensee's database, it also provides that this information shall not be released or transferred outside Nigeria without the prior written consent of the subscriber and commission respectively. This regulation also regards the information stored in the Central Database as the property of the federal government of Nigeria.

iii. **The Freedom of Information Act, 2011,** protects personal data and restricts the disclosure of information which contains personal information by public institutions except where those involved give consent to its disclosure or the information is publicly available. The Act also provides that a public institution may deny the application for disclosure of information that seemed privileged by law e.g. Legal practitioner/Client privilege, Doctor/Patient privilege.[32]

iv. **The Cybercrimes (Prohibition, Prevention. Act 2015** is Nigeria's foremost law on cybercrimes. This Act prohibits, prevents, and punishes cybercrimes in Nigeria and criminalises data privacy breaches. It prescribes that anyone or service provider in possession of any person's personal data

[29]Ibid.
[30]Constitution of the Federal Republic of Nigeria, 1999
[31] Regulation 35 of the Nigeria Consumers' Code of Practice Regulation (NCC) , 2007
[32]Section 14, Freedom of Information Act, 2011.

shall take appropriate measures to safeguard such data.

v. **The Child Rights Act 2003** guarantees the right of every child to privacy, family life, home, correspondence, telephone conversation and telegraphic communications subject to the supervision or control of the parents or guardians.

vi**. Consumer Protection Framework 2016 of the Central Bank of Nigeria (CBN**),[33] prohibits financial institutions from disclosing the personal information of their customers and necessitates the prior written consent of their customers before sharing these data with anyone.

vii. **The National Identity Management Commission (NIMC) Act 2007** requires the approval of the Commission before a corporate body or anyone can have access to data stored in there database. The Act also empowers the NIMC to collect, collate and process data of Nigerian citizens and residents.

viii. **The National Health Act (NHA) 2014** restricts and regulate healthcare personnel from disclosing the personal information of users of health services in their records and also ensures that healthcare providers take the necessary steps to safeguard users' data.

ix. **The Federal Competition and Consumer Protection Act (2019)**, ensures that business secrets of all parties concerned in investigations conducted by it are adequately protected during all stages of the investigation or inquiry.

x. **The National Information Technology Development Agency Act, 2007 (NITDA)** is the primary regulatory authority, responsible for the administration and monitoring of the use of electronic data and other forms of electronic communication transactions in Nigeria.[34]NITDA , issued the Nigeria Data Protection Regulation on 25th January 2019, which sets out to deal comprehensively with the protection of the personal information of Nigerian citizens and anyone resident in Nigeria. An understanding of its contents is therefore crucial to appreciating how far companies can go when handling personal data. The Regulation can also place Nigeria on a higher pedestal on the issue of data protection in Africa.[35]

Under the regulation, personal data can only be processed if at least one of the following good corporate governance practices applies:

- The data subject has given consent without fraud, coercion and undue influence.

[33]Consumer Protection Framework of the Central Bank of Nigeria, 2016 https://www.cbn.gov.ng/out/2016/cfpd/consumer%20protection%20framework%20 (final).pdf. Accessed August 3, 2020

[34]Section 6 of The National Information Technology Development Agency (NITDA) sets out the mandate of the Agency. Yimika Ketiku, 'Data Privacy and Protection in Nigeria'

[35] Chris Brook, 'Breaking Down the Nigeria Data Protection Regulation' (23 April, 2019) available at https://digitalguardian.com/blog/breaking-down-nigeria-data-protection-regulation accessed on 4 August, 2020.

- Processing is necessary for the performance of a contract to which the data subject is party or in order to take steps prior to entering into a contract
- Processing is necessary for compliance with a legal obligation to which the controller is subject
- Processing is necessary in order to protect the vital interests of the data subject
- Processing is necessary for the performance of a task carried out in the public interest or in exercise of official public mandate vested in the controller.
- Any entity involved in data processing or the control of data, needs to develop security measures to protect data, including but not limited to protecting systems from hackers, setting up firewalls, storing data securely with access to specific authorized individuals, employing data encryption technologies, developing organisational policy for handling personal data and other sensitive data, protection of emailing systems and continuous capacity building for staff. Data subjects have the right to object to the processing of personal data that is going to be used for marketing, and should be offered a mechanism to object to any form of data processing.[36]

Data Privacy Breach and Penalty

A data breach can be intentional or accidental. A cybercriminal may hack the database of a company where people have shared their personal information, or an employee at a company may accidentally expose such shared personal information on the Internet. Either way, criminals may access people's key personal details and profit from them at people's expense. Retailers, hospitals, corporations, government offices and colleges have all been targets of data breaches at one time or the other.[37]

The NITDA has resolved no fewer than 790 data protection breaches since the commencement of the implementation of the NDPR in 2019.The feat was achieved in collaboration with the Data Protection Compliance Organisations (DPCOs). NITDA in partnership with DPCOs has issued 230 enforcement and compliance notices aside for routine training of DPCOs.[38]

While hundreds of data breaches have affected consumers around the world, some of the most notable have occurred in just the last few years and involve the exposure of sensitive information, despite cyber security efforts aimed at data protection.

[36] Ibid.

[37]Steve Symanovich, 'What Is a Data Breach and How Can it be Handle?' available at https://www.lifelock.com/learn-data-breaches-data-breaches-need-to-know.html accessed on 31 July, 2020.
[38]Kashifu Inuwa , NITDA Director General made the disclosure during a professional development workshop organized by the agency on August 29, 2020 . Metro News, "NITDA Resolves Over 790 Data Breaches in One Year'' by UnuniChioma .https://thenigerialawyer.com. Accessed on August 25, 2020.

In July 2019, Capital One reported an unauthorized user broke through its security measures and accessed 140,000 U.S. Social Security numbers, 80,000 linked bank account numbers, and approximately one million Canadian Social Insurance Numbers. The breach affected 106 million credit card customers in the U.S. and Canada.

Also, In November 2018, hotel chain Marriott International said it had been hacked through the Starwood guest reservation database, and that the personally identifiable information of about 383 million guests may have been compromised, including names, phone numbers, email addresses, birth dates, and passport numbers.

The Equifax data breach, which impacted more than 145 million American consumers, was disclosed in September 2017. Names, Social Security numbers, birthdates, driver's license numbers, and approximately 200,000 credit card numbers — details that could be used to commit fraud, were exposed in the breach.[39]

Similarly, in 2015, external hackers gained unauthorized access to health care company Anthem and stole a trove of sensitive information impacting roughly 80 million customers. On a global level, Yahoo disclosed two data breaches in 2016, showing how a mountain of personal information can land in the hands of cyber thieves. Combined, the breaches at the online portal affected 1.5 billion user accounts.[40]

The pace of data breaches is increasing on yearly basis with dozens of high-profile cybercrimes reported in recent time. 2019 has been described as a record year for data breaches with the United States of America recording 1,473 incidents, a 17% increase over 2018. Nearly 164 million sensitive records were exposed in those data breaches, a 65 percent increase over 2018 numbers.[41]

Penalty for Data Breach in Nigeria

According to the provision of the Nigeria Data Protection Regulation, any person who is subject to the Regulation,[42] and who is found to be in breach shall be liable to the following:

1. A Data Controller dealing with more than 10,000 Data Subjects, shall be subject to the payment of a fine of 2% of its Annual Gross Revenue of the

[39]Steve Symanovich, 'What Is a Data Breach and How Can it be Handle?' available at https://www.lifelock.com/learn-data-breaches-data-breaches-need-to-know.html accessed on 31 July, 2020.
[40]ibid
[41]The Identity Theft Resource Centre, a San Diego based non-profit organisation
[42]Nigeria Data Protection Regulation 2019

preceding year or payment of the sum of N10,000,000 [ten million Naira], whichever is greater;

2. A Data Controller dealing with less than 10,000 Data Subjects, shall be subject to the payment of the fine of 1% of the Annual Gross Revenue of its preceding year or payment of the sum of N2,000,000 [two million Naira], whichever is greater.[43]

Covid-19 (Coronavirus) and Data Protection

Since the emergence of COVID-19 (Corona Virus)[44] in Asia late 2019, the virus has spread to every continent[45]. The pandemic can be has described as the greatest challenge we have faced since World War II. As of now, some part of the world have experienced the third wave of the Pandemic, with millions succumbing to death through the disease.[46]

The pandemic is much more than a health crisis as it has contributed to an unprecedented socio-economic crisis. The year 2020 has not been as envisaged for many people, the disruption occasioned by the pandemic has adversely affected various aspects of global activities and the data privacy space is not excluded in this unfolding drama crises.[47]The following are some of the weapons deployed by different countries to fight Covid-19;

i. **Surveillance, Modelling and Contact Tracing**

In a bid to effectively track infected persons and curb the spread of Covid -19 ,various governments have resorted to location data analytics, contact tracing, surveillance of its citizens, facial recognition technology and biometrics, thermal cameras and disclosure of health and travel records.[48] A lot of countries now employ real-time phone location data, credit-card transaction records, mobile apps, and CCTV footage to track the movements of virus carriers and persons they may have encountered. South Korea, China, Hong-Kong, Israel and Taiwan are

[43]Yimika Ketiku, Ibidolapo Bolu, 'Nigeria: Data Protection Regulation 2019 – The New Law' (19 December 2019) available at https://www.mondaq.com/nigeria/privacy-protection/876858/data-protection-regulation-2019-the-new-law accessed on 1 August, 2020. Global Legal Group Limited (GB), 'Nigeria Data Protections Laws and Regulations 2020' available at https://iclg.com/practice-areas/data-protection-laws-and-regulations/nigeria accessed on 4 August, 2020.

[44]COVID-19 is a disease caused by a new strain of coronavirus. 'CO' stands for corona, 'VI' for virus, and 'D' for disease. Formerly, this disease was referred to as '2019 novel coronavirus' or '2019-nCoV

[45]In December 2021, Antarctica one of the most remote places on earth lost its status as the last continent free of Covid-19 when 36 people at Chilean Bernardo O' Higgins Research Station tested positive.

[46] World total cases as at August 30, 2021; 218,438,933 and 4,531,745 deaths. Google search. Assessed 1 Sept, 2021.

[47] United Nations Development Programme, 'COVID-19 Pandemic, Humanity needs leadership and solidarity to defeat coronavirus' available on https://www.undp.org/content/undp/en/home/coronavirus.html accessed July 15, 2020.

[48]Bryan Walsh, 'The Pandemic's Coming Health Surveillance State' (21st March 2020) available on https://www.axios.com/coronavirus-brings-a-future-of-health-surveillance-82c7788b-ba30-4f4b-a5fb-a863273b3b88.html> accessed on 16th July, 2020.

employing these measures[49]. Hong Kong and China have employed drones to monitor excessive social interaction. In addition to the above, the world is working remotely and virtually on the internet. The pandemic has seen a spike in the use of several apps for video conferencing like Zoom[50] and entertainment apps, like TikTok and Triller[51]. Lately, more western countries have joined the move to use surveillance as a weapon to combat the rapid spread of Covid -19. For example, France recently passed a law empowering the government to control the movement of its residents, while the United Kingdom and the United States of America are using geo-location data from the mobile app industry to track the movement of their citizens. Furthermore, in many countries, network operators are sharing customer data with health authorities. Nigeria, in her fight against the virus has also towed this path.[52]

When an organisation's policy is unclear, IT needs to ensure that employees are not left to make their own decisions about software and security without the right support and guidance. Employees need clarity from their employers on how to work in their home office environment.[53] For example, people working in the legal profession in Ireland have been told not to conduct work-related calls when they are near certain AI technology devices for fear of privacy and data breaches as a result of devices recording information.[54]

Similarly, monitoring productivity levels throughout the day, potentially encroaches on employee privacy and there is a new concern that mobile phone companies are tracking individuals' locations and using the information to track infected patients and their contacts.[55] The concern for others is that major changes to legislation and tracking could end up eroding individual rights in the long term.[56]

[49]Venture Africa, 'Smartphones, Surveillance and the Fight against COVID-19 Pandemic' available on http://venturesafrica.com/smartphones-surveillance-and-the-fight-against-covid-19-pandemic/ accessed on 16 Jul, 2020

[50]Eric S. Yuan, 'A Message to Our User' (1st April 2020) available on https://blog.zoom.us/a-message-to-our-users/ accessed on 16th July, 2020.

[51]2020 has seen the number of tiktok users grow from 37 million users to over 45 million (13th March, 2020), available on https://www.emarketer.com/content/tiktok-to-surpass-50-million-users-in-us-by-2021 accessed on 16 July, 2020.

[52]TomiwaOnaleye, 'How FG Could Breach Privacy Laws in a Bid to Curb the Spread of Coronavirus Using Phone Data' (18th March 2020) available on https://technext.ng/2020/03/18/how-fg-could-breach-privacy-laws-in-a-bid-to-curb-the-spread-of-coronavirus-using-phone-data/ accessed on 16 July, 2020.

[53]Pragasen Morgan and Paul Smith, 'Four risks to data privacy and governance amid Covid-19' available at https://www.computerweekly.com/opinion/Four-risks-to-data-privacy-and-governance-amid-Covid-19 accessed on 31 July, 2020.

[54]http://searchunifiedcommunications.techtarget.com/news/252468109/aws-microsoft-listening-to-voice-recording-raises-privacy-concerns

[55] https://searchunifiedcommunicationstechtarget.com/news/252468109/aws-microsoft-listening-to-voice-recordings-raises-privacy-concerns.

[56]Pragasen Morgan and Paul Smith, 'Four risks to data privacy and governance amid Covid-19' available at https://www.computerweekly.com/opinion/Four-risks-to-data-privacy-and-governance-amid-Covid-19 accessed on 31 July, 2020.

Other government and private entities' response to the epidemic include the development and deployment of technological solutions focusing on; **documentation,** that is, using technology to say where people are, where they have been or what their disease status is; secondly, **modelling**, that is, gathering data which help explain how the disease spreads and; thirdly, **contact tracing**, which involves identifying people who have had contact with others known to be infected.

The above solutions rely on 'sensitive personal data' such as biometric data, genomic data, location data, and health data – using technical means. Telecommunication companies are also reported to be involved in providing government with archived, "anonymised", and retained location data of customers. In some parts of the world, they are deploying facial recognition, anti-terror methods, symptom tracking, and other measures in the fight against the virus.[57]

The Principles of Necessity and Proportionality of Data processing and COVID-19

The purpose of data protection is to protect people's personal data against abuse. The extant laws allow the use of personal data for public health while adopting the principle of necessity and proportionality. Balancing epidemic response and respect for human rights are vital to the fight against the virus. This is in response to *Cliff Richard v The British Broadcasting Corporation***.**[58]In this case, it was decided that epidemic response should not result in or bring about complete erosion of fundamental right protections and that both private and public driven initiatives should conform to the principles of data protection.

Regulation of Data in the Health Sector in Nigeria versus Public Interest

The National Health Act (NHA) 2014 and the Nigeria Data Protection Regulation (NDPR) 2019, regulate data protection in the health care sector. The NDPR allows the further processing of data for scientific research for public interest. The NHA however states that such data should be de-identified. Similarly, the National Information Technology Development Agency (NITDA) recently declared that the collection of data can be done on the basis of public and vital interest, and such collection should conform to the Nigerian data protection framework.[59]In addition, the Nigerian President relying on the Quarantine Act, signed the COVID-19 Regulation 2020 enabling the government to impose lockdown in the country and to take some other emergency measures.

[57]NurudenOdeshina, 'COVID-19 and Data Protection in Nigeria' (4 April, 2020) available on https://aanoip.org/covid-19-and-data-protection-in-nigeria/ accessed on 16 July 2020
[58] (2018) EWHC 1837 (Ch.)
[59]http://itedgenews.ng/2020/03/30/covid-19- data-collection-complies-with-ndpc-says-nitda

Even though the right to privacy is guaranteed under the Nigerian Constitution[60], the imposition of lockdown to curtail the spread of the virus relaxes the right to movement and association, and is justified under public interest. Similarly, the right to personal liberty is impacted and will be waived in the event of "… persons suffering from infectious or contagious disease, for the purpose of their care or treatment or the protection of the community." However, the constitution is clear that such derogation or waiver of rights will only be possible where it is "reasonably justifiable in a democratic society." As such, most data protection regulations recognize the need for balance between the rights of individuals, their personal data and the justifiable interference with these rights.[61]

Conclusion

In conclusion, while government and organisations can process the data of citizens, without their consent, under the safety net of public interest, this should be done while respecting ethical best practices and complying with data privacy laws. Also, the use of such data should be on the basis of **necessity and proportionality** – **necessity** implies the least intrusive option and that the processing must be a targeted and proportionate way of defeating the pandemic.

Recommendations

- Governments and data privacy regulatory agencies should formulate guidelines for the collection, processing, use and disclosure of personal information in the Covid-19 era. They should also ensure strict compliance with such guidelines. The data collected should be properly safeguarded to avoid a breach of the extant laws.
- Data collected and processed should be the requisite ones to combat COVID-19 and should be disclosed solely to persons directly involved in the fight, and should be erased as soon as it is no longer needed.
- It is also recommended that collection and use of health data, should not be the end, but the data and information collected should be carefully analysed and used to address the pandemic. This is because it is not the data or information gathered that will cure Corona Virus but the interpretations of the gathered facts, will aid more scientific findings and development.
- Health records should be kept for a specific period or temporarily, mainly to fight the epidemic. Accountability entails that measures implemented to manage the emergency and decision-making process should be documented, and controllers should be transparent about these processes.[62]

[60]Section 37 Nigeria 1999 Constitution
[61] Section 45(1)-(3) Nigeria 1999 Constitution
[62]NurudenOdeshina, 'COVID-19 and Data Protection in Nigeria' (4 April, 2020) available on https://aanoip.org/covid-19-and-data-protection-in-nigeria/ accessed on 16 July 2020

ISSN: 2519-9501