Examining the Legal Framework for Data Protection in Nigeria viz a viz the Exercise of Human Rights on the Internet

Nkemnechem S. Danjuma*

Abstract

The importance of data privacy and protection has grown recently, mostly because data has transformed into a valuable resource for the entire world community in the internet era. The widespread breaches of sensitive data on a daily basis are of rising concern, particularly in light of human rights, including the right to privacy and the freedom of speech. Despite incessant data breaches, many developing countries are yet to give full attention to the protection of the personal data of internet users. At this time when personal data is an asset to industrial and political giants, strong data protection measures are more important than ever to further actualize the exercise of rights to privacy and freedom of expression. In Nigeria, some institutional and legislative efforts have helped the country move from the absence of a specific legal framework for data protection to having its Nigeria Data Protection Regulation 2019 (NDPR) and Data Protection Act 2023. This paper examines Nigerian data protection laws in relation to online protection for human rights. To achieve this, eady-existing legislation, published papers, books, and journals were reviewed. The research finds that issues like a lack of enforcement efforts, a lack of understanding of privacy rights, and a dearth of practising specialists are some of the issues impeding the effectiveness of data protection laws on human rights protection. The research recommends that enforcement efforts be strengthened and that the general public in Nigeria be made more aware of their right to privacy and the available legal protection.

Keywords: Data Protection, Data Privacy, Human Rights, Right to Privacy and Freedom of Expression

1. Introduction

Privacy forms one of the essential barrier preventing absolute state control and dominance. According to Olomojobi, the

* LLM (in view), LLB and Bsc, Business Administration, Block SA9 Flat2, 1 Dunukofia Street, Off Toro Street Off Ahmadu Bello way, Area 11, Garki Abuja, Mobile phone: 08035707495, Email: nsdanjuma@gmail.com

constitutional right to privacy places a check on the government's authority.[1] However, the right to privacy, according to Abdulrauf and Daibu, is gravely challenged in Nigeria today by emerging technologies, sometimes known as destroying technologies.[2] Recent technical developments allow people to complete activities that were previously impossible resulting in new problems. The massive violation of people's right to privacy on the internet is one such issue. The issue of safeguarding data spans the globe and raises concerns among diverse stakeholders. It remains persistently under siege from governments and corporate bodies that gather and wield personal information of internet users with little regard for individual rights. The widespread expansion of personal data has its merits, yet it opens individuals to specific vulnerabilities, such as heightened transparency and susceptibility to various transgressions by both state, corporate actors or even perpetrators of criminal activiities. Instances include the misuse of people's data for purposes beyond their original intent, as well as the exposure to risks stemming from insufficient security measures for lawfully collected information.[3] This unchecked handling of personal data might further amplify the asymmetry in information and influence between citizens and these entities, be they governmental or corporate. The increased need for personal data in the globalised and digital era has given rise to all of these problems.[4] The legislation on data protection, such as the new Data Protection Act 2023, specifies basic standards governing the gathering, use, and disclosure of individuals' personal data in order to safeguard their human rights including rights to privacy and freedom of speech. The goal of these legislation is to ensure that personal data is used appropriately rather than to outright forbid its processing, which may be virtually unachievable in today's globalised society, especially considering the ubiquitious nature of the internet. As long as it is done in a way that respects people's rights, personal data can

---

1 Olomojobi, Yinka. "Right to Privacy in Nigeria." (2017) https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3062603 Accessed July 30, 2023.

2 Abdulrauf LA, Daibu AA. New technologies and the right to privacy in Nigeria: Evaluating the tension between traditional and modern conceptions. Nnamdi Azikiwe University Journal of International Law and Jurisprudence. 2016 May 27;7:113-24.

3 Abdulrauf, L.A. and Fombad, C.M. ` Personal data protection in Nigeria: Reflections on opportunities, options and challenges to legal reforms' (2017) Liverpool Law Review, 38, pp.105-134.

4 Ibid.

be gathered and used.[5] In this situation, personal data may be freely used for a variety of reasons as long as the individual subject of the data has considerable control over its collection and use. Therefore, data privacy laws fundamentally shield people from being victims of data misuse which has significant impact on the actualization of their human rights.[6]

Notwithstanding the impressive developments in the legal framework, there have been increase in the level of data breaches in Nigeria. For instance, based on a study from the cybersecurity firm Surfshark, Nigeria records an astounding 82,000 data breaches in Q1 2023, a 64% rise from the previous quarter. In the first three months of 2023 (January through March), Nigeria reported 82,000 data breaches.[7] In this context, a data breach occurs when private, protected, or sensitive information is copied, communicated, viewed, taken, altered, or used by someone who has no right to do so.[8] The most common means of data breach over the internet includes hacking, malware, phishing and human error[9]. Even while legaislative attempts are admirable, numerous individuals are still vulnerable to hazards including exploitation and misuse of their personal information as a result of challenges such as low level of awareness of these frameworks or poor enforcement capacities of the relevant institutions.[10] These and other factors support the necessity for a discussion of data protection. In light of this, this article examines Nigeria's data protection laws and the challenges hindering them from efficiently protecting human rights of internet users.

2. Conceptualization of Terms

Data: Data is characterized as details, notably facts or numerical values, amassed with the intention of being scrutinized, contemplated, and ultimately leveraged to facilitate the process of

---

5 Michael K, Kobran S, Abbas R, Hamdoun S. Privacy, data rights and cybersecurity: Technology for good in the achievement of sustainable development goals. In2019 IEEE International Symposium on Technology and Society (ISTAS) 2019 Nov 15 (pp. 1-13). IEEE.

6 Abdulrauf, L.A. and Fombad, C.M. (n 3).

7 Omoruyi, O. (2023, May 23). Nigeria sees 64% increase in data breaches, with 82,000 episodes in Q1 2023. Technext. https://technext24.com/2023/05/23/nigeria-records-82000-data-breach-in-q1/

8 Ibid.

9 Ibid.

10 Abdulrauf, L.A. and Fombad, C.M. (n 3).

making informed choices[11]The term "data" refers to information, particularly facts or statistics, that has been gathered for analysis, consideration, and application in support of decision-making, as well as information in an electronic format that can be processed by a computer.[12] Hence, data encompasses a wide spectrum of particulars encompassing nomenclature, chronological age, gender, residential domicile, precise banking particulars, comprehensive medical histories, stature, family, contact number, electronic mail addresses, and other information.[13]

Data Subject: the DPA simply defines data subject as 'an individual to whom personal data relates.[14]A Data Subject is the identifiable person who is identified directly or indirectly with reference to an identification number or other factors specific to his/her physical, physiological, mental, economic, cultural or social identity.[15] This definition can easily be couched to mean a natural person with whom certain personal data is identified or identifiable.[16]

Personal Data: Under the DPA, any information relating to a person who can be identified or is identifiable, either directly or indirectly, by reference to an identifier like a name, an identification number, location information, an online identifier, or one or more factors particular to that person's physical, physiological, genetic, psychological, cultural, social, or economic identity is considered personal data.[17]

Data Privacy and Protection: The phrases "data privacy" and "data protection" are occasionally used interchangeably. There are some distinctions despite the fact there are certain shared characteristics. Data security has a branch known as data privacy or information privacy that deals with how to handle data permission, notification,

---

11 Peters P. The Cambridge dictionary of English grammar. Cambridge University Press; 2013.
12 Olawunmi, I. and Emejuo, C.C., 'An Examination of the Legal Framework for Data Privacy and Protection in Nigeria' (2021) University of Illinois College of Law Legal Studies Research Paper, (22-21).
13 Ibid.
14 Section 65 DPA.
15 Section 1.3 of the National Information Technology Development Agency NITDA Data Protection Regulation.
16 Law Insider Dictionary 'Data Subject' Available from https://www.lawinsider.com/dictionary/data-subjects Accessed on 07/17/2020
17 Section 65, DPA 2023.

and legal requirements.[18] To put it another way, the right of a person to be free from unauthorised observation might be referred to as data privacy. On the other hand, data protection means making an effort to safeguard or guard personal data or information against misuse, corruption, breach, or loss. Due to the rapid creation and archival of data, data protection becomes crucial.

Rights to Privacy and Freedom of Expression: The rights to privacy and freedom of expression are fundamental human rights protected by sections 39 and 37 the Nigerian constitution, respectively. The right to privacy encompasses the notion that individuals are entitled to a sphere of self-governing development, social interaction, and autonomy, a "personal realm" that exists whether in isolation or in collaboration with others.[19] This realm should remain shielded from arbitrary state intervention and unwarranted interference from external parties. Activities that curtail the right to privacy, such as surveillance and censorship, can only be deemed justified when they are established by lawful means, essential for attaining legitimate objectives, and commensurate with the goals pursued.[20]

Freedom of expression refer to the act of seeking, receiving, and disseminating information or ideas, regardless of the medium employed.[21]Fundamental human rights are the rights and freedoms that every individual has by virtue of their humanity, including the right to life, the dignity of the human person, the right to a fair trial, the freedom of thought, conscience, and religion, personal liberty.[22] Depriving someone of their human rights would be a serious insult to their sense of justice since they are natural, logical, inviolable, and unchangeable.[23]

---

18 Olawunmi, I. and Emejuo, C.C (n 12)

19 Paradigm Initiative 'The Right to Privacy in the Federal Republic of Nigeria' (2018) Stakeholders Report Universal Periodic Review <https://privacyinternational.org/sites/default/files/2018-05/UPR_The%20Right%20to%20Privacy_Nigeria.pdf> accessed August 2, 2023.

20 Ibid.

21 Williams-Ilemobola O and Abimbola Oladipo, 'An Examination of the Right to Freedom of Expression in Nigeria' Journal of Human Rights Law and Practice. (2018) 1(2) 1-9.

22 Kokpan, Bariyima Sylvester and Nsaa Nuka Anson. "Fundamental Human Rights in Nigeria: Practice, Abuse and Remedy." Social Science Research Network (2021)<https://doi.org/10.2139/SSRN.3831366?sid=semanticscholar> accessed December 20, 2022

23 Onwuazombe, I. I. Human rights abuse and violations in Nigeria: A case study of the oil-producing communities in the Niger Delta region. Annual Survey of International & Comparative Law, (201)7 22(1), 115-160

3. Legal Framework for Data Privacy and Protection in Nigeria

There are several statutory and subsidiary legislation that directly or indirectly regulate data privacy and protection in Nigeria.

a. ***The Constitution of the Federal Republic of Nigeria 1999:*** Section 37 of the Constitution safeguards citizens' privacy encompassing their residences, communications, and telephone discussions. In the case of *Ibironke v. MTN*,[24] the Court reaffirmed the constitutional guarantee of citizens' privacy, implying that data protection is an extension of this safeguarded right.

b. ***Data Protection Act 2023:*** In June 2023, Nigeria's President signed the Data Protection Bill, officially enacting the Data Protection Act, 2023 (the Act), which represents a significant step in the nation's prolonged journey toward a comprehensive data protection framework. The Act, commenced upon presidential signature, introduces key principles common in global data protection frameworks and contains distinctive elements which are discussed later in this paper.

c. ***Nigeria Data Protection Regulation (NDPR) 2019:*** This is the primary regulation in Nigeria that was dedicated to addressing data privacy and protection before the DPA 2023. Enacted by the National Information Technology Development Agency (NITDA) pursuant to powers vested in it by section 6 of the NITDA Act, 2007, the NDPR 2019 replaced the Data Protection Guidelines, 2013. The NDPR not only delineates the rights of a data subject (such as the right to complain, right to be forgotten, right to be informed etc) but also introduces the concept of a 'data controller' who holds sway over the processing of personal data, subject to certain checks. The regulation only covered natural persons and excluded non-personal data.[25]The NDPR creates the position of a data protection officer, designated by the data controller to be responsible for the implementation of the regulation.

---

[24] (2019) LPELR-47483(CA).

[25] Nigerian Data Protection Regulation Section 1.3.

c. ***The Freedom of Information Act, 2011:*** This Act serves to enhance public access to government-held information, superseding the colonial-era Official Secrets Act of 1911. However, the Act limits public institutions from divulging personal information without the concerned individual's consent,[26] and it permits such institutions to reject disclosure requests related to privileged communication.

d. ***The Cyber Crimes (Prohibition, Prevention, etc.) Act, 2015.*** This Act takes a proactive stance against data abuse, fraud, and identity theft.[27] It obliges service providers to store subscriber information for two years and sanctions its release only under specified conditions, including court orders. Additionally, the Act outlaws unauthorized electronic communication interception for criminal investigation without a court order.

e. ***Other legislation:*** There are other laws or subsidiary legislation that directly or indirectly relates to data privacy and protection. The Nigeria Communications Commission (NCC) Consumer Code of Practice Regulations 2007 mandates telecommunication operators to protect customers' data securely. Subsequently, the NCC developed the Registration of Telephone Subscribers Regulations, 2011 which grants data update rights and necessitates data protection for telephone subscribers.[28]

In the health sector, the National Health Act, 2014 safeguards patients' health data and outlines grounds for disclosure.[29] The National Assembly also enacted the HIV/AIDS (Anti-Discrimination) Act in 2014 to protect data of individuals with the disease.

Financial institutions are required under the 2019 Central Bank of Nigeria customer Protection Regulations to maintain customer protection and data privacy. They are also required by the Central Bank of Nigeria's 2016 Consumer Protection Framework to safeguard consumer data against unauthorised access and

---

26 Freedom of Information Act No.4 of 2011. Section 14
27 The Cyber Crimes (Prohibition, Prevention, etc.) Act, 2015. Section 22.
28 Olawunmi, I. and Emejuo, C.C (n 12)
29 National Health Act, 2014. Sections 26 & 29

disclosure.[30] The Credit Reporting Act, 2017 ensures privacy of credit information while the Federal Competition and Consumer Protection Act enacted in 2018 safeguards business secrets during investigations and enables non-disclosure orders. Also, the Finance Act, 2020 amends the Federal Inland Revenue Service Act by providing for taxpayer data confidentiality. Another subsidiary regulation is the Securities and Exchange Commission Regulations on Crowdfunding, 2020 which provides for data privacy provisions for crowdfunding portals.[31]

There is also a National Identity Database, containing the data of registerable persons, which was established by the National Identity Management Commission Act of 2007. Additionally, the Act prohibits the dissemination of registration information without consent unless there are certain circumstances specified in the Act.[32]

4. Key Provisions of the new Data Protection Act 2023

The new DPA provides a legal framework for safeguarding personal information and implementing data protection in Nigeria. Section 2 of the Act provides that data controllers or data processors resident in, operating in or processing personal data in Nigeria are bound by the provisions of the Act. However, data processing carried out by competent authorities for the purposes of prevention or detection of crime, control of national public heath emergency, national security, exercise of legal claims and publication in the public interest for journalism, educational, artistic and literary purposes are exempt from the applicability of the Act.

The Data Protection Commission: The Act establishes the Nigeria Data Protection Commission and the appointment of a governing council[33]. The Commission replaces the Nigeria Data Protection Bureau (NDPB) which was the previous body established in 2022 to achieve the objectives of the NDPR. The Commission, headed by a National Commissioner, is saddled with the responsibility of overseeing the safe practices of data protection in Nigeria which

---

30 Central Bank of Nigeria Consumer Protection Framework 2016, Sections 2.6 & 3 (1)(e)
31 Rule 12 SEC Regulations on Crowdfunding, 2020..
32 National Identity Management Commission Act, 2007. Section 14 and 26
33 Data Protection Act 2023. Section 4.

includes fostering the development of data protection technologies, promoting public awareness of data protection, accrediting data protection compliance services, registering data controllers and data processors of major importance, receiving complaints of violations etc[34]

Processing Personal Data: Under section 24, certain principles are stipulated as necessary considerations to be applied in data processing in Nigeria. A data controller or data processor shall ensure that personal data is processed in a fair, lawful and transparent manner. Personal data must be collected for specified, explicit, and legitimate purposes, and should also be processed in a way that is adequate, relevant, and limited to the minimum necessary for the purposes for which the personal data was collected or further processed. The data must also be secured and protected against unauthorised or unlawful processing, access, loss, destruction, damage, or any form of data breach.[35]

Rights of a Data Subject: Section 4 of the Act confers data subjects with rights, encompassing being informed, accessing, correcting, and objecting to their personal data's processing, with exceptions under section 3 including where such data proceessing carried out by a competent authority as is necessary for national security.

Data Controllers and Processors: According to Section 5 of the Act, a novel classification "data controllers and data processors of major importance" is introduced, necessitating registration, expert Data Protection Officers, and adherence to data protection laws.

Data Breaches: Section 6 of the Act obliges notifying the Commission within 72 hours of breaches, offering a comprehensive breach management procedure, and mandating the retention of breach records.

---

34 Ibid. Section 5.
35 Ibid. Section 24(1)(f).

Cross-Border Data Transfers: As per the provisions of the Act, the transmission of personal information from Nigeria to another nation is permissible solely when the recipient of said personal data is governed by a statute, enforceable corporate regulations, contractual stipulations, ethical guidelines, or accreditation systems that provide a satisfactory degree of safeguarding concerning the personal data.[36]

Third party processing agreement, Indirect Notification of Data and Digital Age of Consent for Children: The Act strengthens the need for a data processing agreement between data controller and third parties processing data under the NDPR Implementation Framework, maintaining the existing requirement. Enhancing transparency and data subject protection, the DPA the right introduced in Article 3.1(7) of the NDPR.[37] When collecting personal data indirectly from the data subject, a data controller must fulfill obligations similar to the original controller. Addressing the digital age of consent for children elaborately, the Act incorporates the European Union's digital age of consent for children aged 13 and above. Additionally, provisions are made for individuals lacking legal capacity to provide consent.[38]

Compliance, Infringements, Penalties and Dispute Resolution: Data controllers and processors must adhere to the Act's provisions, regulations, guidelines, and related subsidiary legislation, with violations leading to appropriate orders from the Commission if it finds breaches or potential breaches. The Commission can issue compliance orders in specific cases of Act violations, direct cessation of unlawful acts, and impose sanctions.[39] Failure to comply with Commission orders constitutes an offense; major controllers/processors may face fines up to ten million naira or 2% of annual revenue, while others might incur fines up to two million naira or 2% of revenue. Courts can also order forfeiture as per the

---

36 Ibid. Sections 41 - 43.
37 Ibid. section 27 (2)
38 Ibid. Section 31.
39 Ibid. Section 46-53.

Proceeds of Crime Act. Injuries from Act violations can lead to civil damages, and companies/officers may be culpable for offences.[40]

5. The Need for Data Protection and Its Nexus with Rights to Privacy and Freedom of Expression on the Internet

Privacy and freedom of expression are now intricately connected, where a breach of one can trigger consequences for the other. This holds especially true in the realm of communication surveillance.[41] Personal conversations, intimate sentiments, connections, reading preferences, and even media consumption habits are highly sensitive and private aspects of an individual's life. These elements have traditionally been regarded as personal matters, not to be accessed or intruded upon without consent or compelling rationale.[42] Innovative technologies have expanded communication possibilities, safeguarding free expression, fostering anonymity, and promoting cross-cultural discussions. Simultaneously, evolving technologies have opened doors for state surveillance, breaching private communications.[43] In Nigeria, fro instance, according to a Premium Times investigation, at least four (4) Nigerian governors—both former and current—have engaged in unlawful surveillance and hacking operations, which entails breaking into target computers and phones to listen in on citizens' private and sensitive communications.[44] The National Security Adviser's office and some of the governments under investigation were cited in the report, which claimed that illegal call interceptions and computer and phone hacking provided these public servants with backdoor access to many people's private lives at the expense of the taxpayers they were sworn to serve.[45]

State-monitored "back doors" in mobile networks, mass interception systems, and voice recognition tech have led to nationwide surveillance. For instance, in remote areas of Ethiopia, where phone

---

40 Ibid.

41 Carly N, 'Two sides of the same coin – the right to privacy and freedom of expression'(2013) Privacy International <https://privacyinternational.org/blog/1111/two-sides-same-coin-right-privacy-and-freedom-expression> accessed August 3, 2023.

42 Ibid.

43 Coccoli J. The challenges of new technologies in the implementation of human rights: An analysis of some critical issues in the digital era. Peace human rights governance. 2017 Jul;1(Peace Human Rights Governance 1/2):223-50.

44 Ogala E, "Investigation: How Governors Dickson, Okowa spend billions on high tech spying on opponents, others," Premium Times, June 9, 2016, <https://www.premiumtimesng.com/investigationspecial-reports/204987-investigation-governors-dickson-okowa-spend-billions-high-tech-spying-opponents-others.html> accessed June 1, 2023.

45 Ibid.

coverage and Internet connectivity are scarce, the government's influence is upheld through widespread networks of informants and a grassroots surveillance framework.[46] This rural tradition has led everyday Ethiopians to perceive mobile phones and other emerging communication technologies as additional means of monitoring their activities. Tools like social media monitoring, deep packet inspection, and trojans are used to track individual online activities. Internet data amassed by companies are accessible to governments, which now mandate data retention.[47]The scope of surveillance has expanded significantly over time. While once focused on private telephone conversations, today's technology has transformed how citizens express themselves, encompassing private dialogues, group discussions, publications, records, and cultural artifacts. These avenues, easily accessible due to modern technology, carry the risk of intrusion by powerful corporate or state entities. When even the most intimate aspects of one's life face potential intrusion, the true freedom of expression is compromised.[48]

Fear of interception of people's words, and relationships can stifle genuine self-expression. Internet content restrictions can impede the flow of information and knowledge, while online identity requirements can lead to social exclusion, undermining expressive rights and deepening inequalities.[49] Such encroachments deter open communication, causing individuals to self-censor and limiting their willingness to engage. Unchecked access to individuals' information undermines the right to seek and receive information. The privacy of reading choices, once assured in physical spaces, becomes uncertain in the digital realm where states can access or manipulate reading materials, websites, and media consumption. Privacy and free expression violations also affect the right to association and assembly, as surveillance undermines confidential relationships and stifles the organization's ability to form. Certain groups, especially citizens relying on privacy to protect sources, are vulnerable to

---

46 Wong, C. M. "They know everything we do." (2023) Human Rights Watch. <https://www.hrw.org/report/2014/03/25/they-know-everything-we-do/telecom-and-internet-surveillance-ethiopia> accessed August 12, 2023.

47 Carly N (n 41).

48 Ibid.

49 Ohemeng FL, Ofosu-Adarkwa K. Overcoming the digital divide in developing countries: An examination of Ghana's strategies to promote universal access to information communication technologies (ICTs). Journal of Developing Societies. 2014 Sep;30(3):297-322.

these violations.[50] Source protection is crucial for freedom of expression, but pervasive surveillance without proper oversight jeopardizes this safeguard. Even limited, non-transparent surveillance can have a chilling effect on freedom of expression without public documentation and safeguards to prevent misuse.[51]

Because of their reliance on online communications and smartphone devices, citizens are also particularly susceptible to being targets of communications monitoring or in some cases are even bombarded with unsolicited contents. This is especially true when citizens are looking into matters of politics or religion. In the case of *Emerging Markets Telecommunication Services v. Eneye*, the Court of Appeal ruled that the appellant's continuous sending of unsolicited text messages to the respondent amounted to a violation of the respondent's constitutional privacy rights.[52] A few other countires where it is commonly known that human rights advocates have been monitored are Colombia, Bahrain, and Algeria.[53] Human rights advocates and political activists claim that in these nations, their each telephone conversation, electronic mail, and activity is tracked. In light of this, it becomes ncessary that individuals can enjoy adequate data protection under the law that avails them the opportunity to contest violations of these human rights.

6. Issues Affecting the Legal and Institutional Framework for Data Protection on the Internet

a. ***Shortage of Competent Professional in the Country:*** The emergence of new roles under novel legislation, such as the DPA and the NDPR, pose one of the major challenges facing data privacy and compliance in Nigeria.[54] Such role is the data protection officers (DPOs). Of course, this calls for the expert knowledge and certain skill sets, but many Nigerians and people in many other third-world countries are not unfamiliar with this role, in contrast to many western countries[55].

---

50 Carly N (n 41).
51 Ibid.
52 6 (2018) LPELR-46193 (CA) at 25- 29 para c.
53 Carly N (n 41).
54 Chika DM, Tochukwu ES. 'An analysis of data protection and compliance in Nigeria.' Int. J. Res. Innov. Soc. Sci. 2020;4(5):377-82.
55 Ibid.

b. ***Weak Enforcement:*** Many social analysts and scholars have expressed concerns about the government's ability to comply with the provisions of the data protection regulation, in part because many agencies and parastatals were known to break the law, in addition to the inadequacy that characterised the country's data privacy legislation. Other regulations, such as section 4.1(2) of the NDPR, which demands that every data controller appoint a data protection officer, are also urgently and consistently need to be followed. Sadly, however, none of these requirements are fulfilled and the regulator continues to do little to enforce them. A recent instance, cited by Chika and Tochuckwu that vividly illustrates this lax approach is the Nigeria Immigration Service's breach of the NDPR[56]. This breach materialized through the unauthorized publication of the international passport data page belonging to a Nigerian resident in the UK on the Immigration Service's social media platforms. Notably, no punitive actions seem to have been applied to the Immigration Service under the NDPR framework despite this clear violation.[57] This case involving the Data Subject's personal information raises pertinent questions about the efficacy of the regulatory measures in place.[58]

c. Consent needed for Data Collection: Unfortunately, both public and private organisations in Nigeria frequently disregarded the requirement of consent before collected of data, causing countless people and even business entities to suffer difficulties.[59] Consent indicates that informed consent must be sought before any personal data is collected. This is especially true when the goal of the data collection is clearly stated and further consent is required for sharing personal information with other parties.[60]However, in Nigeria, there are several occasions where businesses and organisations with which data subjects are likely to have never consciously interacted are

---

56 Ibid.
57 Olumide B (2020) Data Protection and Privacy Challenges in Nigeria (Legal Issues) https://www.mondaq.com/nigeria/dataprotection/901494/data-protection-and-privacy-challenges-innigeria-legal-issues-
58 Chika DM, Tochukwu ES (n 56).
59 Ibid.
60 (European Data Protection Board, 2016).

generating and capturing data and information about them without their awareness.[61]

d. Apathy and Low Level of Awareness: The majority of data subjects are uninformed of their data property rights and Data administrators and collectors are unaware of their responsibility to preserve the privacy of the data entrusted to them. Finally, a startling complicit stillness or lack of controllers in this sector appears to have existed. Nigerians have never actually cared about what happens to their information, as long as their other financial and physical rights remained unaffected, up to the creation of a tiny number of civil organisations that have recently made data privacy and protection their top priorities.

e. Reporting Data Breaches: The majority of data breaches continue to get unreported to the data subjects or unrecorded, despite Nigeria's DPA and NDPR becoming more and more popular. This has been attributed to a number of factors, including delays in notifying the data subject of breaches in some circumstances, failure to report breaches to the authority or to the data processor or controller, failure to report breaches to the authority to determine whether the controller should notify the data subject of the breach, and others. [62]

7. Recommendations for Enhancing Data Protection on the Internet

Based on the various issues identified above the following recommendation are proferred:

a. Both public and private sectors in Nigeria must acknowledge the critical importance of safeguarding the right to privacy, not only as an inherent value but also as an essential foundation for freedom of expression, thought, and information.[63] The recent report from the UN Special Rapporteur on freedom of opinion and expression

---

61 Chika DM, Tochukwu ES (n 56).

62 Dode A, (2018) "The challenges of implementing General Data Protection Law (GDPR)" https://www.academia.edu/37461999/The_challenges_of_impleme nting_General_Data_Protection_Law_GDPR_ accessed July 31, 2023.

63 Carly N (n 41).

underscores these points by stressing that "communications surveillance should be recognized as a deeply invasive act that can impact freedom of expression and privacy rights, endangering the core of democratic societies."[64] It is important that the all relevant government institutions prioritize the need for strict legal regulation of surveillance, criminalization of illegal surveillance by public or private entities, controlled provision of communications data by private sectors, and the preservation of online anonymity and encryption. It is impossible for the government to claim commitment to advancing free expression without prioritizing privacy. This means that Nigerian government must go beyong the laws on paper to actually protect people's data and right to privacy.[65] To fundamentally enhance data protection in Nigeria, a profound dedication from the government is required to hold both public and private institutions and entities liable to openly promulgated laws, uniformly enforced, impartially adjudicated, and harmonious with international human rights norms and standards.

b. Furthermore, there is a need for nigeria to playing a central role in shaping data protection norms across the continent and engaging in global data protection frameworks given its substantial population and prominence in the burgeoning digital economy of Sub-Saharan Africa.[66] Optimally complying with the provisions of Ecowas Supplementary Act on Personal Data Protection and the African Union Malabo Convention can yield substantial benefits especially in respect to cross-border transfer of data.[67]

c. It is also recommended that the relevant agencies should organize orientation exercises for data processors, data subjects and other stakeholders across the country in order to intimate them of their rights, duties and responsibilities under the DPA and NDPR among other legislation. This will foster compliance and ensure the

---

64 Carly N (n 41).

65 Adewumi A. 'Adequate protection': an analysis of Nigeria's data protection laws within an emerging global data protection framework (Doctoral dissertation). https://dspace.library.uvic.ca/bitstream/handle/1828/13888/Adewumi_Adekunle_LLM_2022.pdf accessed August 11, 2023.

66 Ibid.

67 Ibid.

protection of peoples' data in line with their fundamental human rights.

8. Conclusion

From the discussion, it is clear that data has become a ubiquitous asset in the global community, mirroring the transformation of modern societies, in which massive data collection and analysis have become a key competitive advantage on the especially on the internet. However, the transformation also emerges with its own challenges particularly in emerging societies like Nigeria, despite the current mechanisms of alleviating them. Notwithstanding, the enactment of the Nigeria Data Protection Act is a welcome development that is long overdue. Prior to the signing of the Act, many stakeholders had queried the legitimacy of the NDPR on the basis of the absence of a clear statutory provision or enabling Act. However, the Nigeria Data Protection Act now provides an unmistakable statutory basis for privacy law and practice in Nigeria. It is believed that the recommendations will further help in the actualization of individual rights and freedoms such as human rights to privacy and freedom of expression on the internet.