

FREEDOM OF EXPRESSION AND DATA PRIVACY PROTECTION: CHALLENGES AND REMEDIES

Temitope Daniel Bamidele*

Omoniyi Bukola Akinola**

Grace Olamide Bamidele***

Abstract

The right of personal privacy and freedom of expression are said to be quintessential to the preservation of human dignity, self-determination, self-development, and safety. These rights are provided by the Nigerian constitution as well as the African Charter on Human and Peoples' rights. Data protection is an important tool to the development of any country. The importance of data privacy and protection has grown recently, because data has transformed into a valuable resource for the entire world community in the Internet era. The widespread breaches of sensitive data 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

* Temitope Daniel Bamidele, LL.B. LL.M, M.Phil Candidate (Obafemi Awolowo University, Ile-Ife). Email Address: bamidele.temitope007@gmail.com

** Akinola Omoniyi Bukola, LL.B (Hons), LL.M, PhD, Barrister at Law and Professor of Law, Faculty of Law, Baze University, Abuja. Former Dean of Law, Faculty of Law, Redeemer's University, Ede, Osun State, Nigeria. Former Dean of Law, School of Law, Kampala International University, Uganda and Former Deputy Director of Academics, Nigerian Law School. Email Address: profobakinola77@gmail.com, omoniyi.akinola@bazeuniversity.edu.ng

*** Grace Olamide Bamidele (Nee Oke), B1, Ll.b, 08168010825, Email Address: okeolamide01@gmail.com

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. This paper examines Nigerian data protection laws with other jurisdictions in relation to online protection for human rights. To achieve this, legislations, published papers and journals were reviewed. The research finds that issues like a lack of enforcement efforts and a lack of understanding of privacy rights are some of the issues impeding the effectiveness of data protection laws on human rights protection. This paper recommends that enforcement efforts be strengthened and that the general public in Nigeria be made aware of their right to privacy,

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

1.0 INTRODUCTION

Globalization has led the world to move into the digital age, where several activities are done on digital platforms. Nigerians, on their part, have also found social media platforms as one of the most powerful communication tools for engaging the public, marketing, sales, and friendship. As a result of this, the fundamental right to freedom of expression is exercisable online. This online expression and privacy are digital rights in the Internet era.¹ The Freedom of expression is one of the basic fundamental human rights guaranteed in the section 39 of the Constitution of the Federal Republic of Nigeria, 1999 (as amended) and Section 37 of the same Constitution also guarantees right to privacy as the fundamental right which must be protected.

¹ Airat Oyiwonolu Shitta and others, ‘An Overview of Online Expression as a Digital Right’ (2020)

The United Nation which Nigeria is a State Member also affirms that the same fundamental rights that people have offline must also be protected and enjoyed online.² It can be argued that, right to privacy and freedom of expression are exercisable online and they are two side of the same coin which must be protected and enjoyed together. Because, if there is effective application of the right to privacy online, people will express their feelings and opinions freely without fear of interception or interference by any authority.

Privacy issues have also been the subject of legal discourse over time and owing to its significance to the existence of a livable society,³ privacy has attained the status of a fundamental right globally. Privacy rights underpin the people's freedom of association, thought and expression as well as the right to human dignity and freedom from discrimination. They further prevent the Government from spying on persons without just cause.⁴ More so, asides restraining the appetite of governments and its agencies, privacy rights shields individuals from the overreaching and overbearing hands of private sector actors. In short, without privacy we cannot properly function as a society or as individuals. Although privacy rights have long been an issue of discussion, the public discussion surrounding it has

² Adeboye Adegoke, *Digital Rights and Privacy in Nigeria*, (Paradigin Initiative Publication, 2020); 4.

³ Privacy affords individuals the space needed to flourish as human beings. It gives persons the ability to learn, play and make mistakes without the fear of ridicule and the worries of being haunted by the past forever. Privacy forms the cornerstone of certain social, physical and emotional relationships. Patients relate with their doctors; customers with banks; congregation with priests; due to the existence of confidence and a common understanding of confidentiality. Privacy helps individuals define their relationship with the outside world.

⁴ Adeboye Adegoke (n 2)

become intense over the past decades. Before now, privacy concerns were basically physical and included eavesdropping, intrusive searches into people's home, blackmail and stalking.⁵ This follows from the fact that prior to the digital era; it was easy to distinguish between one's private and public spaces. In recent times, this demarcation has been blurred.

New technologies have fundamentally changed how we negotiate and experience privacy. Facial recognition technologies are being used to unlock phones, complete financial transactions, authenticate identities, read expressions during interviews, track the movements of persons, and profile persons, especially in the business and advertising world.⁶ Further, the invention of innovations like the Internet of Things (IoTs), which basically connects everyday devices to the internet to make life easier, and technological devices like the Closed-circuit Television (CCTV) leaves individuals vulnerable to hacks and prying eyes. The digital age has created vast and ubiquitous databases of personal information in universities, corporations, government agencies, and doctors' offices.⁷ Consequently, issues of privacy have significantly evolved from physical Privacy to personal information (data privacy).

2.0 CONCEPTUAL CLARIFICATION

(a) Freedom of Expression

Freedom of expression is a fundamental human right recognized as essential for the conduct of a free society. It enables individuals to voice

⁵ Today, these concerns include other issues bothering on confidential correspondences, email and internet use, medical history, personal data, sexual orientation and personal lifestyle.

⁶ Anupam Chander and Lauren Gelman and Margaret Radin, *Securing Privacy in the Internet Age* (2nd edn, Stanford Law Books 2008)

⁷ Ibid.

opinions, share information, and engage in discourse, contributing to the realization of other rights protected under human rights law. Upholding freedom of expression encourages democratic participation and cultivates an informed citizenry.⁸

The significance of freedom of expression in human rights law lies in its ability to facilitate open dialogue and critique, which are vital to promoting accountability and transparency. This right allows marginalized communities to raise their voices, thereby fostering social equity and justice. In many jurisdictions, national legislation mirrors international standards, reinforcing the protection of this right.⁹

Freedom of expression is also regarded as one of the essential ingredients of a “democratic democracy”. This right prevents the government and individuals from preventing a person from receiving information and ideas available to the public.¹⁰ It imposes obligations and duties on the state or agencies and on individuals to protect and promote human rights and fundamental freedoms. The right of freedom of expression which is stressed in the 1999 constitution in section 39¹¹ that every person shall be entitled to freedom of expression, including freedom to hold opinions and to receive and impart ideas and information without interference as well as protect the right of every person to own, establish and operate any medium for the dissemination of ideas and opinions¹² and without

⁸ [https://lawslearned.com/Understanding Freedom of Expression: Its Importance and Challenges - Laws Learned](https://lawslearned.com/Understanding-Freedom-of-Expression-Its-Importance-and-Challenges-Laws-Learned) accessed 17th April 2026.

⁹ Ibid.

¹⁰ O Ogbu (1999). *Human Rights Law and Practice in Nigeria: An Introduction*. Enugu; IDJAP Press; pp 184.

¹¹ Constitution of the Federal Republic of Nigeria, 1999 (as altered) (CFRN 1999)

¹² E Odike (2005), *Human Right Law and Practices*, Enugu; Chenglo Ltd.

prejudice to the generality of subsections 39.¹³ This provision allows individuals to own, establish and operate any medium for the dissemination of information, ideas and opinions in Nigeria.

In Nigeria, there is also the freedom of information Act of 2011 Laws of the Federation of Nigeria to give more light to the freedom of expression in our society today. Freedom of expression is one of the very crucial aspects of democracy in Nigeria. Being put in the constitution entail that it is being guaranteed for the Nigerian citizen at all times with exceptions in certain circumstances that would lead to defamation which is a restriction to the enjoyment of this right.¹⁴ The freedom of expression is regarded as a cornerstone of democracy which ensures the consolidation and development of democracy. As a result of the exercise of this right, citizens are able to criticize the actions of government, organizations as well as individual. It is also deemed to be essential for the development of knowledge and understanding among people which will lead to true tolerance and operations among nations, this protection extends to freedom to hold opinions and to receive and impact ideas and information without interference as well as protects the right of every person to own establish and operate any medium for the dissemination of information of information, ideas, opinions.¹⁵

The right to freedom of expression is also guaranteed under the various international instruments on human rights and fundamental freedoms. Thus, Article 19 of the Universal Declaration on Human Rights provides as follows: Everyone has the right to freedom of opinion and expression;

¹³ CFRN 1999 Subsection (2), {1,{2},{3}} (n 11)

¹⁴ O Oliyide O & Awolowo (2006), Rights, Lagos; Throne of Grace Limited. Pp 1-12

¹⁵ Ibid.

this right includes freedom to hold opinion without interference and to seek, receive and impart information, and ideas through any media and regardless of frontiers.¹⁶

Similarly, Article 19 of the International Covenant on Civil and Political Rights provides for the right to freedom of expression that everyone shall have the right to hold opinions without interference and everyone shall have the right to freedom of expression; this right shall include freedom to seek, receive and impart information and ideas of all kinds, regardless of frontiers, either orally, in writing or print in the form of art or through any other medium of his choice.¹⁷

Article 9 of the African Charter on Human and Peoples Rights also provides for the protection of the right to freedom of expression in the following terms that every individual shall have the right to receive information and every individual shall have the right to express and disseminate his opinion within the law

(b) Data Privacy 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, and legal requirements.¹⁸ To put it another way,

¹⁶ Universal Declaration of Human Right, UNGA,1998 adopted at General Assembly Paris 10th December, 1948

¹⁷ International Covenant on Civil and Political Right, 1966.

¹⁸ I Olawunmi, and CC Emejue '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).

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.¹⁹ Generally, Data privacy refers to individuals' right to control their personal information and keep it confidential, whereas "data protection" denotes the legal and technical measures to secure that information. In other words, privacy emphasizes the data subject's interests and expectations of consent and confidentiality, while protection emphasizes the obligations of data controllers/processors to implement safeguards and procedures.²⁰ Nigerian law uses "data protection" as its statutory term, but it is premised on the fundamental "right to privacy" guaranteed by the Constitution. Data protection laws aim to operationalize that right by setting rules for the collection, use and sharing of personal data, ensuring data subjects' privacy rights are respected. This distinction is reflected in practice: data privacy is often about policy and consent (what data is collected and why), while data protection involves security measures, compliance programs, and breach response.²¹

The universally recognized right to privacy protects the individual from unauthorized intrusion, this right by extension protects the place of abode and information belonging to the individual. In Nigeria, the right to privacy is a Fundamental Right guaranteed under the Constitution

¹⁹ Ibid.

²⁰ <https://recordoflaw.in/an-> An Overview of Data Privacy and Protection in Nigeria - Record Of Law accessed 17th April 2026.

²¹ Ibid.

specifically in Section 37²² which provides that the privacy of citizens, their homes, correspondence telephone conversations and telegraphic communications is hereby guaranteed and protected This right envisages that unauthorized access to the person of or information about an individual is tantamount to an intrusion, which is a violation of the right. It is on the basis of this that several laws are passed to guard against these violations.

With advancements in information communications technology (hereinafter 'ICT') and a data driven approach to communications, buying and selling, all of which impact everyday life, privacy in the digital age is besieged by new threats, threats beyond the contemplation of the early privacy protection laws.²³ Data Privacy protection has had to develop in the area of privacy protection in a bid to combat these threats. Data Privacy protection regulates the relationship between the collection and dissemination of personal data, technology, the public expectation of privacy, the ability an individual has to determine what personal data in a computer system can be shared with third parties as well as legal and political issues surrounding Data Privacy.²⁴

3.0 THEORETICAL FRAMEWORK

Human rights are one of the significant features of our political reality. It is the moral rights of highest order. Human Rights are evolved out of self-respect. It is inherent to all humans without any discrimination of race, sex, nationality, ethnicity, language, religion and colour etc. It received

²² CFRN 1999.

²³ Lukman Adebisi Abdulrauf, *The Legal Protection of Data Privacy in Nigeria: from Canada and South Africa*

²⁴ Ibid.

new shape when human beings began to think themselves. Every human being are entitled to these rights without any discrimination.²⁵

a Theory of Natural Rights

It states that an individual enters into society with certain basic rights and no government can deny these rights. The natural rights evolved out of the natural law that peoples are the creatures of nature. They exist their lives and organize their society based on rules and principles laid down by nature. When the idea of individualism developed in the 17th century, theory of natural law were modified and focused on the rights of the individuals. It cannot be violated by anyone or by any society because they are natural beings. Therefore, we can clearly say that today's human rights are the child of ancient natural rights.²⁶

The most notable expression of this doctrine is found in the writings of John Locke. John Locke argued that all individuals were gifted by nature with the inherent rights to life, liberty and property of their own and could not be removed or abolished by state. Two things are evident from his view of natural rights, one is the individual is an autonomous being capable of exercising choice and the second is the legitimacy of government depends not only upon the will of the people, but also upon the government's willingness and ability to protect those individual natural rights. Accordingly, human beings are rational and good by nature, and they carried the same rights they had enjoyed in earlier stages of society into political society, and important among them are freedom of worship, the right to a voice in their own government, and the right of

²⁵ Jack. Donnelly, *Universal Human Right in Theory and Practice* ,London, Cornel University Press, London, p. 12

²⁶ E source L. Strauss, *Natural Right and History* (1957)

property.²⁷

b Theory of Legal Rights

According to this theory, rights are created and maintained by the state. The state is the only source of right, and outside the state, an individual has no rights at all and never claims rights against the state. The theory further maintains that rights are not natural to man. The political pluralists object to this theory because the state does not create rights, but only recognizes them. One of the main exponents of this theory was Austin. There is a lot of criticism of this theory because it does not provide an adequate basis for rights. It might tell us the character of a particular state, but it does not tell us what rights need recognition. This theory will lead to a despotic state and the tyranny of laws. It does not provide a basis for knowing which right ought to be ensured. Rights are in fact not what the state grants, but what the man needs for his self-development and what the state should grant.²⁸

4.0 LEGAL FRAMEWORK FOR REGULATING DATA PRIVACY PROTECTION

The entire gamut of laws on a specific subject is referred to as the legal framework. A legal framework comprises a broad system of rules, procedures, which govern and regulate particular subjects in a given jurisdiction. In Nigeria, the protection of Data Privacy is largely dependent on the protection of privacy itself. Consequently, the reality is that the legal framework for Data Privacy protection in Nigeria primarily

²⁷ Ibid

²⁸ P Forsythe, Frederick *Encyclopaedia of Human Rights*, Oxford University Press, New York, 2009.

consists of the constitutional framework for the protection of privacy in Nigeria.²⁹

(a) Constitution of the Federal Republic of Nigeria, 1999

Section 37 of the Constitution of the Federal Republic of Nigeria (CFRN) 1999 (as amended) guarantees the right to privacy. This is the foundation of Data Privacy Protection as a constitutionally assured right in the country, as set out in the fourth chapter. Section 37 of the CFRN provides that the privacy of citizens, their homes, correspondence, telephone communications, and telegraphic communications is hereby guaranteed and protected.³⁰

This provision, by virtue of the authority imbued in the Constitution, extends the right of privacy to all individuals to cover their homes, their personal conversations, and their communications by way of telephone or by telegraph. One commentator has expatiated on the ramifications of section 37 of the Constitution as encompassing the privacy of the person (i.e., from unwanted incursions into physical, emotional, and personal attributes); the sanctity of homes and property (i.e., from unauthorized searches and trespasses); and the protection of correspondence and conversations from being intercepted and diverted.³¹

(b) Nigeria Data Protection Act (NDPA) 2023

²⁹ S. 37 Constitution of the Federal Republic of Nigeria (CFRN) 1999 (as amended). this section provides for the right to private and family life.

³⁰ s 37 of the Constitution of Federal Republic of Nigeria, 1999 (as amended).

³¹ Adedeji Adekunle, *'Right to Privacy and Law Enforcement'* being the Text of a Lecture presented at the Ogun Judges Conference (2016)

The Nigeria Data Protection Act 2023, (NDPA) represents Nigeria's primary legislation governing data privacy and protection. While building upon the existing Nigeria Data Protection Regulation (NDPR) 2019, the Act extends the enforcement of data protection. The act also establishes the Nigeria Data Protection Commission as the central authority responsible for enforcing compliance and overseeing data protection in Nigeria.³² The act aligns closely with global best practices by introducing clear provisions on data processing, user rights, security measures, cross-border data transfers, and enforcement mechanisms. Notably, both the Nigeria Data Protection Act (NDPA) 2023 and NDPR 2019 remain in force, with The NDPA taking precedence in cases of conflict.³³ Consent is a fundamental requirement under in the act, Section 26³⁴ explicitly provides that there must be clear, affirmative, and informed consent before data is processed. Silence or inactivity does not constitute consent; it also allows data subjects to withdraw consent at any time and there is are special provisions for sensitive personal data.

The Nigeria Data Protection Act (NDPA) 2023 grants data subjects several rights to ensure control over their personal information by giving them access in section 34,³⁵ the access is to their personal data and to obtain information about its processing. While Section 35³⁶ allows users to withdraw consent previously granted for data processing while Section 36 establishes the right to object to certain types of data processing, including direct marketing or targeting.

³² SC Ifemeje, and NM Okwuosa, 2021. Data Privacy Protection: Overview of the Legal Framework in Nigeria. *International Review of Law Journal (IRLJ)*, 3, p.111.

³³ Ibid.

³⁴ Ibid. s 26, Nigeria Data Protection Act 2023

³⁵ Ibid. s 34 Nigeria Data Protection Act 2023

³⁶ Ibid. s 35 Nigeria Data Protection Act 2023

The NDPA does not only provide for the rights of data subjects but also ensures that it is duly enforced through strict security measures to prevent unauthorized access, loss, or breaches. In the event of data breach, Section 39³⁷ requires mandatory notification of data breaches to both the Nigerian Data Protection Commission and affected individuals. It also empowers the Nigerian Data Protection Commission to investigate violations and impose penalties. Section 46 enables individuals to file complaints with the Nigerian Data Protection Commission regarding alleged violations, and Section 48³⁸ allows the Commission to issue enforcement orders against non-compliant entities. Penalties include fines based on the severity of infractions, with specific amounts determined by the Commission.

The Nigeria Data Protection Act, 2023, provides for cross-border data transfers. The fundamental principle is that the personal data of Nigerians can only be transferred to countries that provide adequate levels of data protection. This requirement is provided in Section 41³⁹ serves as a safeguard to prevent the transfer of Nigerian data to jurisdictions with insufficient privacy protections. The determination of whether a foreign country provides adequate protection is based on an evaluation established by Section 42⁴⁰ It is based on multiple factors, including the country's international commitments and rules for onward transfers.

(c) Freedom of Information Act

³⁷ s 39 Nigeria Data Protection Act 2023

³⁸ s 48 Nigeria Data Protection Act 2023

³⁹ s 41 Nigeria Data Protection Act 2023

⁴⁰ s 42 Nigeria Data Protection Act 2023

With the rise of the democratic system in Nigeria and after years of military regimes, there came a clear call from the people for there to be more transparency in the actions of the government in carrying out its activities. A result of this clamor is the Freedom of Information Act (FOIA). This Act gives public institutions the power to deny any request for information that contains personal information.⁴¹ The FOIA grants the public access to public records and information as an effort to lift the shroud of obscurity on the actions of the government. This is done in a way that holds the interest of the public close and guarantees the protection of personal information and privacy. Section 14(1) of the FOIA provides that 'a public institution must deny an application for information that contains personal information.' With this provision it is clear that the FOIA cannot be used to gain access to information that is seen as sensitive or personal. This Act defines what may constitute personal information as "any official information held about an identifiable person but does not include information that bears on the public duties of employees and officials."⁴²

The Freedom of Information Act (FOIA) in Nigeria strikes a balance between transparency and data privacy. While granting public access to records, it safeguards personal information. Section 14(1) mandates institutions to deny requests containing personal data, ensuring sensitive information remains protected. The Act defines personal information as data about identifiable individuals, excluding information related to public duties. This provision shields citizens' privacy while promoting government accountability. By limiting access to sensitive information, the FOIA prevents potential misuse and maintains trust in government

⁴¹ s 14 of the Freedom of Information Act 2011.

⁴² Section 30 of the Freedom of Information Act 2011.

institutions. This balance fosters openness while respecting individuals' right to privacy.

5.0 INSTITUTIONAL FRAMEWORK FOR REGULATING DATA PRIVACY PROTECTION

Several Institutions in Nigeria house the substantive laws and regulations relating to privacy and data protection.

(a) Nigeria Data Protection Commission

Sections 4, 5, 6, 7, 8, 9, 10, 11, 12 and 13 of the Nigeria Data Protection Act provide for the establishment, functions, powers, independence of the Commission, establishment of the Governing Council, appointment of members; tenure, cessation of membership of the Council; functions and powers of the Governing Council and conflict of interest of the Council respectively.⁴³

Section 27(1) of the NDPA provides that before a data controller collects personal data directly from a data subject, the data controller must inform the data subject of the identity, residence or place of business and means of communication with the data controller and its representative, where necessary; specific lawful basis of processing under section 25(1) or 30(1) of the NDPA and the purposes of the processing for which the personal data are intended; recipients or categories of recipients of the personal data, if any; existence of the rights of the data subject under Part VI of the NDPA; retention period for the personal data; right to lodge a complaint with the Commission in accordance with section 46(1) of the NDPA; and existence of automated decision-making, including profiling, the

⁴³ Yinka Olomajobi, 'Right to Privacy in Nigeria' (October 31, 2017) accessed 18th April 2026

significance and envisaged consequences of such processing for the data subject, and the right to object to and challenge such processing. Under subsection (2) of section 27, before a data controller collects personal data, other than directly from the data subject, the data controller shall inform the data subject of the matters set out in subsection (1), except where the data subject has already been provided with such information, or the provision of such information is impossible or would involve a disproportionate effort or expense.

(b) Federal Competition and Consumer Protection Commission

The Commission was established by the Federal Competition and Consumer Protection Act, 2018, and operates under the Federal Ministry of Industry, Trade and Investment. The Federal Competition and Consumer Protection Commission (FCCPC) is Nigeria's primary authority for competition and consumer protection. Its mandate is to ensure fair and competitive markets, protect consumer rights, and promote access to safe products by investigating and sanctioning anti-competitive or unfair business practices. Key functions include issuing regulations, resolving disputes, and enforcing compliance through investigations and legal action.⁴⁴ In 2024, the FCCPC fined Meta US\$220 million for violating consumer, privacy/data protection laws (e.g. gathering/sharing personal data without proper consent, exploitative privacy terms). Meta appealed. On 25 April 2025, the Tribunal upheld the fine.⁴⁵

6.0 THE NEED FOR DATA PROTECTION AND ITS NEXUS WITH RIGHTS TO PRIVACY AND FREEDOM OF EXPRESSION

Freedom of expression and privacy protection are two key aspects in the

⁴⁴ Ibid.

⁴⁵ Ibid.

context of human rights that define the complex relationship between individuals, society and government. Freedom of expression refers to the right of every individual to express opinions, speak, and convey ideas without fear of repression or unauthorized restrictions.⁴⁶ Meanwhile, privacy protection concerns the right of individuals to safeguard their personal information from misuse and unauthorized access. In the context of an increasingly digitally-connected society, the debate around the balance between freedom of expression and privacy protection is becoming increasingly relevant and complex.⁴⁷

Freedom of expression, as a fundamental value in democracy, reflects the right of every individual to express their views without fear of the authorities.⁴⁸ The existence of freedom of expression allows people to access information, participate in the political process, and shape public opinion. Along with the development of information and communication technology, freedom of expression also involves digital platforms, where individuals can express their views online. However, this also opens the door to questions regarding the boundaries of freedom of expression, particularly in the face of issues such as hate speech, disinformation, and threats to national security.⁴⁹

On the other hand, privacy protection is becoming increasingly important due to the large amount of personal data collected and processed by

⁴⁶ A Pujiyanto Mulyati, & R Novaria, (2018). Pemanfaatan Big Data Dan Perlindungan Privasi Konsumen Di Era Ekonomi Digital. *Majalah Ilmiah Bijak*, 15(2), 127–137

⁴⁷ Ibid.

⁴⁸ GA Putra, V Taniady & IM Halmadiningrat, (2023). Tantangan Hukum: Keakuratan Informasi Layanan AI Chatbot Dan Pelindungan Hukum Terhadap Penggunaanya. *Jurnal Rechts Vinding Media Pembinaan Hukum Nasional*, 12(2), 281–299

⁴⁹ A Pujiyanto, A Mulyati, & R Novaria, (n 46)

companies and governments. Personal data includes information such as names, addresses, phone numbers and financial information, which are often stored in large databases and used for a variety of purposes, including marketing, risk analysis and national security. When such personal data is not properly protected, individuals are at risk of privacy breaches, identity theft, or misuse of information.⁵⁰ On the other hand, privacy protection is becoming increasingly important due to the large amount of personal data collected and processed by companies and governments. Personal data includes information such as names, addresses, phone numbers, and financial information, which are often stored in large databases and used for a variety of purposes, including marketing, risk analysis, and national security. When such personal data is not properly protected, individuals are at risk of privacy breaches, identity theft, or misuse of personal information for harmful purposes.⁵¹

In an effort to maintain a balance between freedom of expression and privacy protection, many countries have developed laws and regulations governing the use and protection of personal data. Such laws often create a framework for protecting individual privacy while ensuring that freedom of expression is respected. Nonetheless, there are conflicts and ethical dilemmas in dealing with situations where national security interests or other public interests' conflict with individual privacy rights.⁵² One significant example in this debate is the spread of fake news or disinformation in the digital age. While freedom of expression protects the

⁵⁰ E Pertiwi, D Delvina Nuraldini, G Tri Buana & A Arthacerses, (2022). Analisis Yuridis Terhadap Penyalahgunaan Data Pribadi Pengguna Media Sosial. *Jurnal Rechten : Riset Hukum Dan Hak Asasi Manusia*, 3(3), 10–16.

⁵¹ Ibid.

⁵² F Fensi, (2018). Fenomena Hoax: Tantangan terhadap Idealisme Media & Etika Bermedia. *Bricolage : Jurnal Magister Ilmu Komunikasi*, 4(2), 133–209.

right of individuals to express their opinions, disinformation can damage reputations, create social instability, and influence political processes. Therefore, there are calls for stricter restrictions on the content that can be published online to protect society from this threat.⁵³ To address this dilemma, a number of countries have introduced laws or regulations that require online platforms to take steps to identify and remove harmful content. While these efforts are motivated by a desire to fight disinformation, they can also be perceived as a form of censorship or restriction of freedom of expression. Therefore, it is important to create a balanced legal framework, considering the rights of individuals as well as the public interest. On the privacy protection front, legislative and regulatory efforts are also evolving to respond to challenges arising from ever-advancing information technology.⁵⁴

However, privacy protection also faces challenges from rapid changes in technology, such as the use of artificial intelligence and big data analysis. The ability to collect, store and analyze data on an unprecedented scale raises questions about the extent to which individuals can maintain control over their personal information. Companies and governments must operate within a legal framework that recognizes individuals' right to privacy while also enabling technological innovations necessary for the advancement of society.⁵⁵ Along these lines, the concept of privacy-by-design has emerged, where products and services are designed from the

⁵³ Ibid.

⁵⁴ Ibid.

⁵⁵ LKK Saragih, D Budhijanto, & S Somawijaya (2020). *Perlindungan Hukum Data Pribadi Terhadap Penyalahgunaan Data Pribadi Pada Platform Media Sosial Berdasarkan Undang-Undang Republik Indonesia Nomor 19 Tahun 2016 Tentang Perubahan Atas Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi Dan Transaksi Elek. De'Rechtsstaat*, 6(2), 125–142.

ground up with privacy protection in mind as an integral part of the design. This includes the development of strong encryption tools, more transparent privacy settings, and ethical thinking in data collection and use. These principles reflect efforts to create a digital environment that supports the sustainability of freedom of expression and individual privacy.⁵⁶ However, along with these efforts, there remains uncertainty and debate about the extent to which privacy rights should take precedence over the need for national security, crime prevention, and other public interests. These questions highlight the complexity of the relationship between freedom of expression and privacy protection in the context of an increasingly connected and technology-dependent society.⁵⁷

7.0 CHALLENGES TO THE IMPLEMENTATION AND ENFORCEMENT OF DATA PRIVACY PROTECTION IN NIGERIA

Navigating the complex terrain of privacy and data protection regulation presents a myriad of challenges for organizations and individuals alike. That is, in Nigeria, the development of data privacy and protection has been stifled for several reasons, notable among which are as follows:

(a) Increasing risk from advances in information technology

It goes without saying that technology has been, and continues to succeed at, the role of putting the world at our fingertips, to the point that almost all information can be obtained at the convenience of our fingertips. The fact that abusers have taken advantage of these systems' weaknesses to further their actions shows that this is not without problems. Of course,

⁵⁶ Ibid.

⁵⁷ Ibid.

the concerns posed by the advancement of information technology to further improve the circulation and retention of data are cause for concern as they extend to the absence of suitable laws to fully address existing issues relating to the data subject. One of the fundamental flaws in the current data legislation is that there are only measures for protecting digital data and none for offline data, in addition to the fact that there aren't many situations where the issue has been resolved.⁵⁸

(b) Inadequate regulation of the usage and storage of internet data

Since many nations have not yet passed and put into effect data and privacy protection legislation, particularly in Nigeria, this issue is one that affects nations all over the world. The necessity for appropriate rules to recognize and then address concerns coming from data is evident as the world starts to realize the importance of data. The fact that several attempts have been made to reproduce every stage of numerous human activities⁵⁹ and that this has led to the use and preservation of data, particularly on users on social media platforms, is no longer a surprise. As a result, it is even more important that users and prospective users read and comprehend the data and privacy protection policy before or during sign-up.⁶⁰ This is because users' data may be compromised, made public, and subsequently exploited by hackers for malicious purposes. Given the lack of legislation in that area and the abundance of disclosed figures and gaps that reveal our susceptibility, the probability of data abuse becomes alarming. As the NITDA Regulation is largely responsible for Nigeria's

⁵⁸ Olumide Babalola, *'Data Protection and Privacy Challenges in Nigeria (Legal Issues) - Privacy - Nigeria'* (Mondaq.com, 2020) accessed 18th April 2026

⁵⁹ Uche Val Obi SAN, *"An extensive article on data privacy and data protection law in Nigeria | International Network of Privacy Law Professionals"*, (2020).

⁶⁰ Ibid.

historic success in protecting personal information, it must be given more authority to solve data issues. Making the dream a reality requires developing a workable method for carrying out the NITDA Regulations' requirements.⁶¹

(c) Hardware defects and failures in data technology

Failures and data malfunctions are unquestionably fatal since they are expected to result in the loss of irretrievable data, which may be unintentional or due to system corruption or malfunction. Therefore, it is unnecessary to state that data loss can result from hardware failures related to data. Data protection can include, among other things, protection from corruption or hacking.⁶² Fortunately, data recovery or retrieval is probably possible very quickly after the loss or corruption, according to data protection policy.⁶³

Sometimes the failure of data technology can be ascribed to invasion, undoubtedly because there is insufficient data security. Data protection and privacy should be given a lot of attention in order to ensure that the developing internet-world does not become vulnerable and to lessen the likelihood of hacking, especially since there are not enough regulations that cover the entire spectrum of data and privacy.⁶⁴

Moreover, regulations to preserve and protect data on failed data tech hardware are a matter that requires an urgent response. A decentralized

⁶¹ Ibid.

⁶² Paul Crocetti, 'What Is Data Protection and Why Is It Important? Definition From Whatis.Com' (SearchDataBackup, 2021) accessed 18 April 2026.

⁶³ Ibid.

⁶⁴ Camila Winlo, 'The 10 Data Privacy Fails of The Decade – And What We Learnt From Them' (TechRadar, 2020)

system of operation may put an end to this, meaning that people can be left to impose limitations on the usage of unencrypted private data rather than leaving that up to the tech companies to control. This demonstrates the need for legislation as well as other required measures to ensure that data protection and privacy are optimized in order to progress data protection and privacy.⁶⁵

8.0 REMEDIES TO THE IMPLEMENTATION AND ENFORCEMENT OF DATA PRIVACY PROTECTION IN NIGERIA

The following are regarded as attempts to remedy the challenges of data protection, which are as follows:

(a) 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.⁶⁶ 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

⁶⁵ Kurt Nielsen and Ana Alexandre, *'Tech Giants Failed to Protect Consumer Data — TheBlockchain Can Help'* (BeInCrypto, 2021)

⁶⁶ Olumide Babalola: *Data Protection and Privacy Challenges in Nigeria (Legal Issues)*, 09 March 2020, page 9, Available <https://www.mondaq.com/nigeria/data-protection/901494/data-protection-and-privacy-challenges-in-nigeria-legal-issues->. Accessed on 18 April, 2026.

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.⁶⁷

(b) 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.⁶⁸

(c) 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 be set at the international level and apply to all states, regardless of whether a country is developed. Conflicting or nonexistent laws hamper the fight against illegal data access and cybercrime. Developing countries need to establish common laws that can be uniformly applied in different countries for the

⁶⁷ Ibid.

⁶⁸ Uche Val Obi: *Data Privacy and Protection Regulations in Nigeria*, Available at <https://inplp.com/latest-news/article/challenges-confronting-implementation-of-data-privacy-and-protection-regulations-in-nigeria/>. Accessed on 18th April 2026.

same crime. Relevant stakeholders in developing countries should therefore hold common forums within which certain laws can be harmonized.⁶⁹

9.0 COMPARATIVE PERSPECTIVES

In this section, a comparative analysis of legal and institutional frameworks for privacy, data protection, and cybersecurity for South Africa, the United Kingdom, and Illinois (Chicago) is undertaken.

9.1 United Kingdom

The UK retained GDPR principles post-Brexit through the UK GDPR and Data Protection Act 2018.⁷⁰ Their Information Commissioner's Office (ICO) is a model of independence and enforcement. In *Lloyd v. Google LLC* [2021] UKSC 50, the Supreme Court clarified that representative claims for data breaches require proof of material damage or distress.⁷¹ This ruling narrowed the scope for class actions but reinforced the importance of judicial interpretation in shaping privacy law. In Nigeria, our courts are only beginning to engage with digital rights. We must encourage more robust jurisprudence.

9.2 United States – Illinois (Chicago)

Illinois, particularly Chicago, offers a compelling sub national model of biometric privacy regulation. The Biometric Information Privacy Act (BIPA), enacted in 2008, requires informed consent before collecting

⁶⁹ 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,

⁷⁰ Data Protection Act 2018 (UK) available at accessed 18th April 2026 UK GDPR.

⁷¹ *Lloyd v. Google LLC* [2021] UKSC 50.

biometric identifiers such as fingerprints and facial scans.⁷² What is remarkable and instructive for Nigeria is that BIPA allows individuals to sue even without proving actual harm. In *Rosenbach v. Six Flags Entertainment Corp.*, the Illinois Supreme Court held that a mere violation of BIPA is enough to confer standing.⁷³ This has led to a surge in litigation, especially in Chicago, where biometric privacy is taken seriously. In comparison to Nigeria, the National Identity Management Commission, 2007 mandates the collection of biometric data including fingerprints and facial images for the issuance of the National Identification Number (NIN).⁷⁴ While the Act outlines data protection obligations under Sections 19 and 20, it lacks the granular consent requirements and enforcement mechanisms seen in BIPA. Moreover, the NIMC operates largely in isolation from the Nigeria Data Protection Commission, raising concerns about institutional overlap and accountability.

9.3 South Africa

South Africa's Protection of Personal Information Act (POPIA), enacted in 2013 and enforced from July 2021, feels familiar to us.⁷⁵ Like our NDPA, it emphasises consent, purpose limitation, and lawful processing. But what sets South Africa apart is the Information Regulator a dedicated body with teeth. Their Cybercrimes Act 2021 complements POPIA by criminalising offenses like cyber fraud and unlawful interception.⁷⁶ The

⁷² Biometric Information Privacy Act, 740 ILCS 14 (Illinois)

⁷³ *Rosenbach v. Six Flags Entertainment Corp.*, 2019 IL 123186.

⁷⁴ Sections 5–6, 19–20, National Identity Management Commission Act, Cap N155, Laws of the Federation of Nigeria 2004 (enacted 2007),

⁷⁵ Protection of Personal Information Act 4 of 2013 (South Africa) available at accessed 18th April 2026

⁷⁶ Cybercrimes Act 19 of 2020 (South Africa) available at accessed 18th April 2026

synergy between their data protection and cybersecurity laws is something we should emulate. In Nigeria, our institutions often operate in silos. We must bridge that gap.

10. CONCLUSION AND RECOMMENDATIONS

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. Before the signing of the Act, many stakeholders had queried the legitimacy of the NDPR based on 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 below will further help in the actualization of individual rights and freedoms such as human rights to privacy and freedom of expression.

(a) A Comprehensive and Effective Data Privacy Law

As quickly as possible, Nigeria needs to enact a comprehensive Data privacy law like the United Kingdom General Data Protection Act and data legislations from other develop countries, including the EU GDPR. A nation is seen as taking data privacy seriously when substantial legislation, rather than a supplementary regulation, is passed. Foreign investors increasingly heavily weigh a country's data privacy profiles when making investment decisions. For instance, the EU GDPR and other

data privacy regulatory bodies of several nations have made it illegal for their private and corporate citizens to transfer or share data obtained within their borders with nations with weak or non-existent data privacy regulations.⁷⁷

(b) Public Awareness on Data Privacy and protection:

The public should be educated about the requirements of the NDPR and the importance of upholding data privacy. Both data subjects and data processors should be the focus of the sensitization programs, who should inform them of their rights and the consequences of violations of the NDPR. This can be done through collaboration with the mainstream media or social media. This will improve the effectiveness data privacy protection. Response to hardware malfunctions and failures in data technology: Data must be safeguarded from physical threats such hardware malfunction and data technology failure. Users have a crucial role to play in preventing system failure since users may be the cause of system failure.⁷⁸ Testing the code as well as user guides that incorporate system specs are the best techniques for preventing system failure.⁷⁹

⁷⁷ Uche Val Obi SAN (n 65)

⁷⁸ Ibrahim Shehu and Sani Rabiun Bello, 'Challenges to the Implementation and Enforcement of Data Protection in Nigeria', (2022) 121 *Journal of Law, Policy and Globalization*, 54.

⁷⁹ MD Tovi, MN Muthama, *Addressing the Challenges of Data Protection in Developing Countries*, (2013) 1(1) *European Journal of Computer Science and Information Technology*, 6.