



digicivic
INITIATIVE

DIGITAL RIGHTS AND CIVIC SPACE MANUAL

Copyright © 2024 by DigiCivic Initiative

All rights reserved. This book or any portion thereof may not be reproduced, stored in a retrieval system, transmitted in any form or by any means, electronic, mechanical, photocopying, recording, or otherwise, or used in any manner whatsoever without the express written permission of the publisher except for the use of brief quotations in a book review.

Printed in Nigeria

For enquiries: digicivicinitiative@gmail.com

First Printing 2024

ISBN

Published by DigiCivic Initiative: Digicivic.org

This Manual was prepared to serve as a resource for training on digital rights.

Support for this work was provided by the Advocacy Assembly.

Designed by

LMNG CREATIVE STUDIO

ABOUT THE AUTHOR

Mojirayo Oluwatoyin Ogunlana is a digital rights lawyer on a mission to establish a legal framework at national and regional levels that safeguards a free and open internet while upholding human rights. She champions strategic litigation in courts to challenge constraints on freedom of expression, association and assembly. Mojirayo coordinates advocacy campaigns to enforce these fundamental rights across West Africa, envisioning a thriving civic space for current and future generations in the region.

With over 12 years of legal practice, Mojirayo has committed the past eight years to defending the rights of journalists, primarily on a pro bono basis, before Nigerian courts and the West African regional ECOWAS Court. She is renowned for her pivotal role in prosecuting the landmark case of Amnesty International, Togo & 7 Others v. The Republic of Togo, which addressed the internet shutdown and earned the Judgment the 2022 Columbia University Global Freedom of Expression Prize for a Significant Legal Ruling.

Mojirayo actively engages in litigation related to gender rights, sexual and gender-based violence, and gender discrimination. She represented Amnesty International Sierra Leone in advocating for the rights of pregnant schoolgirls in Sierra Leone in the W.A.V.E vs. Sierra Leone case at the ECOWAS Court.

Mojirayo is the Principal Partner of M.O.N. Legal, a law firm based in Abuja, Nigeria and the founder of the DigiCivic Initiative, a non-governmental organization. She is a fellow of the Internet Society Nigeria and co-chair of the Legal and Digital Rights Working Group.

Table of Contents

ACKNOWLEDGEMENT.....	4
PREFACE.....	4
INTRODUCTION.....	5
BACKGROUND.....	7
A GENERAL INTRODUCTION OF DIGITAL RIGHTS AND THEIR INTERSECTION WITH THE CIVIC SPACE.....	10
DIGITAL RIGHTS KEY TERMS.....	14
INTERNATIONAL AND REGIONAL FRAMEWORKS FOR DIGITAL RIGHTS IN NIGERIA.....	16
LEGAL FRAMEWORK FOR DIGITAL RIGHTS IN NIGERIA.....	38
BASIC DIGITAL RIGHTS ISSUES AND TERMS.....	44
AN INTRODUCTION TO INTERNET SHUTDOWNS.....	109
THE CONCEPT OF NATIONAL SECURITY AND DIGITAL RIGHTS.....	127
ONLINE HUMAN RIGHTS VIOLATIONS.....	135
ADDITIONAL JURISPRUDENCE ON DIGITAL RIGHTS.....	148

ACKNOWLEDGEMENT

This Manual is my way of contributing to the future of DigiCivic Initiative. The Manual was conceptualised in Senegal during the Impact West Africa Fellowship organised by the Aspen Global Innovators Institute and Niyel for 2023/2024 cohort. Therefore, I find it very necessary to acknowledge the role of the organisers, the assigned Mentor, Sabra Saleh, who made the journey worthwhile and joined others to review this work, Olumide Babalola, a seasoned digital rights and privacy lawyer in Nigeria, and the Advocacy Assembly for their generous funding and support of the project.

Internally, I thank members of the team, Ada Isamade and Cristina Longe for their research which contributed to the work.

PREFACE

DigiCivic Initiative (Registered as ADVOCATES FOR THE PROMOTION OF DIGITAL RIGHTS AND CIVIC INTERACTIONS INITIATIVE) is a non-governmental and public interest-driven organisation established to promote digital rights and the civic space, to organise public interest actions, advocacy and litigation for the promotion and preservation of digital rights and the civic space. It is positioned as an organization to raise awareness on the promotion of digital rights and the civic space, to empower members to take active roles in safeguarding digital rights and the civic space in compliance with the rule of law, to collaborate with other industry experts and organisations to create a world in which digital rights are respected and civic society can thrive, to engage in meaningful dialogues with government to foster an atmosphere where digital rights and the civic space are respected and protected, to empower members to act together to promote and uphold civic freedoms, to raise public awareness of the value of digital rights and civic space through film, online platforms, and other innovative tools, to organise public interest actions, including speaking engagements, press conferences, seminars, workshops, mentorship programs, peer review activities for the promotion of digital rights and the civic space, to encourage members in digital rights advocacy and litigation, and to promote active civic participation in good governance.

DIGICIVIC INITIATIVE in contributing to the legal development of digital rights in Nigeria developed this Manual as a free resource for training and building the capacity of Judges in Nigeria. The Manual sets out to describe the term digital

rights, identify various evolving terms in the digital space, identify emerging issues on digital rights, and applicable national, regional, and international frameworks for assisting Judges in analysing and arriving at informed decisions when confronted with digital rights matters.

INTRODUCTION

The Digital Rights and Civic Space Manual was developed as a resource for training Judges in Nigeria. It was a necessary tool because of prevailing evolutions of the internet with all its innovative changes.

The Manual became necessary because of the complexities of the online space. It aims to provide a resource on specific digital rights, such as the right to freedom of expression, assembly, association, and privacy.

Digital rights have become indispensable worldwide for people around the world to exercise and enjoy their fundamental rights in the digital space. Digital rights are online guaranteed human rights. In this sense, they focus on the right to access information, the right to free speech, the right to association, the right to freedom of assembly, and the right to privacy. The promotion and protection of these rights invariably leads to a more vibrant and thriving civic space both online and offline.

With the advancement in technology, information and communications technologies (ICT), there has been an expansion in the global market, health services, human interactions, transactions. Nigerian youths, reported as having the largest population of youth in the world, have not been excluded from this migration to the digital space.

More youths are leveraging on the increasing digitisation of the financial technology industry, which currently stands at 51%. This has led to increased e-commerce and a steady growth of online businesses. Therefore, it has become critical that the country apply the principles of openness, accountability, and participation in the governance of these digital platforms and ensure that the rights of those using the different technologies and platforms are protected.

Fresh challenges to digital rights and justice have also emerged with these new technologies. These issues include access to the internet to enjoy the several opportunities available, deprivation of access to the internet, access but restricted in circumstances leading to censorship or privacy matters, criminality and human rights violations by individuals, and so on.

However, these challenges must be tackled in compliance with the rule of law, due process and maintaining international human rights standards, which must be applied to all, and not deployed for the increased agency of intermediaries and non-state actors in obstructing the exercise of freedom of expression, political dissent and opposition state surveillance of media platforms and media rights activists perceived to be enemies of the State.

Thus, government and citizens have a role to play in ensuring that digital rights and the civic space are promoted and protected to actualize citizens' data protection, online privacy, freedom of expression online, online participation and assembly, internet governance, and regulation.

The Manual shall be a resource for training judicial officers in Nigeria. It is noted that for a better adjudication of cases involving digital rights, it is imperative that Judges in Nigeria be exposed as much as possible to all the relevant information and peculiarities required for them to make informed decisions on digital rights. This way, they would be equipped with a resource that provides an exhaustive appreciation of the digital space and how to balance rights to ensure that citizens fully enjoy their online rights and that the government performs their international obligations to promote, protect and fulfil online human rights.

Judges in Nigeria are not different from their counterparts adjudicating in the regional and international space, so there shouldn't be any gap in existence that differentiates the quality of their judgements from others. The judgements from Nigeria must be characterized by sound judicial reasoning, which should always reflect international human rights standards that show that the Judiciary has a full grasp of the law as well as the evolution of human rights in the digital space.

The Manual provides a broad description of digital rights, civic space, and international jurisprudence from the last decade that have shaped the space. It will reinforce efforts to address acute and unwarranted restrictions (including inter alia, undue obstruction, criminalization, and excessive use of force) on the online right to freedom of expression, freedom of association, freedom of assembly and privacy.

BACKGROUND

Digital rights, the rights to freedom of expression, freedom of association, freedom of assembly, and the strengthening of civic space are inextricably linked. They represent a combination of human rights that enable other rights. Among others, they enable individuals to express themselves collectively and participate in shaping their societies. The significance of these rights is that they advance human rights, the rule of law, democracy, peace, and sustainable development. A healthy and thriving civic space requires that these rights are protected, promoted and fulfilled by the government as well as the citizenry.

However, in Nigeria, there are strong restrictions on the civic space and media repression. This is evidenced by the consistent measures deployed over time and significantly by the executive arm of government during specific events of citizenry cohesion. Examples are The ENDSARS events of the evening of 20th October 2020 and morning of 21st October 2020 that occurred in Lekki Lagos, Nigeria, in which the agents of the Nigerian government, the Nigerian Army and the Nigeria Police shot sporadically at innocent, peaceful and unarmed citizens of Nigeria carrying out their guaranteed rights to freedom of assembly, association, movement and expressions in the form of a peaceful protest against police brutality in Nigeria. Another event was when the government, through the office of the Minister for Information, Lai Mohammed, shut down Twitter for 222 days. This was a direct attack not only on the civic space but on the rights of Nigerians, and Journalists from accessing and disseminating information.

In this light, Nigeria, like many countries, intensified attacks on the media, the major protagonists of freedom of expression. Members of the press are violently attacked with impunity and authorities continue to clamp down on the rights and freedoms of expression and information.

Physical violence is only one of the many threats facing media practitioners in Nigeria. According to the Press Attack Tracker of the Centre for Journalism Innovation and Development (CJID), over 1,033 attacks on journalists and media organizations in Nigeria have taken place in Nigeria. It recorded that there was a substantial increase in attacks against journalists between 2019-2023 with a total of 595 journalists attacked.

Many countries achieve the repression of information through insidious and unconscionable but completely legal means. They cloak their repression with the legitimacy of laws and policies. To perpetuate media censorship and deny citizens

vital information of public interest, security forces in countries like Nigeria use cybercrimes and terrorism laws to hound journalists under the guise of national security or other citizens in the pretext of the protection of reputation, protection of minors against abusive online contents, checking incidences of hate speeches, racial discriminatory messages on online platforms, privacy, intellectual property, etc.

The repression also comes in other forms, including Internet shutdowns and social media platform suspensions (e.g., the Twitter case in Nigeria), increased agency of intermediaries and non-state actors in obstructing the exercise of freedom of expression, and State surveillance of media rights activists perceived to be enemies of the State. Low-income governments, like Nigeria, stretch already-thin budgets even thinner to purchase modern surveillance technologies like Pegasus to monitor and intercept communications. The result is wanton State-sanctioned violence on journalists and other human rights defenders engaged in holding their governments accountable.

This issue has eaten deep into the fabric of society, in that the government keeps pushing for regulations and laws to regulate the press in an unprecedented manner.

In recent times, the government made moves to amend the Broadcasting Code of the National Broadcasting Commission (NBC), which seeks to regulate social media; the attempt to create a Media Certification Board to license journalists, the enactment of the Lawful Interception of Communication Regulations (enacted in 2019 by the Nigerian Communications Commission (NCC), which has also been used to monitor the movement of citizens, to track activities of civic actors online, intercept private communications, restrict online civic space, and limit the ability of civic space actors to organize, associate and assemble freely.

It is observed that these measures result in a chilling effect and create an environment of repression. As a result, members of the press refrain from spreading quality information or permit this on their platforms for fear of reprisal. This affects the rights of Nigerians to receive genuine information and also restricts them from imparting and freely sharing their opinions, associating over the space to engage and participate in the political arena, which are necessary for a healthy and thriving civic space- and ultimately the sustenance of democracy.

OBJECTIVES

The aim of the organization is to develop a comprehensive resource that will be used to train Judges in Nigeria, which will continue to be updated as the digital environment evolves. The integration of this manual into the judges' curriculum will form a foundational basis for judges to properly handle digital rights cases in Nigeria. This Manual will address the following:

1. A general introduction to digital rights and their intersection with the civic space
2. Digital rights key terms
3. International and regional frameworks for digital rights in Nigeria
4. Legal frameworks for digital rights in Nigeria
5. Basic digital rights issues and terms
6. An introduction to internet shutdowns
7. The concept of national security and digital rights
8. Online human rights violations
9. Additional jurisprudence on digital rights
10. The concept of national

MODULE ONE

A GENERAL INTRODUCTION OF DIGITAL RIGHTS AND THEIR INTERSECTION WITH THE CIVIC SPACE

The concept of digital rights emerged from the evolution of human relations beyond the physical environment, into a virtual one where discussion focuses on Internet rights, online or communication rights.

Digital rights are however a broad concept that recognises the use of different terms to mean different things. Digital as a term encompasses different meanings which could include online presence or internet, or mean technologies adopted offline, such as biometric data- facial recognition and fingerprint checking, etc. Digital could just simply be technologies that are not analogue.

Therefore, digital rights in the context of this Manual simply mean human rights that are facilitated through technology and the internet. It exposes our minds and thoughts to the unconventional understanding of human rights. Traditionally, human rights have focused on principles espoused in international documents like the UN Declaration of Human Rights of 1948 and definitions provided in other international and regional instruments such as the international covenant on civil and political rights, the African Charter on Human rights, etc.

However, the unprecedented shift of human existence to the internet space, a new and fast paced environment, makes it essential that these rights as we know and enjoy them offline are applied in the online space to regulate our behaviour and interactions in the online space. The internet continues to develop in a way that has opened up spaces for evolutions in the fields of education, health care, banking sector, entertainment industry, online marketing, online shopping, information, connectivity, job creation, research, obtaining public services, etc., while also exposing individuals to negative implications, such as, interference with people's privacy, virus and threats, identity theft, stalking, phishing, spreading fake news, trolling, and cybercrimes in general.

Definition

Digital rights are universal human rights promoted and protected in the online space. They are rights available for the protection of internet users especially as regards their ability to assemble and participate online with other internet users, freely express themselves and share their varying perspectives and views about governance as well as other social issues, and to do all these while ensuring that their privacy is safeguarded from any form of intrusions, whether by governments or other internet users.

It should be noted however that there are digital rights that can be exercised both offline and online, while there are those that cannot be exercised offline, for example, the right to be forgotten. This also means that there are rights that can only be exercised in the digital environment, facilitated through the internet, such as a complete erasure of an individual's data on a social media platform.

The World Economic Forum in 2015 described digital rights as basically human rights in the internet era.¹ It has also been described as fundamental human right in the digital environment.² They are human rights that are facilitated through the internet and technological developments.

The UN General Assembly Resolution dated 18 Dec. 2013 No. 68/167 "The Right to Privacy in the Digital Age" notes that the rapid pace of technological development enables people in all regions of the world to benefit from new information and communication technologies, while at the same time increasing the ability of governments, companies, and individuals to track, intercept and collect information that may violate or undermine human rights (especially the right to privacy). It is emphasized that the need to ensure public safety may justify the collection and protection of some confidential information, but states must ensure that their international human rights obligations are fully respected (Wong et al., 2021).³

According to the United Nations, the world's highest human rights body, digital rights are rights that exist online and are also available offline. They are human rights that operate online just as they do offline.⁴

¹ <https://www.weforum.org/agenda/2015/11/what-are-your-digital-rights-explainer/>

² <https://www.apc.org/en/news/coconet-what-are-digital-rights>

³ Wong, M.Y.H., Kwong, Y.H., & Chau, V.Y.W. (2021). Democracy, constitutional framework, and human rights: A comparison of Monaco, Tonga, Hong Kong, and Singapore. *International Journal of Law, Crime and Justice*, 64. <https://doi.org/10.1016/j.ijlcrj.2020.100438>

⁴ UN 2016 resolution A/HRC/32/L.20 of 30th June 2016)⁴ UN Human Rights Council, 'The promotion, protection and enjoyment of human rights on the Internet' A/HRC/32/L.20 (2016) at para 1 (accessible at: https://www.article19.org/data/files/Internet_Statement_Adopted.pdf

Digital Rights involve the exercise of the freedom to information, express opinions and ideas, disseminate information, access online safe space, access platforms for associating and assembly, enjoy safety and security, privacy and data protection, enjoy equality and freedom from all forms of discrimination, violence and surveillance.

Digital rights in this Manual thus focuses on the rights to freedom of expression, association and assembly, access to internet devices, rights and access to information, access to platforms (i.e. Facebook, Twitter, and more), online safe space, security and safety, privacy and data protection. All these are necessary for the promotion and protection of the civic space.

The civic space is not a farfetched idea. It is the environment that enables citizens of an open and democratic society to freely organize, communicate and share ideas without hindrances, to exercise their duties by engaging in the political, economic, social and cultural life for the advancement of the society.

It is simply the democratic environment that allows citizens to enjoy their rights to freedom of expression, association and assembly. These rights encompass other derivative rights, such as the right to a free and open internet. The civic space is a dynamic environment that exists to promote accountability, transparency, and in general help to put governments on their toes. It defends citizens' rights to information, expression and resolve for good governance.

The civic space is critical for the enjoyment of an open, secure and safe environment that is free from all acts of intimidation, harassment and reprisals, whether online or offline. An open and thriving civic space is vital for a healthy democracy, strong social justice, and to safeguard the rule of law.

According to the United Nations High Commissioner for Human Rights, *“If space exists for civil society to engage, there is a greater likelihood that all rights will be better protected. Conversely, the closing of civil society space, and threats and reprisals against civil society activists, are early warning signs of instability. Over time, policies that delegitimize, isolate and repress people calling for different approaches or legitimately claiming their rights can exacerbate frustrations and lead to instability or even conflict.”*

However, the civic space is constantly under pressure from repressive laws and there is an increased restriction on freedoms to express, participate, assemble and

associate. In recent times, the Nigerian government has realized the power wielded by its citizens in the civic space and continues to find ways to limit or totally remove this power in favour of the political few, the elites who have failed woefully to bring advancement to the country.

Citizens need to engage their governments positively to achieve better governance and their desired political environment. This is what the civic space promotes.

Where the civic space is suppressed or repressed, this will be to the detriment of citizens as governments and its institutions will drastically reduce their response to citizens' requests. This means that any restrictions on the civic space require conformity with the international human rights standards for safeguarding the civic space.

Therefore, digital rights are intertwined with civic space, and judges must be able to grasp the nuances fully to arrive at informed decisions whenever they are confronted with opposing arguments for or against any digital right.

MODULE TWO

DIGITAL RIGHTS KEY TERMS

Key Terms

Digital Rights- DR for the purpose of this Manual is strictly privacy, freedom of expression, freedom of association and freedom of assembly.

Digital Environment-This is a social space created through the interactions of one or more digital devices, such as computers, tablets or cellular phones, in which communications and information are exchanged and managed. It is a virtual environment involving the use of the internet, which includes components such as websites, cloud servers, search engines, social media outlets, mobile apps, audio and video, and other web-based resources.

Digital Equality- This simply means equal access to the internet, knowledge and skills to use of information and communication technologies for participation in the digital environment. This usually encompasses concepts such as, digital inclusion which involves access to affordable broadband Internet services, Internet-enabled devices, access to digital literacy training, quality technical support, and applications and online content designed to enable and encourage self-sufficiency, participation, and collaboration.

Digital literacy- This refers to the ability to live, use, create, interact, operate, and function in a digital environment where information and communication play critical roles through the increased use of digital technologies such as the internet, social media platforms, digital health services, etc.

Digital Identity- This is the information or data of external agents received and stored by a computer as a means of recognizing these agents in future interactions. These agents include individuals, organizations, applications, or devices. It could also be referred to as the virtual or online personality of an individual.

Encryption: This is a technology that is used for the protection of data. It is a system initiated to protect data from being stolen, changed, or compromised. This involves the encoding of data from plain text to unintelligent scribbles.

IP address: Internet Protocol address is a unique number that identifies a specific computer on the Internet and also provides information about the physical location of the network through which it is connecting.

Personal Information- It is also referred to as personal data. It is the information peculiar to a particular identifiable person. This includes distinguishing characteristics of the person, such as, the name, phone number, birthmarks, email address, medical records, etc.

Information Technologies- This is generally defined as the use of computers for the creation, storage, processing, management, transmission, or manipulation of any information.

DOS attack- Denial of service attack is a cyber-attack in which a malicious actor or perpetrator aims to shut down a machine or network, in order to render it inaccessible to its intended legitimate users by disrupting the device's normal operations or services.

DDOS- Distributed denial of service attack is a malicious activity that involves the disruption of normal traffic to on a server by flooding that server with internet traffic so that a system, such as an application or web, becomes unavailable to a legitimate end user.

DSL- Networking technology that provides broadband (high-speed) Internet connections over conventional telephone lines TCP/IP blocking transparent HTTP proxy.

MODULE THREE

INTERNATIONAL AND REGIONAL FRAMEWORKS FOR DIGITAL RIGHTS IN NIGERIA

The African Commission on Human and Peoples' Rights (ACHPR)⁵ has firmly settled that offline rights must also be protected online. This follows the affirmation by the UN Human Rights Council in resolutions adopted in 2012 and 2014⁶ that 'the same rights that people enjoy offline must also be protected online'.

There are several regional and international instruments that protect digital rights. These frameworks provide guidance for Judges and jurists in adjudicating on digital rights matters as described in this Manual.

The Universal Declaration of Human Rights (UDHR)⁷

This is regarded as the foremost instrument that paved way for the establishment of enforceable human rights treaties. The instrument though not binding was the first legal document to set out the fundamental human rights and provided a clear foundation for the adoption of human rights provisions in the world. It became the template from which many countries derived their constitutional and legal provisions. In certain situations, some countries incorporated specific provisions of the UDHR in their national laws. Some of these relevant digital rights include the right to life and human dignity; equality before the law; freedom of speech, assembly, and association; religious freedom and privacy.

One salient provision in the UDHR that is pertinent in the digital environment is the right to work. Article 23(1) of the UN Universal Declaration on Human Rights:

⁵⁵ ACHPR, 'Resolution on the right to freedom of information and expression on the internet in Africa', ACHPR/Res.362(LIX) (2016) (accessible at: <https://www.achpr.org/sessions/resolutions?id=374>)

⁶ RightDocs, *The promotion, protection and enjoyment of human rights on the Internet* (July 2014), available at: <https://www.right-docs.org/doc/a-hrc-res-26-13/#:~:text=Resolutions-.RES%2F26%2F13%20The%20promotion%2C%20protection%20and%20enjoyment%20of,human%20rights%20on%20the%20Internet.&text=1%20A%2FHRC%2F17%2F,%2F23%2F40%20and%20Corr.&text=policies%20that%20have%20the%20objecti ve.8>

⁷ Adopted by the UN General Assembly on 10 December 1948 (accessible at: <https://www.un.org/en/about-us/universal-declaration-of-human-rights>)

“Everyone has the right to work, to free choice of employment, to just and favourable conditions of work and to protection against unemployment.”

The International Covenant on Civil and Political Rights (ICCPR)⁸

This is a treaty that obligates signatories to respect, protect and preserve the civil and political rights of their citizens. The instrument provides binding obligations on member States of the UN who have ratified the law in their countries. Nigeria ratified the treaty on 29 July 1993

Some of these relevant digital rights include:

Article 3- The States Parties to the present Covenant undertake to ensure the equal right of men and women to the enjoyment of all civil and political rights set forth in the present Covenant.

Article 6 (1)- Every human being has the inherent right to life. This right shall be protected by law. No one shall be arbitrarily deprived of his life.

Article 7- No one shall be subjected to torture or to cruel, inhuman or degrading treatment or punishment.

Article 17 (1) & (2)- 1. No one shall be subjected to arbitrary or unlawful interference with his privacy, family, home or correspondence, nor to unlawful attacks on his honour and reputation. 2. Everyone has the right to the protection of the law against such interference or attacks.

Article 18 (1)- Everyone shall have the right to freedom of thought, conscience and religion. This right shall include freedom to have or to adopt a religion or belief of his choice, and freedom, either individually or in community with others and in public or private, to manifest his religion or belief in worship, observance, practice and teaching.

Article 19 (1) & (2)- Everyone shall have the right to hold opinions without interference. 2. Everyone shall have the right to freedom of expression; this right shall include freedom to seek, receive and impart information and ideas of all

⁸Adopted by the General Assembly of the United Nations on 19 December 1966 (Accessible at: https://treaties.un.org/pages/ViewDetails.aspx?src=TREATY&mtdsg_no=IV-4&chapter=4&clang=en)

kinds, regardless of frontiers, either orally, in writing or in print, in the form of art, or through any other media of his choice.

Article 21- The right of peaceful assembly shall be recognized. No restrictions may be placed on the exercise of this right other than those imposed in conformity with the law and which are necessary in a democratic society in the interests of national security or public safety, public order (ordre public), the protection of public health or morals or the protection of the rights and freedoms of others.

Article 22 (1) & (2)- Everyone shall have the right to freedom of association with others, including the right to form and join trade unions for the protection of his interests. 2. No restrictions may be placed on the exercise of this right other than those which are prescribed by law and which are necessary in a democratic society in the interests of national security or public safety, public order (ordre public), the protection of public health or morals or the protection of the rights and freedoms of others. This article shall not prevent the imposition of lawful restrictions on members of the armed forces and of the police in their exercise of this right.

Article 24 (1)- Every child shall have, without any discrimination as to race, colour, sex, language, religion, national or social origin, property or birth, the right to such measures of protection as are required by his status as a minor, on the part of his family, society and the State.

Article 25 (a) & (c)- Every citizen shall have the right and the opportunity, without any of the distinctions mentioned in article 2 and without unreasonable restrictions: (a) To take part in the conduct of public affairs, directly or through freely chosen representatives; (c) To have access, on general terms of equality, to public service in his country.

Article 26- All persons are equal before the law and are entitled without any discrimination to the equal protection of the law. In this respect, the law shall prohibit any discrimination and guarantee to all persons equal and effective protection against discrimination on any ground such as race, colour, sex, language, religion, political or other opinion, national or social origin, property, birth or other status.

International Covenant on Economic Social and Cultural Rights (ICESCR)⁹

⁹ Adopted by the General Assembly of the United Nations on 16 December 1966 (Accessible at https://treaties.un.org/doc/treaties/1976/01/19760103%2009-57%20pm/ch_iv_03.pdf)

This is one of the international instruments relevant to the digital environment. The treaty obligates state parties to ensure the equal right of men and women to the enjoyment of all economic, social and cultural rights. Nigeria ratified the treaty on 29 July 1993.

Some of these relevant digital rights include:

Article 6-The right to work, which includes the right of everyone to the opportunity to gain his living by work which he freely chooses or accepts, and will take appropriate steps to safeguard this right.¹⁰

Article 7- The right of everyone to the enjoyment of just and favourable conditions of work, which includes having a decent living for themselves and their families in accordance with the provisions of the present Covenant.

Article 8 (1)- The right of everyone to form trade unions and join the trade union of his choice, subject only to the rules of the organization concerned, for the promotion and protection of his economic and social interests. No restrictions may be placed on the exercise of this right other than those prescribed by law, and which are necessary in a democratic society in the interests of national security or public order or for the protection of the rights and freedoms of others...

Article 10 (3)- Special measures of protection and assistance should be taken on behalf of all children and young persons without any discrimination for reasons of parentage or other conditions. Children and young persons should be protected from economic and social exploitation. Their employment in work harmful to their morals or health or dangerous to life or likely to hamper their normal development should be punishable by law. States should also set age limits below which the paid employment of child labour should be prohibited and punishable by law.

Article 11 (1)- The States Parties to the present Covenant recognize the right of everyone to an adequate standard of living for himself and his family, including adequate food, clothing and housing, and to the continuous improvement of living conditions. The States Parties will take appropriate steps to ensure the realization

¹⁰ the International Covenant on Economic, Social and Cultural Rights (ICESCR) Article 6(1) of the International Covenant on Economic, Social and Cultural Rights (ICESCR): “*The States Parties to the present Covenant recognize the right to work, which includes the right of everyone to the opportunity to gain his living by work which he freely chooses or accepts and will take appropriate steps to safeguard this right.*”

of this right, recognizing to this effect the essential importance of international co-operation based on free consent.

Article 12 (1)- The States Parties to the present Covenant recognize the right of everyone to the enjoyment of the highest attainable standard of physical and mental health.

Article 13 (1)- The States Parties to the present Covenant recognize the right of everyone to education. They agree that education shall be directed to the full development of the human personality and the sense of its dignity, and shall strengthen the respect for human rights and fundamental freedoms. They further agree that education shall enable all persons to participate effectively in a free society, promote understanding, tolerance and friendship among all nations and all racial, ethnic or religious groups, and further the activities of the United Nations for the maintenance of peace.

Article 15- (1) (a) (b)- The States Parties to the present Covenant recognize the right of everyone: To take part in cultural life and to enjoy the benefits of scientific progress and its applications;

There are several resolutions, protocols and General comments adopted by the UN General Assembly and its treaty bodies to actualize the rights agreed upon by States in treaties and conventions. These relevant instruments are also important when considering digital rights and making decisions as to whether there have been violations. A few of these are listed as follows:

UN Human Rights Committee, General Comment No 27: Article 12: Freedom of Movement UN Doc CCPR/C/21/Rev.1/Add.9 (2 November 1999)

United Nations, Committee on Economic, Social and Cultural Rights – The Right to Work, General Comment No. 18, Doc No. E/C. 12/GC/186 February 2006

UN Human Rights Council, Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression UN Doc A/HRC/17/27 (2011)

UN Human Rights Committee, General Comment No 34: Article 19: Freedoms of opinion and expression UN Doc CCPR/C/GC/34 (12 September 2011),

UN Human Rights Council, Resolution 32/13 on the promotion, protection and enjoyment of human rights on the Internet UN Doc A/HRC/RES/32/13 (1 July 2016)

UN General Assembly, Resolution 53/144: Declaration on the Right and Responsibility of Individuals, Groups and Organs of Society to Promote and Protect Universally Recognized Human Rights and Fundamental Freedoms¹¹
UN Special Rapporteur on Freedom of Opinion and Expression, OSCE Representative on Freedom of the Media, OAS Special Rapporteur on Freedom of Expression and ACHPR Special Rapporteur on Freedom of Expression and Access to Information¹²

Resolutions On the Right to Privacy in The Digital Age¹³

This resolution anchored on the principles of the Charter of the United Nations, the human rights and fundamental freedoms enshrined in the Universal Declaration of Human Rights and other relevant international human rights treaties, including the International Covenant on Civil and Political Rights, the International Covenant on Economic, Social and Cultural Rights, as well as the Vienna Declaration and Programme of Action; was adopted following the Covid-19 pandemic.

The resolution reaffirms the fundamental importance of the right to privacy and renews international commitment to ending all global abuses and violations of the right. It stresses the need for States to ensure that national security and public health measures, including the use of technology to monitor and contain the spread of infectious diseases, are in full compliance with the obligations of States under international human rights law and adhere to the principles of lawfulness, legality, legitimacy with regard to the aim pursued, necessity and proportionality and the need to protect human rights, including the right to privacy, and personal data in the response to health or other emergencies.

It emphasized that:

“unlawful or arbitrary surveillance and/or interception of communications, as well as the unlawful or arbitrary collection of personal data, hacking and the unlawful use of biometric technologies, as highly intrusive acts, violate the right to privacy, can interfere with the right to freedom of expression and to hold opinions without interference, the right to freedom of peaceful assembly and association and the right to freedom of

¹¹ UN Doc A/RES/53/144 (8 March 1999)

¹² *Joint Declaration on Freedom of Expression and the Internet* (1 June 2011), available at: <https://www.osce.org/files/f/documents/e/9/78309.pdf>

¹³ Resolution 75/176 was adopted by consensus at the U.N. General Assembly on 16 December 2020 following the COVID-19 pandemic. (Accessible at <https://documents.un.org/doc/undoc/gen/n20/371/75/pdf/n2037175.pdf?token=2iY6McOjgOoG8m7Wnm&fe=true>)

religion or belief and may contradict the tenets of a democratic society, including when undertaken extraterritorially or on a mass scale”

It stresses the interdependence and indivisibility of the right to privacy with other fundamental human rights, including freedom of opinion and expression, peaceful assembly and association, and equality and non-discrimination.

This very important resolution for the enjoyment of digital rights also emphasized.

“that, in the digital age, technical solutions to secure and to protect the confidentiality of digital communications, including measures for encryption, pseudonymization and anonymity, are important to ensure the enjoyment of human rights, in particular the rights to privacy, to freedom of opinion and expression and to freedom of peaceful assembly and association, and recognizing that States should refrain from employing unlawful or arbitrary surveillance techniques, which may include forms of hacking, ...”

The Resolution called upon States to among others, respect and protect the right to privacy, including in the context of digital communications; take measures to put an end to violations of the right to privacy and to create the conditions to prevent such violations, including by ensuring that relevant national legislation complies with their obligations under international human rights law; review, on a regular basis, their procedures, practices and legislation regarding the surveillance of communications, their interception and the collection of personal data, including mass surveillance, interception and collection, as well as regarding the use of profiling, automated decision-making, machine learning and biometric technologies, with a view to upholding the right to privacy by ensuring the full and effective implementation of all their obligations under international human rights law; establish or maintain existing independent, effective, adequately resourced and impartial judicial, administrative and/or parliamentary domestic oversight mechanisms capable of ensuring transparency, as appropriate, and accountability for State surveillance of communications, their interception and the collection of personal data; provide individuals whose right to privacy has been violated by unlawful or arbitrary surveillance with access to an effective remedy, consistent with international human rights obligations; etc.

General comment No. 25 (2021) on children’s rights in relation to the digital environment¹⁴

This general comment anchored on the United Nations Convention on the Rights of the Child (UNCRC),¹⁵ recognises that the rights of children now apply online as they do offline. The Committee on the rights of the child provides guidance to State Parties on the interpretation of certain articles of the CRC and on relevant legislation, policy and other measures designed to ensure full compliance with their obligations under the Convention. It clarifies to State the peculiarities of the digital environment for achieving children’s civil rights and freedoms, including rights to privacy, non-discrimination, protection, education, play, and more. It explains the accountability of the state as the primary duty bearer in ensuring that the provisions of the UN Convention on the Rights of the Child (UNCRC) are adhered to, measures to take to implement the online rights of children, and States’ obligations to ensure that all entities whose activities impact children within their jurisdiction meet their responsibilities regarding children’s rights.

The Committee emphasizes that the rights of every child must be respected, protected and fulfilled in the digital environment. It encourages states to disseminate information and conduct sensitization on children’s rights in the digital environment, and facilitate educational programs for children, parents, caregivers, the public, and policymakers to improve their knowledge of children’s rights in relation to the opportunities and risks associated with digital products and services.

The comment recognises that the digital environment is constantly evolving and expanding, encompassing information and communications technologies, including digital networks, content, services and applications, connected devices and environments, virtual and augmented reality, artificial intelligence, robotics, automated systems, algorithms and data analytics, biometrics and implant technology, and that societies have progressively come to rely upon these digital technologies as the digital environment becomes increasingly important across most aspects of children’s lives, including during times of crisis, as societal functions, including education, government services and commerce.

¹⁴ The General Comment 25 was adopted by the Committee on the Rights of a Child on 2nd March 2021 and launched on the 24th of March 2021. (Accessible at <https://www.unicef.org/bulgaria/en/media/10596/file>)

¹⁵ Resolution 44/25 is a legally-binding international agreement setting out the civil, political, economic, social and cultural rights of every child, regardless of their race, religion or abilities which was adopted by the United Nations General Assembly on 20 November 1989 (Accessible at <https://www.ohchr.org/en/instruments-mechanisms/instruments/convention-rights-child>). Nigeria ratified the Convention on the Rights of the Child (CRC) on 19th April 1991.

It also recognises that the digital environment affords new opportunities for the realization of children’s rights, which may be vital for children’s life and survival, such as, providing a unique opportunity for children to realize the right to access to information. In this regard, the Committee calls on States parties to *“ensure that children have access to information in the digital environment and that the exercise of that right is restricted only when it is provided by law and is necessary for the purposes stipulated in article 13 of the Convention.”*

The comment also emphasizes that the digital environment poses risks of violation or abuse to children as it can include gender-stereotyped, discriminatory, racist, violent, pornographic and exploitative information, as well as false narratives, misinformation and disinformation and information encouraging children to engage in unlawful or harmful activities; and so *“States parties should protect children from harmful and untrustworthy content and ensure that relevant businesses and other providers of digital content develop and implement guidelines to enable children to safely access diverse content, recognizing children’s rights to information and freedom of expression, while protecting them from such harmful material in accordance with their rights and evolving capacities...”*

Summarily, the comment calls on States to:

Adopt and properly resource the implementation of comprehensive child online safety policies based on children’s rights to access the digital world in ways that are safe and secure.

Ensure businesses with control of online environments conduct comprehensive human rights and environmental due diligence that integrate child rights. Actions must assess impacts across operations and value chains, establish saliency, and lead to changing practices to address risks to children’s rights in the digital environment.

Ensure Big Tech platforms disclose adequate information about how they conduct human rights due diligence, moderate online content, test and deploy algorithmic systems, and use of personal data.

The African Charter on Human and People’s Rights (ACHPR)¹⁶

This is one of the relevant laws on digital rights in Africa. The African Charter laid out a range of rights and duties that should always be respected, protected and preserved. It established the African Commission to oversee its implementation and later on June 1998 the OAU adopted a protocol to establish African Court on Human and Peoples’ Rights. The African Charter is a set of rules, called Articles,

¹⁶ African Commission on Human and People’s Rights, African Charter on Human and People’s Rights of Kenya on 27 June 1981 (accessible at: https://au.int/sites/default/files/treaties/36390-treaty-0011_-_african_charter_on_human_and_peoples_rights_e.pdf)

guaranteeing certain human rights and fundamental freedoms for individuals. It also guarantees certain rights of entire peoples. The majority of the human rights and fundamental freedoms in the African Charter are the same as those contained in international human rights treaties adopted by the UN. Many African states have ratified these treaties and have therefore agreed to be bound by their provisions.

The African Charter is similar to two other regional treaty-based systems established to promote and protect human rights: the European Convention for the Protection of Human Rights and Fundamental Freedoms (1953), the American Convention on Human Rights (1978).¹⁷ Like those systems, it set out particular fundamental rights in line with the provisions of the UDHR and recognises salient rights that are relevant for the digital environment such as the right to freedom of expression in Article 9. Nigeria ratified the treaty on 22 JUNE 1983. Some of the relevant digital rights include:

Article 3 1. Every individual shall be equal before the law. 2. Every individual shall be entitled to equal protection of the law.

Article 4 Human beings are inviolable. Every human being shall be entitled to respect for his life and the integrity of his person. No one may be arbitrarily deprived of this right.

Article 5 Every individual shall have the right to the respect of the dignity inherent in a human being and to the recognition of his legal status. All forms of exploitation and degradation of man particularly slavery, slave trade, torture, cruel, inhuman or degrading punishment and treatment shall be prohibited.

Article 8 Freedom of conscience, the profession and free practice of religion shall be guaranteed. No one may, subject to law and order, be submitted to measures restricting the exercise of these freedoms.

Article 9 1. Every individual shall have the right to receive information. 2. Every individual shall have the right to express and disseminate his opinions within the law.

Article 10 1. Every individual shall have the right to free association provided that

¹⁷ American Convention on Human Rights (adopted 22 November 1969, entered into force 18 July 1978) 1144 UNTS 123

he abides by the law. 2. Subject to the obligation of solidarity provided for in 29 no one may be compelled to join an association.

Article 11 Every individual shall have the right to assemble freely with others. The exercise of this right shall be subject only to necessary restrictions provided for by law in particular those enacted in the interest of national security, the safety, health, ethics and rights and freedoms of others.

Article 13 1. Every citizen shall have the right to participate freely in the government of his country, either directly or through freely chosen representatives in accordance with the provisions of the law. 2. Every citizen shall have the right of equal access to the public service of his country. 3. Every individual shall have the right of access to public property and services in strict equality of all persons before the law.

Article 15 Every individual shall have the right to work under equitable and satisfactory conditions, and shall receive equal pay for equal work.

Article 16 1. Every individual shall have the right to enjoy the best attainable state of physical and mental health. 2. States Parties to the present Charter shall take the necessary measures to protect the health of their people and to ensure that they receive medical attention when they are sick.

Article 17 1. Every individual shall have the right to education. 2. Every individual may freely, take part in the cultural life of his community. 3. The promotion and protection of morals and traditional values recognized by the community shall be the duty of the State.

Article 22 1. All peoples shall have the right to their economic, social and cultural development with due regard to their freedom and identity and in the equal enjoyment of the common heritage of mankind. 2. States shall have the duty, individually or collectively, to ensure the exercise of the right to development.

Article 24 All peoples shall have the right to a general satisfactory environment favorable to their development.

African Commission on Human and People's Rights (ACHPR)

The African Charter established the ACHPR as the primary body for the promotion and protection of human rights on the continent. The body was charged with three

major functions: the protection of human and peoples' rights, the promotion of human and peoples' rights, and the interpretation of the African Charter on Human and Peoples' Rights.

Over the years, the African Commission on Human and People's Rights (ACHPR) has developed several instruments and resources covering issues related to the protection of human rights and freedoms in the digital space. The Commission has continued to play prominent role in promoting digital rights and the right to access the internet through its resolutions and protocols.

Protocols address additional rights and obligations to a treaty. They are also instruments that provide specific substantive obligations that implement the general objectives of a previous framework or umbrella convention. Usually, ratifying of a treaty will normally involve the ratification of a Protocol (whether an optional protocol or one based on a Framework Treaty).

Resolutions are very significant in the human rights context and have helped to shape the implementation of international and regional instruments. The ACHPR resolutions represent the position of the Commission on particular human rights issues and situations. These resolutions could be enunciated to address either country specific or thematic human rights issues and can lead to actions that help to resolve the issues.

The Commission emphasizes that freedom of expression and access to information are fundamental human rights guaranteed by Article 9 of the African Charter, and that those rights are also affirmed in the African Charter on the Rights and Welfare of the Child, the Protocol to the African Charter on Human and Peoples' Rights on the Rights of Persons with Disabilities in Africa, the African Union Convention on Preventing and Combating Corruption, the African Charter on Statistics, the African Youth Charter, the African Charter on Democracy, Elections and Governance, the African Charter on Values and Principles of Public Service and Administration, and the Protocol to the African Charter on Human and Peoples' Rights on the Rights of Women in Africa.

Some of the details of the Commissions resolutions in this regard are described as follows:

The African Platform on Access to Information Declaration of 2011.

This declaration was adopted in 2011 following the commissioning of a Working Group¹⁸ African Platform on Access to information (APAI) comprising of relevant stakeholders and experts on access to information in Africa. The group convened in Cape Town with representatives from African governments, African Union Commission, UNESCO, the UN Special Rapporteur on Freedom of Expression an Opinion, the Special Rapporteur on Freedom of Expression and Information in Africa, human rights, civil society organizations and the media and then adopted the APAI declaration, emphasizing the centrality of access to information and its importance in the promotion and protection of fundamental human rights and in advancing democratic values and accountability.

The Commission has also adopted relevant soft law standards important to digital rights promotion and protection, such as the Model Law on Access to Information for Africa of 2013; the Guidelines on Access to Information and Elections in Africa of 2017; the African Union Convention on Cyber Security and Personal Data Protection.

The Resolution on the right to freedom of information and expression on the internet 2016

The Resolution on the right to freedom of information and expression on the internet¹⁹ calls on countries to guarantee, respect, and protect citizens' right to freedom of information and expression through access to internet services. The Resolution mandates African States to respect and protect freedom of expression on the Internet including by adopting legislative measures. This Declaration on Internet Rights and Freedoms was adopted to promote human rights standards and principles of openness in Internet policy formulation and implementation in Africa.

¹⁸ Statement of the Working Group on Access to Information on African at the 51st Session of the African Commission on Human and Peoples' Rights Banjul April 2012 (Accessible at <https://achpr.au.int/index.php/sw/node/1071>)

¹⁹ African Commission on Human and Peoples' Rights [ACHPR]. (4th November 2016). Resolution on the Right to Freedom of Information and Expression on the Internet in Africa - ACHPR/Res362(LIX)2016 (Accessible at <https://achpr.au.int/en/adopted-resolutions/362-resolution-right-freedom-information-and-expression-internet>)

The commission by the resolution spotlighted the issues regarding “emerging practice of State Parties of interrupting or limiting access to telecommunication services such as the Internet, social media and messaging services, increasingly during elections” and stated the importance of having a “clear and comprehensive principles are established to guide the promotion and protection of human rights in the online environment”²⁰

The Commission took note of the African Declaration on Internet Rights and Freedoms, which highlighted 13 key principles to be promoted and respected in the digital space, such as freedom of expression, freedom of peaceful assembly and association, gender equality, privacy and data protection. The declaration calls on African governments to ratify and give effect to all relevant international and regional human rights treaties related to the protection of human rights on the internet, as well as to ensure that legal, regulatory, and policy frameworks for the protection of these rights are in full compliance with international standards and best practices. Civil society groups are encouraged to include identified abuses of internet rights and freedoms in their reports to international human rights bodies and mechanisms and to communicate with the Special Rapporteur on Freedom of Expression and Access to Information in Africa on measures to uphold freedom of expression in relation to the internet. A relevant text of the resolution is reproduced below:

“The Commission:

1. Calls on States Parties to respect and take legislative and other measures to guarantee, respect and protect citizen’s right to freedom of information and expression through access to Internet services;
2. Urges African citizens to exercise their right to freedom of information and expression in the Internet responsibly;
3. Encourages the Special Rapporteur of Freedom of Expression and Access to Information in Africa to take note of developments in the Internet age during the revision of the Declaration of Principles on Freedom of Expression in Africa, which was adopted by the Commission by 2002;
4. Urges State Parties, civil society and other stakeholders to collaborate with the Special Rapporteur by contributing to the process of revising the Declaration to consider Internet rights.”

Also at the 68th session of the African Commission on Human and Peoples’ Rights (ACHPR), which held virtually from 14 April to 4 May 2021, digital rights was emphasized.

²⁰ Resolution on the Right to Freedom of Information and Expression on the Internet in Africa - ACHPR/Res.362(LIX)2016 (Accessible at <https://achpr.au.int/en/adopted-resolutions/362-resolution-right-freedom-information-and-expression-internet>)

The Declaration of Principles on Freedom of Expression and Access to Information in Africa

The Commission adopted a Declaration of Principles on Freedom of Expression and Access to Information in Africa in 2019.²¹ The Commission emphasized the importance of freedom of expression and access to information as fundamental rights protected under the African Charter and other international human rights laws and standards. The Commission stated unequivocally that the respect, protection and fulfilment of the rights freedom of expression and access to information are crucial and indispensable for the free development of the human person, the creation and nurturing of democratic societies and for enabling the exercise of other rights.” Amongst several principles, it stated that media diversity and pluralism is essential for democracy, and “State or private monopoly over print, broadcast and online media is not compatible with the right to freedom of expression.”

These principles accentuate subjects on internet access, freedom of expression online, the right to anonymity, and the right to privacy and data protection in the digital space.

In summary, the declaration calls on State parties to do as follows:

- a. Adopt laws, policies, and other measures to provide universal, equitable, affordable, and meaningful access to the internet without discrimination.
- b. Not to interfere with the right of individuals to seek, receive, and impart information through any means of communication and digital technologies. This means refraining from measures such as the removal, blocking, or filtering of content unless such interference is justifiable and compatible with international human rights law and standards.
- c. Not to engage in or support any disruption of access to the internet and other digital technologies for segments of the public or an entire population,

²¹ Principles on Freedom of Expression and Access to Information in Africa was adopted by the African Commission during its 65th Ordinary Session held from 21 October to 10 November 2019 in Banjul, The Gambia. (Accessible at <https://achpr.au.int/en/node/902>). See also African Commission on Human and Peoples’ Rights, *Declaration of Principles on Freedom of Expression in Africa*, ACHPR/Res.62 (XXXII) 02 (23 October 2002), Principle II (2)

- d. Not to require internet intermediaries to proactively monitor content which they have not authored or otherwise modified.
- e. Not to adopt laws or other measures prohibiting or weakening encryption, including backdoors, key escrows, and data localisation requirements unless such measures are justifiable and compatible with international human rights law and standards.
- f. To only engage in targeted communication surveillance that is authorised by law, conforms with international human rights law and standards, and is premised on the specific and reasonable suspicion that a serious crime has been or is being carried out or for any other legitimate aim.

Resolution on the Protection of Women Against Digital Violence in Africa²²

This is a resolution adopted in 2022 on the protection of women against digital violence in Africa. The resolution calls on states to adopt or review legislation to combat digital violence against women and facilitate women's access to education in digital technology domains. The Commission recognised that "online violence manifests in different ways to include cyberstalking, unsolicited, sexually explicit content, doxing (sharing of personal information online), cyber-bulling and the non-consensual sharing of intimate images" and raised concerns "that women who access the internet are constantly at the risk of violence and that majority of women who access the internet have been subjected to some form of harassment while States continue to have gaps in their legal framework to protect women against digital violence"

The Commission therefore called on States to:

1. Review/adopt legislation that aims at combating all forms of digital violence, and expanding the definition of gender-based violence to include digital violence against women including cyber-harassment, cyberstalking, sexist hate speech amongst other ICT-related violations;
2. Undertake research on digital violence against women. This research should include studies and the adjustment of crime statistics on digital violence against women to identify legislative and non-legislative needs;
3. Undertake awareness-raising programmes which target boys and men, as well as campaigns involving all relevant stakeholders. These programmes should address the root causes of digital violence against women within the general context of gender-based violence in order to bring about changes in social and cultural attitudes and remove gender norms and stereotypes, while promoting the respect of fundamental rights in the online space, with special regard to social media platforms;

²² Resolution on the Protection of Women Against Digital Violence in Africa - ACHPR/Res. 522 (LXXII) 2022 (Accessible at <https://achpr.au.int/en/adopted-resolutions/522-resolution-protection-women-against-digital-violence-africa-achpr>)

4. Facilitate women's access to education in digital technology domains in order to remove the digital gender gap, and ensure gender diversity in the tech sector;
5. Undertake mandatory and continuous training for practitioners and professionals dealing with victims of digital violence including law enforcement authorities, social and child healthcare staff, criminal justice actors and members of the Judiciary;
6. Ensure and facilitate effective cooperation between law enforcement authorities and service providers with regards to the identification of perpetrators and gathering of evidence, which should be in full compliance with fundamental rights and freedoms and data protection rules.
7. Implement victim friendly and gender-sensitive policies when handling cases of digital violence against women;
8. Undertake measures to safeguard women journalists from digital violence, including gender-sensitive media literacy and digital security training;
9. Repeal vague and overly wide laws on surveillance as they contribute to the existing vulnerability of female journalists.

Resolution on the deployment of mass and unlawful targeted communication surveillance and its impact on human rights in Africa²³

At its 77th Ordinary Session which held from 20 October to 9 November 2023 in Arusha, Tanzania, the ACHPR adopted Resolution 573 to address the deployment of mass and unlawful targeted communication surveillance and its impact on human rights in Africa. This resolution recognised the importance of human rights protection in an increasingly interconnected world, particularly the need to safeguard internet access, privacy rights and data protection in the face of evolving technological advancements.

It should be noted that states can have legitimate interests for pursuing specific or targeted surveillance in response to issues of public concern, including addressing serious and organized crime and national security threats, such as cyberterrorism, radicalization and trafficking.

However, States must exercise powers within their international and regional obligations to protect, promote and fulfil human rights; and this requires that States should ensure a balance, for instance, between legitimate security concerns and the protection of privacy rights. At every point in time, States are encouraged to adopt a measure that is proportionate to the legitimate interest they intend to protect. Measures must be implemented in good faith to give effect to their obligations and

²³ Resolution on the deployment of mass and unlawful targeted communication surveillance and its impact on human rights in Africa - ACHPR/Res.573 (LXXVII) 2023 (Accessible at <https://achpr.au.int/en/adopted-resolutions/573-resolution-deployment-mass-and-unlawful-targeted-communication>)

commitment to the promotion and protection of human rights especially in the use of modern technologies.

The Commission affirmed Articles 2, 9, 10, 11 of the African Charter “on the rights of all peoples to enjoy the rights and freedoms guaranteed in the African Charter without distinction including the rights to receive information, to express and disseminate opinions, for freedom of association and assembly within the confines of the law,”

The resolution drew its essence from the provisions of the Declaration of Principles on Freedom of Expression and Access to Information in Africa, which in Principle 5 provides that “the same rights that people have offline should be protected online, in accordance with international human rights law and standards”; and the Resolution on the Right to Freedom of Information and Expression on the Internet in Africa, which recognise the right to privacy, confidentiality of communications, and the protection of personal information.

The resolution addresses the increasing use of mass surveillance and unlawful targeted surveillance by governments in Africa, which have posed huge threats to human rights defenders, journalists, political opponents, and ultimately democracy and the rule of law.

The resolution highlighted Principle 41 of the Declaration which provides that “*States should only engage in targeted surveillance in conformity with international human rights law and ensure that any law authorizing targeted communication surveillance provides adequate safeguards for the right to privacy,*” and Principle 42(7) which provides that “*every individual shall have legal recourse to effective remedies in relation to the violation of their privacy and the unlawful processing of their personal information*”

The Commission therefore called on States to:

- i. Ensure that all restrictions on the rights to privacy and other fundamental freedoms, such as freedom of expression, freedom of association and freedom of assembly, are necessary and proportionate, and in line with the provisions of international human rights law and standards;
- ii. Align approaches on the regulation of communication surveillance with relevant international human rights law and standards, considering safeguards such as the requirement for prior authorization by an independent and impartial judicial authority and the need for effective monitoring and regular review by independent oversight mechanisms;

- iii. Only engage in targeted communication surveillance that is authorized by law, which conforms with international human rights law and standards, and premised on reasonable suspicion that a serious crime has been or is being carried out;
- iv. Promote and encourage the use of privacy-enhancing technologies and desist from adopting laws or other measures prohibiting or weakening encryption, including backdoors, key escrows and data localization requirements, unless such measures are justifiable and compatible with international human rights law and standards;
- v. Ensure that victims of violations arising from arbitrary surveillance measures have access to effective remedies and take specific measures to investigate and prosecute cases of illegal and indiscriminate surveillance.

Other relevant resolutions for making informed decisions on digital rights are as follows:

Resolution on the need to undertake a study to assess the level of compliance of national legislations with the Guidelines on Freedom of Association and Assembly in Africa - ACHPR/Res.571 (LXXVII) 2023

Resolution on the Need to Protect Civic Space, Freedom of Association and Assembly in Africa - ACHPR/Res.569 (LXXVII) 2023

Resolution on the need to undertake a Study on human and peoples' rights and artificial intelligence (AI), robotics and other new and emerging technologies in Africa - ACHPR/Res. 473 (EXT.OS/ XXXI) 2021

Resolution on the need to protect civic space and freedom of association and assembly - ACHPR/Res. 475 (EXT.OS/ XXXI) 2021

Resolution on the Safety of Journalists and Media Practitioners in Africa.

African Union Convention on Cyber Security And Personal Data Protection

This Convention, popularly referred to as the Malabo Convention²⁴, was adopted in 2014 to establish a framework for cyber-security and personal data protection and mandated member States to develop legal frameworks for the protection of personal data, the promotion of cybersecurity, the combating of cybercrime, and standards for e-commerce. The document which came into force on 8 June 2023, nine years after its adoption, addresses electronic transactions, provisions relating to data protection, e-transactions, cybercrimes and cybersecurity. It attempts to promote and harmonise legislation in the area of data protection policies in Africa

²⁴ Adopted in Malabo on the (accessible at: https://au.int/sites/default/files/treaties/29560-treaty-0048_-_african_union_convention_on_cyber_security_and_personal_data_protection_e.pdf)

by actualizing digital rights, mainly data protection, privacy and internet freedom, e-transactions, cybercrimes and cybersecurity in Africa.

The Convention criminalizes a broad range of cyber activities, including hacking, cyber fraud, and identity theft. It also establishes procedures for investigating and prosecuting cybercrime, including international cooperation between African countries. The Convention also recognises the right to privacy and provides a framework for protecting personal data. It mandates countries that adopt the Convention to establish data protection authorities and ensure that personal data is collected, processed, and stored securely.

It defines key terms such as child pornography, data subject, information, processing of personal data, racism and xenophobia in information and telecommunication technologies, Interconnection of personal data, encryption, etc. The provisions relating to electronic transactions are contained in Chapter I, data protection is contained in Chapter II (and contain the conditions for the lawful processing of personal information, as well as the rights afforded to data subjects), and chapter III addresses promoting cyber security and combatting cybercrime.

The convention identified major issues affecting the development of ecommerce in Africa to be of a security nature and listed them to include the absence of specific legal rules that protect consumers, intellectual property rights, personal data and information systems; The rules applicable to cryptology devices and services; etc. Article 13 of the Convention identifies six principles relating to data protection: Consent and legitimacy; Lawful and fair processing; Purpose, relevance and retention of data; Accuracy of data over its lifespan; Transparency of processing; and Confidentiality and security of personal data

However, the Convention is not yet applicable in Nigeria. It must first acquire the force of law in Nigeria through the domestication provision contained in Section 12 of the 1999 Constitution of the Federal Republic of Nigeria (as amended) which requires the National Assembly to enact the convention into a law enforceable in Nigeria.

On the Sub regional level, the Economic Community of West African States (ECOWAS) has an act on personal data protection adopted in 2010²⁵,

²⁵ Economic Community of West African States [ECOWAS] Supplementary Act A/SA. 1/01/10 on Personal Data Protection within ECOWAS of 16 February 2010 (Accessible at <https://ccdcoe.org/uploads/2018/10/ECOWAS-100216-PersonalDataProtection.pdf>)

The Supplementary Act on Personal Data protection within ECOWAS

The Economic Community of West African States (ECOWAS) is a 15-member regional group aimed at promoting economic integration in several fields of activity among the constituent countries. The group adopted this Act in 2010 to address the legal vacuum on the protection of personal data generated by the use of the internet and to harmonise legal frameworks in this regard.

The Act stipulates the content of data privacy laws: the scope of the Act, basic concepts, data processing, data subject rights, cross-border data transfers and localization, etc. It defines personal data processing and other terms in respect of data protection, such as sensitive data, personal data, health data, data subject, etc. It enjoins member states to develop national legal frameworks for the protection of data and privacy and to establish data protection authorities (DPA). It states that the Act shall be annexed to the ECOWAS Treaty²⁶ and shall be an integral part of it (Article 48 of the Act) and is legally binding on manner states who are to implement the Act within two years of its adoption. Each member state is required to establish its own data protection authority that must be independent and responsible for ensuring that personal data is processed in compliance with the provisions of the Act.²⁷ It also outlined the requirements for the DPA, that must not be members of government, or business executives or own shares in businesses in the information or telecommunications sector.²⁸ In particular, the data protection authority must ensure that ICTs do not constitute a threat to public liberties and privacy²⁹

Article 19 provides that the data protection authority shall, among other things, inform data subjects and data controllers of their rights and obligations; respond to all requests for an opinion relating to processing of personal data; authorise the processing of files in certain cases, especially sensitive files; examine the prerequisite conditions for implementing personal data processing; receive claims, petitions and complaints and inform data subjects of actions taken; immediately inform the judicial authority of certain types of offences which it may gain knowledge; carry out verifications of any processing of personal data; impose

²⁶ ECOWAS Treaty of 28 May 1975 adopted in Lagos, Nigeria and revised in Cotonou, Benin Republic in July 1993.

²⁷ Article 14(2) of the Act

²⁸ Article 16 of the Act

²⁹ Article 19 of the Act

administrative and financial sanctions on controllers; update a register of personal data processing and make it available to the public; provide advice; authorise cross-border transfers of personal data; recommend improvements to the data processing legislative and regulatory framework; set up mechanisms for cooperation with third-party data protection authorities; participate in international negotiations concerning the protection of personal data; and draft activity reports.

In this regard, some member states have passed the relevant laws, in some cases titled the data protection act, while some have not. Nigeria passed the Data Protection Act 2023, while countries like Togo, the Gambia, Guinea Bissau, Sierra Leone and Liberia are yet to pass laws to implement the ECOWAS Supplementary Act.

MODULE FOUR

LEGAL FRAMEWORK FOR DIGITAL RIGHTS IN NIGERIA

The Constitutional framework for digital rights in Nigeria is basically found in Chapter IV of the 1999 Constitution³⁰ of the Federal Republic of Nigeria (As Amended).

The Nigerian Constitution provides Nigerian citizens with the fundamental right to privacy, freedom of expression (access to information and expressing opinion), freedom of association and assembly.

Section 22 provides that “The press, radio, television and other agencies of the mass media shall at all times be free to uphold the fundamental objectives contained in this chapter and uphold the responsibility and accountability of the Government to the people”.

Section 37 The section guarantees privacy protections to citizens in their homes, correspondence, telephone conversations and telegraphic communications. However, the Constitution did not define the scope of privacy or contained detailed privacy provisions.

38. (1) Every person shall be entitled to freedom of thought, conscience and religion, including freedom to change his religion or belief, and freedom (either alone or in community with others, and in public or in private) to manifest and propagate his religion or belief in worship, teaching, practice and observance.

39. (1) Every person shall be entitled to freedom of expression, including freedom to hold opinions and to receive and impart ideas and information without interference.

(2) Without prejudice to the generality of subsection (1) of this section, every person shall be entitled to own, establish and operate any medium for the dissemination of information, ideas and opinions...

³⁰ Cap. C.23 Laws of the Federation of **Nigeria**, 2004 available at National Library of Nigeria <https://nigeriareposit.nln.gov.ng/server/api/core/bitstreams/b62fb209-2716-48c4-b277-f684ca18d29d/content>

40. Every person shall be entitled to assemble freely and associate with other persons, and in particular he may form or belong to any political party, trade union or any other association for the protection of his interests...

42. (1) A citizen of Nigeria of a particular community, ethnic group, place of origin, sex, religion or political opinion shall not, by reason only that he is such a person:

(a) be subjected either expressly by, or in the practical application of, any law in force in Nigeria or any executive or administrative action of the government, to disabilities or restrictions to which citizens of Nigeria of other communities, ethnic groups, places of origin, sex, religions or political opinions are not made subject; or

(b) be accorded either expressly by, or in the practical application of, any law in force in Nigeria or any such executive or administrative action, any privilege or advantage that is not accorded to citizens of Nigeria of other communities, ethnic groups, places of origin, sex, religions or political opinions.

OTHER NATIONAL FRAMEWORKS FOR DIGITAL RIGHTS IN NIGERIA

Legislations on right to privacy in Nigeria.

1. Nigeria Data protection Act 2023

The Nigeria Data Protection Act 2023 (NDPA) is Nigeria's main data protection legislation. The NDPA was signed into law on 14 June 2023.

2. Nigeria Data Protection Regulation 2019

Before the enactment of the NDPA, the Nigerian Data Protection Regulation, 2019 (NDPR) was in existence, it was issued by the National Information Technology Development Agency (NITDA) the main agency responsible for the regulation of data protection at that time. Although enforceable, it remains a subsidiary legislation. The NDPR is still

applicable to data protection in Nigeria and are now treated as regulations issued by the NDPC (Section 64 of the NDPA). Thus, the NDPR operates side by side with the NDPA, but the NDPA will prevail where there is a conflicting provision in the NDPR (Section 63 of the NDPA).

3. Cybercrimes (Prohibition, Prevention Etc) (Amendment) Act 2015

The Cybercrimes (Prohibition, Prevention Etc) (Amendment) Act makes provision for a legal and regulatory framework that prohibits, prevents, detects, prosecutes and punishes cybercrimes in Nigeria. It requires financial institutions to retain and protect data and criminalizes the interception of electronic communications.

4. Child Rights Act 2003

The Child Rights Act 2003 restates the constitutional right to privacy as it relates to children. Section 8 of the Act guarantees a child's right to privacy subject to parent or guardian rights to exercise supervision and control of the child's conduct. Some Nigerian states have enacted Child Rights Laws. Under the Act/Laws, age of a child is any person under the age of 18.

5. Freedom of Information Act, 2011 (FOI Act)

This an Act to make public records and information more freely available, provide for public access to public records and information, protect public records and information to the extent consistent with the public interest and the protection of personal privacy, protect serving public officers from adverse consequences of disclosing certain kinds of official information without authorization and establish procedures for the achievement of those purposes and; for related matters.(Preamble to the Act)

The FOI Act makes provision for the protection of personal privacy. Section 14 of the FOI Act provides that a public institution is obliged to deny an application for information that contains personal information unless the individual involved consents to the disclosure, or where such information is publicly available. Section 16 of the FOI Act provides that a public institution may deny an application for disclosure of information that is subject to various forms of professional privilege conferred by law (such as lawyer-client privilege, health workers-client privilege, etc.).

6. Consumer Code of Practice Regulations 2007 (NCC Regulations)

The Nigeria Communication Commission Regulations was issued by the Nigerian Communications Commission. It requires all licensees to take

reasonable steps to protect customer information against improper or accidental disclosure and ensure that such information is securely stored and not kept longer than necessary. The NCC Regulations further prohibit the transfer of customer information to any party except to the extent agreed with the customer, as permitted or required by the NCC or other applicable laws or regulations.

7. Consumer Protection Framework 2016 (Framework)

The Consumer Protection Framework 2016 was enacted pursuant to the Central Bank of Nigeria Act 2007. The Framework includes provisions that prohibit financial institutions from disclosing customers' personal information. The Framework further requires that financial institutions have appropriate data protection measures and staff training programs in place to prevent unauthorized access, alteration, disclosure, accidental loss or destruction of customer data. Financial services providers must obtain written consent from consumers before personal data is shared with a third party or used for promotional offers.

8. The Consumer Protection Regulations 2020

Issued by the Central Bank of Nigeria ("CBN"), Nigeria's apex bank, it provides the minimum standards required of institutions under the regulatory purview of the bank on fair treatment of consumers, disclosure and transparency, business conduct, complaints handling and redress in order to protect the rights of consumers and to hold the institutions accountable.

9. National Identity Management Commission (NIMC) Act 2007

The NIMC Act creates the National Identity Management Commission (NIMC) to establish and manage a National Identity Management System (NIMS). The NIMC is responsible for enrolling citizens and legal residents, creating and operating a National Identity Database and issuing Unique National Identification Numbers to qualified citizens and legal residents. Section 26 of the NIMC Act provides that no person or corporate body shall have access to data or information in the Database with respect to a registered individual without authorization from the NIMC. The NIMC is empowered to provide a third party with information recorded in an individual's Database entry without the individual's consent, provided it is in the interest of National Security.

10. Nigerian Communications Commission (registration of telephone subscribers) Regulation 2011

Section 9 and 10 of the Nigerian Communications Commission Regulation provides confidentiality for telephone subscriber records maintained in the NCC's central database. The Regulation further provides telephone subscribers with a right to view and update personal information held in the NCC's central database of a telecommunication company in camera.

11. National Health (NH) Act 2014

The NH Act provides rights and obligations for health users and healthcare personnel. Under the NH Act, health establishments are required to maintain health records for every user of health services and maintain the confidentiality of such records. The NH Act further imposes restrictions on the disclosure of user information and requires persons in charge of health establishments to set up control measures for preventing unauthorized access to information. The NH Act applies to all information relating to patient health status, treatment, admittance into a health establishment, and further applies to DNA samples collected by a health establishment.

12. The HIV and AIDS (Anti-Discrimination) Act, 2014.

The Act makes provisions for the prevention and the protection of human rights of people living with or infected with the HIV virus. It provides that the confidentiality of the health and medical records of any person living with HIV or infected by AIDS must be protected at all times.

13. The CBN Guidelines on Point of Sale Card Acceptance Services 2011.

The guidelines were issued with the objective of having a framework for the provision of minimum standards and requirements for the operations of point of sale (POS) card acceptance services.

14. The Official Secrets Act 1962.

An Act that seeks to protect certain public records and information.

15. The Guidelines for the Management of Personal Data by Public Institutions in Nigeria 2020

The guideline was issued by NITDA to create a framework for the regulation of information technology and also to ensure the privacy of Nigerians.

Legislation on Right to Freedom of Expression in Nigeria

Freedom of Information Act 2011

The Freedom of Information Act was enacted in response to the outcry of dissatisfaction expressed towards the provisions of the Constitution on freedom of information and other laws such as the Official Secrets Act and the Criminal Code, especially as it relates to Government policy development and decision making.

Legislation on Freedom of Assembly and Association in Nigeria.

1. The Trade Union Act Cap T14 LFN 2004

Section 43 of the Act makes it lawful for any member or person acting on behalf of a trade union to engage in strike actions or protests.

2. Public Order Act 2004(CAP, 382 LFN, 2004)

This is the primary legislation regulating the right to assembly in Nigeria.

3. Rules of Guidance in the use of Firearms by the Police

The Police Force Order 237 provides that: A police officer may use firearms when “necessary to disperse rioters or to prevent them from committing serious offences against life and property”.

4. The Child’s Right Act 2003

Particularly Section 6 of the Act provides for the right of children to assemble as follows:

“Every child has a right to freedom of association and peaceful assembly in conformity with the *law and in accordance with the necessary guidance and directions of his parents or guardians.*”

MODULE FIVE

BASIC DIGITAL RIGHTS ISSUES AND TERMS

ACCESS TO THE INTERNET

There is no universal right to the internet. However, internet access has been described as a catalyst for the attainment of other rights. That is, the internet facilitates the realization of recognised rights.

Two critical issues arise when access to the internet is considered. First, access signifies the ability to access the online content that interests the user within the permissible restrictions. Second, access entails the availability of the physical infrastructure to be able to use the internet.

This was the focus of the United Nations Human Rights Council in 2012 when it resolved and called upon States to “facilitate access to the Internet and international cooperation aimed at the development of media and information communications facilities in all countries”. It stated also “facilitating access to the Internet for all individuals, with as little restriction to online content as possible, should be a priority for all States.” This is available at resolution A/HRC/20/L.13, 29 June 2012 (UNHRC- ‘Resolution on the promotion, protection and enjoyment of human rights on the internet’). This was expanded upon further the following year in resolution A/HRC/Res/26/13 (UNHRC- ‘Resolution on the promotion, protection and enjoyment of human rights on the internet’)

The human right body resolved amongst others as follows:

- a. It recognised that the global and open nature of the Internet is a driving force in accelerating progress towards development in its various forms, including in achieving the Sustainable Development Goals.
- b. It called on States to ensure that the Internet is open, accessible and nurtured by multi-stakeholder participation.
- c. It affirmed that quality education plays a decisive role in development, and therefore calls upon all States to promote digital literacy and to facilitate access to information on the Internet, which can be an important tool in facilitating the promotion of the right to education.
- d. It is important that a human rights-based approach should be applied when providing and expanding access to the Internet and requested States to make

efforts to bridge the many forms of digital divides, specifically the gender digital divide affecting the empowerment of women and girls, by enhancing the use of enabling technology, in particular information and communications technology.

- e. Measures aiming to or that intentionally prevent or disrupt access to or dissemination of information online in violation of international human rights law are very disturbing.
- f. It is of great concern that human rights violations and abuses are committed against persons for exercising their human rights and fundamental freedoms on the Internet and that these violations and abuses are impunity.
- g. Disconnecting individuals from the internet is a violation of human rights and goes against international law.

There are several methods adopted by governments to disrupt access to the internet. These manifests in the different following ways:

a. **Network Blackout:**

This is also known as internet shutdowns. It occurs when government cuts access to the critical network infrastructure leaving citizens unable to place calls, text or access the internet. The network infrastructure is generally referred to as the hardware and software that enables network connectivity and communication between users, devices, apps, and the internet.

This blackout can look like shutting off mobile networks or Fibre/Cable/DSL networks. It could even be shutting the power grid. Blackouts can occur at any level but are often played out at a national level or targeted to a specific region or municipality. This has been the case in several instances within Africa and Nigeria.

b. **DNS Blocking:**

This usually occurs when governments block access to specific major social media platforms or communication applications such as Facebook, WhatsApp, Twitter, Telegram, or via a VPN like Psiphon. It also involves instances when internet users are prevented from locating specific domain names or websites on the internet. An example of such instance was reported by the Open Observatory of Network Interference (OONI), who on November 2017, found that 16 websites were blocked by means of DNS tampering as ordered by the Nigerian Communications Commission (NCC).

This OONI connectivity test is used for measuring whether access to websites has been tampered with by means of DNS tampering, TCP/IP blocking, or by a transparent HTTP proxy. The measurements would reflect responses in the form of “generic timeout errors”, “DNS lookup errors” and “connection errors” which are signs of network anomalies. However, these do not necessarily serve as evidence of internet censorship, since they may have occurred due to transient network failures.

A common way this occurs in other jurisdictions is to make configuration changes at its DNS resolver. That is, when a user asks to access a particular website, the DNS resolver of the customer’s ISP recognizes the domain as a blocked site, does not allow it to be translated into an IP address, and responds to the user that the domain does not exist or provides a modified IP address that redirects users to a webpage declaring that the domain is blocked. It is reported that this generally affects the globally consistent namespace, a fundamental building block of the Internet. The manipulation and interference with the resolution of DNS records breaks the integrity of the DNS system, with long-term effects that reduce the reliability, openness, and usability of the global Internet. Fracturing the name space creates additional costs, overhead, and friction within the network.

- c. **Network Throttling:** Throttling, also known as bandwidth throttling occurs when internet service providers (ISPs) deliberately slow down the speed of the internet to reduce web performance. This could be reflected in different forms, such as, specific websites are blocked or made nonfunctional, some websites or services are slower than others, download speeds are slowed, buffering or lagging of videos, internet speed is slower than usual, Wi-Fi connection is broken, etc.

It should however be noted that not all slow internet speeds are due to throttling. There are instances when an ISP has poor connectivity, and this affects the functionality of the network. There are also times when an ISP throttles to regulate the network traffic. This presupposes a good intention for balancing access within its area of operation. This could be to conserve shared bandwidth so that more people are able to access basic, non-media-heavy content online.

Throttling can be as a result of a government’s interference with an intentional request to gag its citizens and the media. This is one of the new

emerging methods by governments to stifle the free flow of information during politically significant movements or moments of active citizen's engagement in their political affairs. This is usually ordered by government to telecommunications companies, as a means, for example, of preventing the flow of information during gross human rights abuses, making it onerous for journalists to report accurately, or witnesses to share their narratives with others, or to prevent citizens from documenting and disseminating footage of violent police behaviour. Therefore, it hampers journalism; stifle free flow of information, especially during significant national politically critical moments, such as peaceful demonstrations to protest increasing inflation, rise in fuel costs, austerity and hunger.

In recent times in Africa, there have been an increasing number of governments forcing internet service providers to slow their services or the services of specific websites in order to restrict access to such websites or the internet to serve the governments purposes. The implications of governments forcing ISPs to slow down a part of the web, such as social media platforms, or the entire network is that it stifles citizens' access to information, to organize properly to demonstrate, to exercise their constitutionally guaranteed rights to voice or express their opinions online or to communicate with their important relationships over the internet.

The involvement of government or its institutions in throttling becomes a problem especially as it brings up issues such as net neutrality, which is a principle that requires equality in the management of all internet data to ensure that there is no undue influence or interference by ISPs.

The significant problem with throttling is that it threatens several foundational human rights necessary for a thriving civic space. These include the freedom of expression, the right to information, freedom of assembly and association online. The attendant effect of this extends also in major significance to scientific, economic and academic fields as it restricts development and access to research in these fields which is generally detrimental to the progress of a county.

Governments resort to this form of interference as it is considerably difficult to detect unlike when there is a social media shutdown or internet blackout; while they effectively censor their citizens and the media. This is because in countries with weak digital infrastructures it could easily be dismissed as accidental as their infrastructures are prone to disruptions even without

government interventions. Another thing is that throttling may not impact the general public. It usually impacts only certain platforms, or some platforms, such that network speeds will appear normal for some users, while for others, the web, or some parts of it, will be virtually inoperable.

However, it should be noted that throttling can be detected and proven before the Court where appropriate tests are carried out. The measure for detection is usually through a speed test.

An individual can determine if an ISP is throttling the network in the following ways:

- a. Connecting a laptop or device to the ISP router
- b. Logging onto the high speed online tool at <https://www.highspeedinternet.com/tools/speed-test> to assess the upload and download speed.
- c. Connecting the device to a VPN and conducting the same high-speed test to assess the upload and download speed.
- d. Where the network is faster on VPN than when it was directly on the ISP's supply then it is highly possible that this was as a result of throttling.

d. **IP Blocking:**

This refers to internet access restriction to certain websites and applications to specific users. It is also known as IP address blocking. It prevents a specific IP address or groups of IP addresses from communicating with a server, computer, the web or internet. It could also be described as a digital bouncer that immediately rejects or denies entry to a network or websites from specific IP addresses.

Ordinarily, this is a security measure that helps to prevent unwanted access to content or malicious behaviour, such as cyber-attacks or spam. That is, IP addresses are blocked to prevent unwanted or harmful sites or servers from connecting with an organization's network, or an individual's computer. Examples are blocking anyone on the Internet trying to reach the accounting server of the Supreme Court, or a hospital blocking its internal IPs to protect patients' confidential data from network users who shouldn't have access to that information.

IP blocking are relevant and used as a reactive defence mechanism that protects an organization's computer system from attacks, such as a denial of service (DOS) attack or a distributed denial of service (DDOS) attack, in which the target server gets multiple requests from a malicious system until it shuts down. This same measure is deployed when mail servers are instructed to reject messages from unknown addresses or email addresses known to send out bulk spam emails.

Therefore, it is first a good thing, especially in an era where hackers deliberately send out malicious bots and viruses to attack the data centres of organizations.

However, in most cases, IP blocking has a wider reach. Where an IP address is part of a group, the entire group is blocked because it is difficult to isolate a specific IP address that belongs to a group. This usually occur when an Internet access provider has a huge volume of malicious attacks, rather than locate the specific IP address causing the attacks, which could take a lot of time and resources, it blocks the entire access provider. This can also apply to the entirety of a country. It can be used to block all internet traffic from a single country from using a server and its resources. It occurs where it is discovered that a copious number of fraudulent activities can be traced to IP addresses within a single country.

It should be noted that IP addresses can be masked. Masking takes place when a system uses an intermediary server, called a proxy, to connect to the internet. There are a lot of public proxy servers that any internet user can use, which will effectively protect the identity of the original IP address. For this reason, some network administrators allow a widespread blocking of proxy servers.

Common reasons for IP blocking are hacking, bots, confidential data, mail server spam, viruses, limiting access, criminal activities, extensions, throttling, etc.

From the foregoing, this type of blocking happens on a regular basis that most internet users are oblivious to it. It only becomes noticeable if there is a large-scale blocking or an expert research and reports on it. This was when an Austrian Court, in an attempt to block 14 websites for copyright violation, ordered exparte Austrian Internet Service Providers to block 11 of Cloudflare's IP addresses, which rendered thousands of websites

inaccessible to ordinary internet users in Austria for over two days. These several other thousands of websites became collateral damages. It becomes a challenge to assess the amount of damage done but some organizations may be able to quantify the damage with their expertise.

Over blocking websites is a big problem in the digital era and has legal implications because it raises issues of violations of rights especially where citizens are unable to exercise their digital rights. This means that governments, the executive and its agencies should not interfere in IP blocking by exercising unfettered discretion that would infringe the rights of others, that is, over reach in the exercise of their powers; and the Courts have a legal obligation to ensure that their orders are necessary and proportionate, and ensure not to affect unoffending addresses. Therefore, issuing of blanket orders or search warrants could amount to human rights violations.

This was the case before the European Court of Human Rights in the case of **VLADIMIR KHARITONOV VS. RUSSIA**, when the European Information Society Institute, a Slovakia-based nonprofit, reviewed Russia's regime for website blocking in 2017. It was reported that Russia exclusively used IP addresses to block contents. In this case, a website was blocked in Russia because it shared an IP address with a blocked website. The website owner brought suit over the block. The European Information Society Institute submitted that IP blocking led to "collateral website blocking on a massive scale" and noted that as of June 28, 2017, 6,522,629 Internet resources had been blocked in Russia, of which 6,335,850 – or 97% – had been blocked without legal justification. The Court ruled that the Russian authorities' decision to block the IP address of an offending website, which in turn resulted in the blocking of the applicant's website, amounted to a violation of the applicant's right to impart information (Article 10), and the right to an effective remedy (Article 13 read in conjunction with Article 10) of the European Convention of Human Rights (ECHR).³¹ The Court concluded that the indiscriminate blocking was impermissible, ruling that the block on the lawful content of the site "*amounts to arbitrary interference with the rights of owners of such websites.*"

³¹ Vladimir's case

<https://blog.cloudflare.com/consequences-of-ip-blocking>

e. **Filtering:**

Filtering is another mechanism for restricting access which involves blocking access to contents over the internet that are considered offensive, inappropriate, illegal and dangerous. This is closely linked with blocking and is also a tool that is used by governments to restrict users from accessing information online. Filtering can be done by government to censor and control what citizens are able to access online. Generally filtering is carried out against harmful sites or contents.

There are different forms of filtering. There is the web filtering or URL filtering. Web filtering restricts access to specific websites. This could involve restrictions to keywords, file types, malware correlations, etc, while URL filtering restricts access to specific URLs, specially making it impossible for users to find results for searched content if the results are only available on a platform that has been blocked. This also involves filtering of specific pages, images, videos, or downloads within a website, such as blocking access to social media, adult content, or streaming sites.

There is a form of filtering which is gaining notoriety. This is called the Deep Packet Inspection-based (DPI). This is an advanced and sophisticated firewall technique which filters the results of a search query, identifies specific prohibited keywords and cuts off the connection. An example of a government that uses this is China. China restricts its citizens to government-controlled websites and so popular websites, such as Facebook are inaccessible within China or users would be redirected to a similar government controlled one.

There are advantages to filtering if performed within defined and the provision of the law. That is, enacted with clarity, sufficient precision and unambiguity so that the people understand the demands of the law and conduct themselves appropriately as not to be found wanting.

Such advantages for filtering include, reduces risk of data breaches, helps in adhering to legal and industry standards, prevents access to obscene, adult, or violent images, Protects against malware and phishing, etc.

f. **Internet censorship:**

The history of the internet and its evolution shows that this technology was created and has been responsible for a lot of advancement in the human society. The internet as a tool of modernity has brought about several recognised and unprecedented development which necessitated the United Nations Human Rights Council to call on governments to “promote digital literacy and to facilitate access to information on the Internet,” as it can be “an important tool in facilitating the promotion of the right to education.”

There is no doubt that there are several advantages to the internet and how it has facilitated the spread of information, allowed its dissemination and affording internet users to share their thoughts and opinions across borders. However, it is also a fact that the internet has been a tool exposed to criminal minds as well. Several crimes have been adapted to fit the internet model which motivated some laws to counter them. It therefore shows that like any other technology made by man, the internet can also and is being misused by criminal elements.

Nevertheless, the internet remains the environment for global association, assembly, sharing and obtaining of information, innovation and creativity, economic, psychological and mental development. It has become the new environment where survival is dependent just like our physical environment. Noting this trajectory, some governments began to censor the information over the internet under the guise of protecting the ‘well-being’ of citizens or the ‘national security’ in countries where there are political unrests.

Internet censorship involves the manipulation of the internet to control information and people with regards what they access, publish, or view over the internet. This is closely related to internet shutdown but differs in that it involves the filtering of information by one authority who arbitrarily and without judicial oversight decides what contents could be shared or acquired, and what platforms could be visited. This authority can be government, social media platforms or tech companies. It is accomplished by government and its institutions, or by private organizations and individuals under the instruction of the government.

In recent years, online platforms have grown to the extent that they wield enormous powers to shape facts and the interpretation of events, by censoring, deleting, or completely removing information relevant to a subject. This was evident during the COVID 19 pandemic, where all dissenting opinions were classified as conspiracy theories, even opinions from medical professionals. These platforms, such as Twitter, Facebook,

Instagram, YouTube, etc, began to function contrary to the human nature and the tenets of the physical environment, which allows for free and open debate that strengthens democracy and the right of persons to freely hold opinions.

It is evident that some governments have ordered platforms to engage in selective censorship, especially of critics, opponents, human right defenders, journalists and media houses. This is clearly undemocratic and can only be sustained in autocratic societies, such as China, Iran and Russia, countries topping the charts on repression. Interestingly, some countries in Africa have also taken the lead on censorship. For example, it was reported³² that Uganda manipulates online conversations to control dissent particularly during elections,

This form of censorship also exists in circumstances where individuals or organizations are coerced into censoring or filtering the information they share due to intimidation or out of fear of legal or other measures, or ultimately to conform to societal pressures. This takes place frequently in a country like Nigeria where Media Houses are forced to self-censor in order not to be sanctioned for sharing information that ‘threatens the corporate existence’³³ of the entity.

It should be noted that this brings to fore the principle of **Prior Restraint**. Prior restraint is a form of censorship by government to prevent the publication or broadcast of any speech or other forms of expression in anticipation of a wrongdoing. Some governments have claimed that the internet is being used to as a medium for racism, sexism, pornography, fraud, other forms of violence and criminal activities but their arguments fall short of reasoning considering the physical environment also suffers the same problem, hence the justification for several criminal laws without the shutting down of the society.

Prior restraint anticipates a wrongdoing. It operates as a means to justify the imposition of subsequent punishment on expression. That is, prior restraint functions in a similar sense as punishing an individual for an offence that doesn’t exist at the time the action was taken. That is, the very core ideology that is contrary to the principle of legality in criminal law which prohibits

³² <https://www.nytimes.com/2021/01/13/world/africa/uganda-facebook-ban-elections.html>

³³ Lai Mohammed

the punishment of an offence that has not been prescribed or clearly punished by law.³⁴

Prior Restraint is a means by which state actors curtail the rights to expression. The doctrine frowns at the overuse of arguably permissible censorship by self-serving, unaccountable, or insensitive government officials. In most cases, restraint is arbitral and subject to the discretion of one actor without recourse to a clearly defined law that has met the requirements of necessity and proportionality as defined under the Article 19 of the International Covenant on Civil and Political Rights (ICCPR)³⁵. It is as a result of this that there is a presumption against the constitutional validity of the doctrine because it is generally unnecessary and disproportionate, and prone to cause a chilling effect on the right to freedom of expression.

William Blackstone did a legal analysis of the concept of Previous Restraint in volume 4 of his Commentaries on the Laws of England.³⁶ This work gave a further understanding on the concept in relation to freedom of expression. He wrote:

The liberty of the press is indeed essential to the nature of a free state: but this consists in laying no previous restraints upon publications, and not in freedom from censure for criminal matter when published. Every freeman has an undoubted right to lay what sentiments he pleases before the public: to forbid this, is to destroy the freedom of the press: but if he publishes what is improper, mischievous, or illegal, he must take the consequence of his own temerity. To subject the press to the restrictive power of a licenser, as was formerly done, both before and since the

³⁴ Nullen crimen sine lege

³⁵ Iccpr here

³⁶ Book 4: Public Wrongs ... COMMENTARIES ON THE LAWS OF ENGLAND (1765-69), By Sir William Blackstone, Former Justice of the Common Pleas of England and Wales. His work gave an historical context to the emergence of the freedom of the press when he wrote as follows: "The art of printing, soon after its introduction, was looked upon (as well in England as in other countries) as merely a matter of state, and subject to the coercion of the crown. It was therefore regulated with us by the king's proclamations, prohibitions, charters of privilege and of license, and finally by the decrees of the court of star chamber; which limited the number of printers, and of presses which each should employ, and prohibited new publications unless previously approved by proper licensers. On the demolition of this odious jurisdiction in 1641, the long parliament of Charles I, after their rupture with that prince, assumed the same powers as the star chamber exercised with respect to the licensing of books; and in 1643, 1647, 1649, and 1652, (Scobell. i. 44, 134. ii 88, 230.) issued their ordinances for that purpose, founded principally on the star chamber decree of 1637. In 1662 was passed the statute 13 & 14 Car. II. c. 33. which (with some few alterations) was copied from the parliamentary ordinances. This act expired in 1679 but was revived by statute 1 Jac. II. c. 17. and continued till 1692. It was then continued for two years longer by statute 4 W. & M. c. 24. but, though frequent attempts were made by the government to revive it, in the subsequent part of that reign, (Com. Journ. 11 Feb. 1694. 26 Nov. 1695. 22 Oct. 1696. 9 Feb. 1697. 31 Jan. 1698.) yet the parliament resisted it so strongly, that it finally expired, and the press became properly free, in 1694; and has ever since so continued."

revolution is to subject all freedom of sentiment to the prejudices of one man, and make him the arbitrary and infallible judge of all controverted points in learning, religion, and government. But to punish (as the law does at present) any dangerous or offensive writings, which, when published, shall on a fair and impartial trial be adjudged of a pernicious tendency, is necessary for the preservation of peace and god order, of government and religion, the only solid foundations of civil liberty. Thus the will of individuals is still left free; the abuse only of that free will hereby laid upon freedom, of thought or inquiry: liberty of private sentiment is still left; the disseminating, or making public, of bad sentiments, destructive of the ends of society, is the crime which society corrects. A man (says a fine writer on this subject) may be allowed to keep poisons in his closet, but not publicly to vend them as cordials. And to this we may add, that the only plausible argument heretofore used for restraining the just freedom of the press, "that it was necessary to prevent the daily abuse of it," will entirely lose its force, when it is shown (by a seasonable exertion of the law) that the press cannot be abused to any bad purpose, without incurring a suitable punishment: whereas it never can be used to any good one, when under the control of an inspector. So true will it be found, that to censure the licentiousness, is to maintain the liberty, of the press.

The issue of prior restraint was also considered at the Supreme Court of the United States in the case of *NEW YORK TIMES CO. V. UNITED STATES, 403 U.S. 713 (1971)*³⁷ when the question came before the Court to decide whether the government could prevent the New York Times and the Washington Post from publishing what it termed 'classified information', materials he claimed belonged to a classified Defence Department study regarding the history of United States activities in Vietnam. The documents (known as the Pentagon Papers) detailed the decision-making leading to the United States' involvement in the Vietnam War. In the case, the Nixon administration argued that prior restraint was necessary to protect national security. The Court analysed the submissions alongside the provision of the first amendment to the United States Constitution, of which part states "...The people shall not be deprived or abridged of their right to speak, to write, or to publish their sentiments, *and the freedom of the press, as one of the great bulwarks of liberty, shall be inviolable.*"³⁸ The Court considered earlier

³⁷ <https://www.law.cornell.edu/supremecourt/text/403/713>

³⁸ The other parts were:

"The civil rights of none shall be abridged on account of religious belief or worship, nor shall any national religion be established, nor shall the full and equal rights of conscience be in any manner, or on any pretext, infringed."

"The people shall not be restrained from peaceably assembling and consulting for their common good, nor from applying to the Legislature by petitions, or remonstrances, for redress of their grievances."

judgements bearing on the same circumstances of the case and held per Justices Black and Douglas that “Any system of prior restraints of expression comes to this Court bearing a heavy presumption against its constitutional validity”³⁹. The Government “thus carries a heavy burden of showing justification for the imposition of such a restraint.”⁴⁰ It was further stated that “The dominant purpose of the First Amendment was to prohibit the widespread practice of governmental suppression”.

Justice Stewart stated⁴¹:

“In the governmental structure created by our Constitution, the Executive is endowed with enormous power in the two related areas of national defense and international relations. This power, largely unchecked by the Legislative and Judicial branches, has been pressed to the very hilt since the advent of the nuclear missile age. For better or for worse, the simple fact is that a President of the United States possesses vastly greater constitutional independence in these two vital areas of power than does, say, a prime minister of a country with a parliamentary form of government. In the absence of the governmental checks and balances present in other areas of our national life, the only effective restraint upon executive policy and power in the areas of national defense and international affairs may lie in an enlightened citizenry -- in an informed and critical public opinion which alone can here protect the values of democratic government. For this reason, it is perhaps here that a press that is alert, aware, and free most vitally serves the basic purpose of the First Amendment. For, without an informed and free press, there cannot be an enlightened people.

Per Justice Black, and the concurring opinion of Justice Douglas⁴²,

‘...To find that the President has "inherent power" to halt the publication of news by resort to the courts would wipe out the First Amendment and destroy the fundamental liberty and security of the very people the Government hopes to make "secure." No one can read the history of the adoption of the First Amendment without being convinced beyond any doubt that it was injunctions like those sought here that Madison and his collaborators intended to outlaw in this Nation for all time. **The word "security" is a broad, vague generality whose contours should not be invoked to abrogate the fundamental law embodied in the First Amendment.** The guarding of military and diplomatic secrets at the expense of informed representative government provides no real security for our Republic. The Framers of the First Amendment, fully aware of both the need to defend a new nation and the abuses of the English and Colonial governments,

³⁹ *Bantam Books, Inc. v. Sullivan*, [372 U. S. 58](#), [372 U. S. 70](#) (1963); *Near v. Minnesota*, [283 U. S. 697](#) (1931)

⁴⁰ *Organization for a Better Austin v. Keefe*, [402 U. S. 415](#), [402 U. S. 419](#) (1971)

⁴¹ *Id.* at Page 403 U. S. 728

⁴² *Id.* at Page 403 U. S. 720

sought to give this new society strength and security by providing that freedom of speech, press, religion, and assembly should not be abridged. This thought was eloquently expressed in 1937 by Mr. Chief Justice Hughes -- great man and great Chief Justice that he was -- when the Court held a man could not be punished for attending a meeting run by Communists." The greater the importance of safeguarding the community from incitements to the overthrow of our institutions by force and violence, the more imperative is the need to preserve inviolate the constitutional rights of free speech, free press and free assembly in order to maintain the opportunity for free political discussion, to the end that government may be responsive to the will of the people and that changes, if desired, may be obtained by peaceful means. Therein lies the security of the Republic, the very foundation of constitutional government."⁴³

Justice Brennan, concurring with the lead Judgement, added that *"The error that has pervaded these cases from the outset was the granting of any injunctive relief whatsoever, interim or otherwise. The entire thrust of the Government's claim throughout these cases has been that publication of the material sought to be enjoined "could," or "might," or "may" prejudice the national interest in various ways. The First Amendment tolerates absolutely no prior judicial restraints of the press predicated upon surmise or conjecture that untoward consequences may result"*⁴⁴

It was therefore reasoned that so long as publication would not cause an inevitable, direct, and immediate event imperilling the safety of American forces, prior restraint was unjustified.

The above case goes to show that the reliance on national security as justification for restrictions on internet access would only be considered valid where the government is able to convince the Court that the measures taken is necessary in a democratic society and proportionate to the legitimate aim the government pursues.

The Inter-American Court of Human Rights (IACtHR) has also been foremost in pronouncing on the permissible restrictions to the right to freedom of expression. The case of **OLMEDO BUSTOS ET AL. V. CHILE**⁴⁵ stands out. The case is not the only instance in which the Inter-American Court of Human Rights (IACtHR) ruled on the right to freedom of expression. In fact, the Court has ruled on the violation of the right to freedom of expression in at least 18 cases.

⁴³ *De Jonge v. Oregon*, 299 U. S. 353, 299 U. S. 365.

⁴⁴ *Id.* at Page 403 U. S. 726

⁴⁵ "The Last Temptation of Christ" Case, Series C No. 73 Judgement of 5 February 2001

However, the Court's decision in this instance became a catalyst for the amendment of the Chilean Constitution. In the case, the National Cinematographic Classification Council (NCCC) approved the showing of the film, *The Last Temptation of Christ*. A group of applicants sued for themselves and in the name of Jesus Christ and the Catholic Church arguing that the image of Christ was diminished in the film. The Court of Appeals of Santiago delivered a judgment annulling the administrative decision of NCCC and this was upheld at the Supreme Court and stated to be a violation of the freedom of religion. The Applicants applied to the IACHR arguing that there has been a judicial censorship by the Chilean Courts. The IACHR considered the merits of the case as follows⁴⁶:

63. Article 13 of the American Convention establishes that:

1. Everyone has the right to freedom of thought and expression. This right includes freedom to seek, receive, and impart information and ideas of all kinds, regardless of frontiers, either orally, in writing, in print, in the form of art, or through any other medium of one's choice.
2. The exercise of the right provided for in the foregoing paragraph shall not be subject to prior censorship but shall be subject to subsequent imposition of liability, which shall be expressly established by law to the extent necessary to ensure:
 - a. Respect for the rights or reputation of others;
 - b. The protection of national security, public order, or public health or morals.
3. The right of expression may not be restricted by indirect methods or means, such as the abuse of government or private controls over newsprint, radio broadcasting frequencies, or equipment used in the dissemination of information, or any other means tending to impede the communication and circulation of ideas and opinions.
4. Notwithstanding the provisions of paragraph 2 above, public entertainments may be subject by law to prior censorship for the sole purpose of regulating access to them for the moral protection of childhood and adolescence.
5. Any propaganda for war and any advocacy of national, racial or religious hatred that constitute incitements to lawless violence or to any other similar illegal action against any person or group of persons on any grounds including those of race, colour, religion, language, or national origin shall be considered as offences punishable by law.

69. The European Court of Human Rights has indicated that:

[The] supervisory function [of the Court] signifies that [it] must pay great attention to the principles inherent in a 'democratic society'. Freedom of expression constitutes one of the essential bases of such a society, one of the primordial conditions for its progress and for the development of man. Article 10.2 [of the European Convention on Human Rights] is valid not only for the information or ideas that are favourably received or considered inoffensive or indifferent, but also for those that shock, concern or offend the State or any sector of the population. Such are the requirements of pluralism, tolerance and the spirit of openness, without which no 'democratic society' can exist. This means that any

⁴⁶ Id. Para 63-103

formality, condition, restriction or sanction imposed in that respect, should be proportionate to the legitimate end sought.

Also, those who exercise their freedom of expression assume' obligations and responsibilities', the scope of which depends on the context and the technical procedure used.

70. It is important to mention that Article 13.4 of the Convention establishes an exception to prior censorship, since it allows it in the case of public entertainment, but only in order to regulate access for the moral protection of children and adolescents. In all other cases, any preventive measure implies the impairment of freedom of thought and expression.

71. In the instant case, it has been proved that, in Chile, there is a system of prior censorship for the exhibition and publicity of cinematographic films and that, in principle, the Cinematographic Classification Council prohibited exhibition of the film "The Last Temptation of Christ" and, reclassifying it, permitted it to be exhibited to persons over 18 years of age. Subsequently, the Court of Appeal of Santiago decided to annul the November 1996 decision of the Cinematographic Classification Council, owing to a remedy for protection filed by Sergio García Valdés, Vicente Torres Irrarrázabal, Francisco Javier Donoso Barriga, Matías PérezCruz, Jorge Reyes Zapata, Cristian Heerwagen Guzmán and Joel González Castillo, "for and in the name of [°] Jesus Christ, the Catholic Church and themselves"; a decision that was confirmed by the Supreme Court of Justice of Chile. Therefore, this Court considers that the prohibition of the exhibition of the film "The Last Temptation of Christ" constitutes prior censorship in violation of Article 13 of the Convention.

72. This Court understands that the international responsibility of the State may be engaged by acts or omissions of any power or organ of the State, whatsoever its rank, that violate the American Convention. That is, any act or omission that may be attributed to the State, in violation of the norms of international human rights law engages the international responsibility of the State. In this case, it was engaged because article 19.12 of the Constitution establishes prior censorship of cinematographic films and, therefore, determines the acts of the Executive, the Legislature and the Judiciary.

73. In the light of the foregoing considerations, the Court declares that the State violated the right to freedom of thought and expression embodied in Article 13 of the American Convention, to the detriment of Juan Pablo Olmedo Bustos, Ciro Colombara López, Claudio Márquez Vidal, Alex Muñoz Wilson, Matías Insunza Tagle and Hernán Aguirre Fuentes.

103. Therefore, 1. Finds that the State violated the right to freedom of thought and expression embodied in Article 13 of the American Convention on Human Rights.

The Court ordered the state to allow the screening of this particular film. It also held that Chile had failed to repeal Article 19 of the Chilean Constitution of 1980, which allowed prior censorship of the exhibition and publicity of cinematographic production and was therefore contradictory to the guarantees established in the

IACHR. The Court ordered the state to modify its constitutional laws to eliminate prior censorship, and as a result, the Chilean Congress approved a constitutional amendment where prior censorship was substituted by a system of categorization regulated by law.⁴⁷

To conclude on issues bordering on the access to the internet, it must be stated at this point that the question of access to the internet has also been severally dealt with by regional Courts. In **KALDA V. ESTONIA**⁴⁸, a prisoner in Estonia serving a life sentence was denied access to the online *Gazette*, Supreme Court and administrative court online decisions, and to the online judgments of the European Court of Human Rights. He challenged this in the domestic Courts and exhausted all available national legal processes before approaching the ECHR to determine if his right to access information available online has not been violated. The applicant submitted that the ban on his accessing the websites of the Council of Europe Information Office in Tallinn, the Chancellor of Justice and the Riigikogu violated his right to receive information and was in breach of Article 10 of the Convention. The applicant referred the Court to the relevance and the volume of information now accessible through the Internet (legal acts, case-law, parliamentary activities, newspapers, and so on). He argued that a ban on Internet access actually amounted to a total ban on access to information. The applicant submitted that his aim was to be able to undertake legal research in order to understand his rights and obligations and in order to be able to defend his rights in court on an equal footing, if necessary.

The Government maintained that there had been no violation of Article 10 of the Convention. They argued that neither the Estonian Constitution nor the Convention prescribed that everyone should be entitled to obtain through the Internet information such as that in issue in the present case. They submitted that the State had discretion to restrict the right of specific groups of people (such as prisoners) to access information through specific channels. According to the Government, prisoners were not in a position comparable to that of persons at liberty. They added that the restriction of prisoners' access to the Internet had a legal basis in section 31-1 of the Imprisonment Act. The aim of that provision was to maintain prison security and the safety of persons outside the prison, as well as the prevention of crime and the protection of victims. They further submitted that the

47 Commentaries by **Laura Bernal-Bermúdez** "Is the Inter-American Court of Human Rights setting regional standards?" (Accessible at <https://debateglobal.wordpress.com/tag/case-olmedo-bustos-et-al-vs-chile/>)

48 Application No. 17429 19 January 2016 (accessible at: <https://hudoc.echr.coe.int/eng?i=001-160270>).

restriction was proportionate to the aims pursued. Granting access only to specific websites that constituted the official databases of legislation and the database of judicial decisions was justified by the demands of security. Making additional websites available and technically as secure as possible would incur additional expense. In view of the fact that all websites contained references, search engines, links (including to social networks), and the like, and having regard to the fact that websites were updated on a daily basis, it was impossible to completely avoid or prevent security vulnerabilities.

After listening to both sides, the Court considered the submissions and stated as follows:

“The Court has consistently recognised that the public has a right to receive information of general interest. Within this field, it has developed case-law in relation to press freedom, the purpose of which is to impart information and ideas on such matters. The Court has also found that the function of creating forums for public debate is not limited to the press. That function may also be exercised by non-governmental organisations, the activities of which are an essential element of informed public debate. Furthermore, the Court has held that the right to receive information basically prohibits a Government from preventing a person from receiving information that others wished or were willing to impart (see **Leander v. Sweden**, 26 March 1987, § 74, Series A no. 116). It has also held that the right to receive information cannot be construed as imposing on a State positive obligations to collect and disseminate information of its own motion (see **Guerra and Others v. Italy**, 19 February 1998, § 53, Reports of Judgments and Decisions 1998-I). In the present case, however, the question in issue is not the authorities’ refusal to release the requested information; the applicant’s request concerned information that was freely available in the public domain. Rather, the applicant’s complaint concerns a particular means of accessing the information in question: namely, that he, as a prisoner, wished to be granted access – specifically, via the Internet – to information published on certain websites. In this connection, the Court reiterates that in the light of its accessibility and its capacity to store and communicate vast amounts of information, the Internet plays an important role in enhancing the public’s access to news and facilitating the dissemination of information in general (see **Delfi AS v. Estonia [GC]**, no. 64569/09, § 133, ECHR 2015; **Ahmet Yildirim v. Turkey**, no. 3111/10, § 48, ECHR 2012; and **Times Newspapers Ltd v. the United Kingdom (nos. 1 and 2)**, nos. 3002/03 and 23676/03, § 27, ECHR 2009).

Nevertheless, the Court notes that imprisonment inevitably involves a number of restrictions on prisoners’ communications with the outside world, including on their ability to receive information. It considers that Article 10 cannot be interpreted as imposing a general obligation to provide access to the Internet, or to specific Internet sites, for prisoners. However, it finds that in the circumstances of the case, since access to certain sites containing legal information is granted under Estonian law, the restriction of access to other sites that also contain legal

information constitutes an interference with the right to receive information. The Court notes that the websites of the Council of Europe Information Office in Tallinn, the Chancellor of Justice, and the Riigikogu, to which the applicant wished to have access, predominantly contained legal information and information related to fundamental rights, including the rights of prisoners. For example, the website of the Riigikogu contained bills together with explanatory memoranda to them, verbatim records of the sittings of the Riigikogu, and minutes of committee sittings. The website of the Chancellor of Justice (who is also an ombudsman in Estonia) contained his selected legal opinions. The Court considers that the accessibility of such information promotes public awareness and respect for human rights and gives weight to the applicant's argument that the Estonian courts used such information and the applicant needed access to it for the protection of his rights in the court proceedings. The Court has also taken note of the applicant's argument that legal research in the form of browsing through available information (in order to find relevant information) and making specific requests for information were different matters and that the websites were meant for legal researches rather than making specific requests. Indeed, in order to make a specific request one would need to be aware of which particular information is available in the first place. The Court also notes that the domestic authorities have referred to alternative means of making available to the applicant the information stored on the websites in question (for example, by mail – see paragraph 17 above), but did not compare the costs of these alternative means with the additional costs that extended Internet access would allegedly incur.

The Court cannot overlook the fact that in a number of Council of Europe and other international instruments the public-service value of the Internet and its importance for the enjoyment of a range of human rights has been recognised. Internet access has increasingly been understood as a right, and calls have been made to develop effective policies to attain universal access to the Internet and to overcome the “digital divide” (see paragraphs 23 to 25 above). The Court considers that these developments reflect the important role the Internet plays in people's everyday lives. Indeed, an increasing amount of services and information is only available on the Internet, as evidenced by the fact that in Estonia the official publication of legal acts effectively takes place via the online version of Riigi Teataja and no longer through its paper version (see paragraph 7 above). The Court reiterates that the online version of Riigi Teataja also currently carries Estonian summaries and Estonian translations of the Court's judgments (see paragraph 40 above).”

As regards the issue of whether the interference was “necessary” within the meaning of Article 10 § 2, the Court notes that according to the Government, granting prisoners access to a greater number of Internet sites would have increased security risks and required the allocation of additional material and human resources in order to mitigate such risks. By contrast, the applicant was of the opinion that allowing access to three more websites (in addition to those already authorised) would not have given rise to any additional security issues.

Possible security issues were already effectively managed by the Ministry of Justice, which blocked any links or other such features on already authorised websites that could cause security concerns; there was no reason, according to the applicant, why this should be different in the case of the three requested additional websites...The Court also considers that the Supreme Court and the Government have failed to convincingly demonstrate that giving the applicant access to three additional websites would have caused any noteworthy additional costs. In these circumstances, the Court is not persuaded that sufficient reasons have been put forward in the present case to justify the interference with the applicant's right to receive information.

The Court concludes that the interference with the applicant's right to receive information, in the specific circumstances of the present case, cannot be regarded as having been necessary in a democratic society. There has accordingly been a violation of Article 10 of the Convention."

One other example is the case of **JANKOVSKIS V. LITHUANIA**⁴⁹ considered by the European Court of Human Rights in 2017. The Applicant was a prisoner serving a term in the Lithuanian prison. At some point he wrote the Ministry of Education and Science requesting information about the possibility of enrolling at the university. He informed them of having graduated in 1996 from the Medical Faculty of Vilnius University and stated that he wished to pursue studies via distance learning to acquire a second university degree. The Ministry replied informing him that all necessary information about study programs could be found on its website. However, the prison authorities refused the applicant access to the Internet to view this website. He filed a suit before the European Court of Human Rights, claiming that his right to access information has been denied. He complained that he had not had internet access in prison. He argued that this had prevented him from receiving education-related information, in breach of Article 10 of the Convention. The applicant contended that the restriction of inmates' use of the Internet in prison was not prescribed by law.

Article 10 reads:

"1. Everyone has the right to freedom of expression. This right shall include freedom to hold opinions and to receive and impart information and ideas without interference by public authority and regardless of frontiers. This Article shall not prevent States from requiring the licensing of broadcasting, television or cinema enterprises.

2. The exercise of these freedoms, since it carries with it duties and responsibilities, may be subject to such formalities, conditions, restrictions or penalties as are prescribed by law and are necessary in a democratic society, in the interests of national security, territorial integrity or public safety, for the

⁴⁹ Application No. 21575/08 17 January 2017 [https://hudoc.echr.coe.int/fre#{%22itemid%22:\[%22001-170354%22\]}](https://hudoc.echr.coe.int/fre#{%22itemid%22:[%22001-170354%22]})

prevention of disorder or crime, for the protection of health or morals, for the protection of the reputation or rights of others, for preventing the disclosure of information received in confidence, or for maintaining the authority and impartiality of the judiciary.”

Among other submissions, the government argued that:

the prohibition of Internet access in prison was aimed at preventing crime, given that the Internet could be used as a means of communication like other prohibited items, such as mobile phones, which prisoners sometimes use illegally from inside prison to commit new crimes – particularly telephone fraud – or to influence participants in criminal proceedings. It submitted further that the complaint was manifestly ill-founded, as the denial of one particular means of receiving information could have been circumvented by using other means available to the applicant. It also stated that the interference had been necessary and proportionate. As noted by the Supreme Administrative Court, the wide scope of opportunities afforded by the Internet could pose a threat to the rights of other persons. This, in turn, would require “huge efforts” by the prison authorities to prevent any such potential illegal acts. The Internet was only one means of receiving information, and the prisoners could effectively exercise that right by other means, such as by postal correspondence (letters) via the prison authorities. In the present case, the information which the applicant sought was available in various forms – the information concerning admission to educational institutions is announced in the press, special publications are printed, and such information could also have been imparted by the applicant’s relatives. Prisoners may also receive information concerning the possibility of studies in social rehabilitation units or correctional institutions. General and vocational education was organised in Lithuania in prisons so as to guarantee the inmates’ the right to education, and the applicant had made use of those possibilities whilst serving his sentence.

On the existence of an interference with the right of the Applicant to access the internet, the Court considered the submissions of both parties and held as follows:

“The Court has consistently recognised that the public has a right to receive information of general interest. Furthermore, the Court has held that the right to receive information basically prohibits a Government from preventing a person from receiving information that others wished or were willing to impart. In the present case, however, the question at issue is not the authorities’ refusal to release the requested information... the applicant’s request concerned information that was freely available in the public domain. Rather, the applicant’s complaint concerns a particular means of accessing the information in question: namely, that he, as a prisoner, wished to be granted access – specifically via the Internet – to information published on a website belonging to the Ministry of Education and Science. In this connection, the Court reiterates that in the light of its accessibility and its capacity to store and communicate vast amounts of information, the Internet plays an important role in enhancing the public’s access to news and facilitating the dissemination of information in general (see **Delfi AS v. Estonia [GC], no. 64569/09, § 133, ECHR 2015; Ahmet Yıldırım v. Turkey, no. 3111/10, § 48, ECHR 2012; and Times Newspapers Ltd v. the United Kingdom (nos. 1 and 2),**

nos. 3002/03 and 23676/03, § 27, ECHR 2009). Nevertheless, the Court notes that imprisonment inevitably entails a number of restrictions on prisoners' communications with the outside world, including on their ability to receive information. It considers that Article 10 cannot be interpreted as imposing a general obligation to provide access to the Internet, or to specific Internet sites, for prisoners (see Kalda, cited above, § 45). However, in the circumstances of the present case, since access to information relating to education is granted under Lithuanian law (see paragraph 34 above), the Court is ready to accept that the restriction of access to the Internet site to which the Ministry referred the applicant in reply to his request to provide information constituted an interference with the right to receive information."

On whether the interference was justified the Court stated that "The above-mentioned interference contravened Article 10 of the Convention unless it was "prescribed by law", pursued one or more of the legitimate aims referred to in paragraph 2 of that Article and was "necessary in a democratic society" for achieving such aim or aims... The Court notes that the website to which the applicant wished to have access contained information about learning and study programmes in Lithuania. The information on that site was regularly updated to reflect, for example, admission requirements for the current academic year. It also provided up to date information from the Lithuanian Labour Exchange about job vacancies and unemployment (see paragraph 7 above). It is not unreasonable to hold that such information was directly relevant to the applicant's interest in obtaining education, which is in turn of relevance for his rehabilitation and subsequent reintegration into society. As underlined by the CPT, a satisfactory programme of activities, including education, is of crucial importance for the well-being of all detainees, including prisoners awaiting trial. This is all the more relevant in relation to sentenced prisoners (see paragraph 35 above), and the applicant, who was serving a sentence in the Pravieniškės Correctional Home, was one such prisoner (see paragraph 5 above). In fact, as regards the Pravieniškės Correctional Home, the CPT specifically noted after its 2008 visit that steps should be taken to ensure that all sentenced prisoners in that prison were able to engage in purposeful activities of a varied nature, such as educational programmes (see point 49 in fine of the CPT report, quoted in **Mironovas and Others v. Lithuania, nos. 40828/12, 29292/12, 69598/12, 40163/13, 66281/13, 70048/13 and 70065/13, § 65, 8 December 2015**). The Court also considers that accessing the AIKOS website in the manner advised by the Ministry of Education and Science – namely browsing through it in order to find information that was relevant – was more efficient than making requests for specific information, as was proposed by the Government (see paragraph 46 above). Indeed, in order to make a specific request to an educational institution one would need to be aware of the competencies of that institution and the services provided by it. Such preliminary information would be provided by the AIKOS website. The Court furthermore notes the applicant's argument that the information about the study programmes was of a constantly evolving nature (see paragraph 40 above). This fact is also highlighted on the AIKOS website itself (see paragraph 7 above). Turning to the Lithuanian authorities' decisions, the Court cannot but observe that they essentially focused on the legal ban on prisoners having Internet access as such, instead of examining the applicant's argument that access to a particular website was necessary for

his education (see paragraphs 10, 12, 14, 15, 16 and 19 above). It is true that the Pravieniškės Correctional Home authorities pointed out the presence of a secondary school in that prison, as well as the possibility of following computer courses at Elektrėnai vocational school (see paragraph 18 above). However, this appears to be a very remote proposition in relation to the applicant's wish to acquire a second university degree (see paragraph 6 above). In the present case the Court also observes that the prison authorities or the Lithuanian courts did not even go so far as to argue that extended Internet access could incur additional costs for the State (see paragraphs 14, 15, 16 and 19 above). Whilst the security considerations arising from prisoners' access to Internet, as such, and cited by the prison authorities (see paragraph 14 above) may be considered as relevant, the Court notes that the domestic courts failed to give any kind of consideration to the fact that the applicant asked for access to a website created and administered by the Ministry of Education and Science, which was a State institution. In fact, both courts were completely silent on the matter of education (see paragraphs 16 and 19 above).

Lastly, the Court is mindful of the fact that in a number of the Council of Europe's and other international instruments the public-service value of the Internet and its importance for the enjoyment of a range of human rights has been recognised. Internet access has increasingly been understood as a right, and calls have been made to develop effective policies to achieve universal access to the Internet and to overcome the "digital divide" (see Kalda, cited above, § 52). The Court considers that these developments reflect the important role the Internet plays in people's everyday lives, in particular since certain information is exclusively available on Internet. Indeed, as has already been established in this case, the AIKOS website provides comprehensive information about learning possibilities in Lithuania. In this connection it is also noteworthy that the Lithuanian authorities did not even consider a possibility of granting the applicant limited or controlled Internet access to this particular website administered by a State institution, which could have hardly posed a security risk.

In these circumstances, the Court is not persuaded that sufficient reasons have been put forward in the present case to justify the interference with the applicant's right to receive information. Moreover, having regard to the consequences of that interference for the applicant (see paragraphs 59-61 above), the Government's objection that the applicant had not suffered significant disadvantage (see paragraph 50 above) must be dismissed.

The Court concludes that the interference with the applicant's right to receive information, in the specific circumstances of the present case, cannot be regarded as having been necessary in a democratic society. There has accordingly been a violation of Article 10 of the Convention.

In Africa, the ECOWAS Community Court has been foremost in pronouncing on the importance of and having access to the internet. In the case of **ASSOCIATION DES BLOGUEURS DE GUINÉE (ABLOGUI) AND OTHERS V THE STATE OF GUINEA**, Judgment no. ECW/CCJ/JUD/38/23/22 (31 October 2023), paragraph 60, the Court stated as follows:

“of the opinion that the Internet plays an important role in the development of a country because websites contribute to improving access to news through real-time dissemination of information...”

In the same vein, the Court had in an earlier landmark judgment of **AMNESTY INTERNATIONAL TOGO AND OTHERS V THE TOGOLESE REPUBLIC JUDGMENT NO ECW/CCJ/JUD/09/20 (25 JUNE 2020)** held unequivocally that by virtue of Article 9 of the ACHPR and Article 19 of the ICCPR the internet is a “derivative right to access information, which is not a stand-alone right but a complementary right to the enjoyment of the right to freedom of expression.”⁵⁰ It stated that:

“...right to internet access is closely linked to the right to freedom of speech which can be seen to encompass freedom of expression as well. Since access to internet is complementary to the enjoyment of the right to freedom of expression, it is necessary that access to the internet and the right to freedom of expression be deemed to be an integral part of human right that requires protection by law and makes its violation actionable.”⁵¹

Therefore, the Internet plays an important role in enhancing the public’s access to news and facilitating the dissemination of information in general.⁵² It provides a global platform to share information and ideas instantaneously at a relatively low cost. It has changed the way many now receive their news and information, and the Internet is regarded as one of the primary and principal means for individuals to exercise their right to freedom of expression.⁵³

NET NEUTRALITY

The internet infrastructure as we have come to understand is such that operates under the exclusive control of ISPs, who can determine how and when to make it available to users. This poses a challenge in the modern society as there is a likelihood of abuse and arbitrary withholding of access to the internet under circumstances where societies could be held at ransom by these few corporations who provide the internet services. Generally, ISPs can decide to stop, slow down, or tamper in whatsoever manner the internet infrastructure.⁵⁴ In this case, ISPs

⁵⁰ ECOWAS Court, *The Registered Trustees of The Socio-Economic Rights and Accountability Project (SERAP) and 3 Others v Federal Republic of Nigeria*, Judgment No: ECW/CCJ/JUD/40/22 (14 July 2022), para 67

⁵¹ ECOWAS Court of Justice, *Amnesty International Togo and others v The Togolese Republic* Judgment no ECW/CCJ/JUD/09/20 (25 June 2020), para 38

⁵² ECtHR, *Times Newspapers Ltd v the United Kingdom (Nos 1 and 2)* Apps nos 3002/03 and 23676/03 (10 March 2009) para 27

⁵³ UN Special Rapporteur on Freedom of Opinion and Expression, OSCE Representative on Freedom of the Media, OAS Special Rapporteur on Freedom of Expression and ACHPR Special Rapporteur on Freedom of Expression and Access to Information, *Joint Declaration on Freedom of Expression and the Internet* (1 June 2011), available at:

<https://www.osce.org/fom/78309?download=true>

⁵⁴ Net Neutrality-Stanford University (Accessible at

<https://cs.stanford.edu/people/eroberts/cs201/projects/2010-11/NetNeutrality/Articles/Proponents.html>)

could decide to make their services available at a faster speed for companies or platforms that can pay more for ‘better services’ while neglecting small content providers. This foresees a situation of network imbalance and discrimination. It is as a result of this that the principle of net neutrality was conceptualized as a principle for ensuring access to the internet. The concept was popularized by **Tim Wu**, a professor at Columbia Law School, in his 2003 paper titled "**Network Neutrality, Broadband Discrimination.**"⁵⁵

It is a principle that requires all internet service providers to ensure that there is equality in access to websites, contents and data on the internet and not charge differently based on content or the size of the user. That is, there should be equal access to information and services on the internet, irrespective of their financial resources or the size and power of the websites they use, or content, application, service, device, sender or recipient address. The principle demands that there should not be discrimination in providing internet traffic to all users.⁵⁶ This means that Internet Service Providers are mandated not to prioritize access to information among users but rather ensure that speed and access are made available in equal proportions to users, whether individuals, government or organizations, without undue interference.

The impact of a system where net neutrality is not laid out was described by the United Nations Special Rapporteur (UNSR) on freedom of expression in his 2017 report, who observed that “net neutrality protections are designed to safeguard freedom of expression and access to information online by ensuring that such freedoms are not determined by market forces or curtailed by network providers... Essentially, this means that internet service providers (**ISPs**) must remain neutral and impartial when providing internet access. In this regard, ISPs cannot alter competition, or unduly interfere with or diminish opportunities for content providers.”⁵⁷

⁵⁵ Tim Wu, *Network Neutrality, Broadband Discrimination*, 2 J. ON TELECOMM. & HIGH TECH. L. 141 (2003). Available at: https://scholarship.law.columbia.edu/faculty_scholarship/1281

⁵⁶ See article “India just approved net neutrality rules that ban ‘any form’ of data discrimination” 7 November 2018 (Accessible at <https://www.theverge.com/2018/7/11/17562108/india-department-of-telecommunications-trai-net-neutrality-proposal-approval>)

⁵⁷ Net Neutrality: An overview of Net Neutrality by Media Defence (Accessible at <https://www.mediadefence.org/ereader/publications/advanced-modules-on-digital-rights-and-freedom-of-expression-online/module-5-trends-in-censorship-by-private-actors/net-neutrality/#:~:text=The%20UNSR's%202017%20Report%20focused,treated%20equally%20without%20undue%20interference.>)

India is one of the few countries that have adopted clear norms as regards net neutrality.⁵⁸ The department of Telecommunications approved rules that provide clear directions for ISPs as regards the neutrality of the internet. The key essentials of the principle prohibit blocking, throttling and paid prioritization. The rule states amongst others that “any form of discrimination or interference” with data, including “blocking, degrading, slowing down, or granting preferential speeds or treatment to any content.” But they don’t apply to “critical IoT services” or “specialized services,” is prohibited.

The net neutrality principle is considered important in today’s discourse and for the future of the digital environment as it promotes an environment that encourages healthy competition, innovation, and a levelled platform for growth and development. Therefore, net neutrality necessitates a free and open internet, which is essential for maximizing opportunities for free expression, innovation, and economic growth. That is, ensuring that the internet maintains its democratic values and openness. This means that State and non-State actors, particularly companies that control vital communications infrastructures, should not be allowed to exploit that control to restrict access, expression, or innovation. Where governments use any form of advance technology or networking equipment to censor content, track internet users, or intercept internet communications, the democratic nature of the internet may be compromised, which may also foster and give room to diverse human rights violations.

The value of providing an Internet that is free from arbitrary interference has been widely acknowledged by international bodies and experts. In 2014, the UN Human Rights Council called upon “all States to promote and facilitate access to the Internet, and international cooperation aimed at the development of media and information and communication facilities and technologies in all countries.

PRIVACY

The right to privacy and the need to protect personal information has gained grounds over the years and increasingly become topical as a result of the increase in the spread of internet access and the digitization of every aspect of life. As a result of increased reliance on the internet and virtual life, there has been an increase in online dissemination of information and data collection. This has made it imperative for the protection of the right to privacy and data collection, storage and use.

58

The right to privacy is provided for under Article 17 of the International Covenant on Civil and Political Rights as follows:

- “(1) No one shall be subjected to arbitrary or unlawful interference with his privacy, family, home or correspondence, nor to unlawful attacks on his honour and reputation.**
- (2) Everyone has the right to the protection of the law against such interference or attacks.”**

The Nigerian 1999 Constitution as amended provides in Section 37 that:

“The privacy of citizens, their homes, correspondence, telephone conversations and telegraphic communications is hereby guaranteed and protected.”⁵⁹

This right protects the privacy of Nigerian citizens, that is, their personal lives and information.

However, in the information age there has been an increasing intrusion into the privacy of citizens, both from governments and individuals. Interferences from government have been in the forms of the use of modern technologies, such as surveillance tools that are exploited to penetrate the privacy of citizens. A major surveillance tool that has been allegedly employed is Pegasus spyware.

The Pegasus is a spyware developed by the Israeli cyber-arms company NSO Group for the main purpose of intruding the privacy of targeted individuals. The spyware is usually marketed to governments as a digital tool that can breach barriers installed on electronic devices, particularly mobile phones in order to fight crimes such as terrorism.⁶⁰ Barriers erected on mobile devices are usually in the forms of encoding, known as encryption. Encryption is a process that allows individuals to protect their information from intrusion from third parties. It is one of the processes that have been regarded as a valuable tool for online freedom of expression, as it permits journalists, lawyers, human rights activists, and citizens to communicate in a safe manner. This process is particularly significant for journalists whose jobs are to uncover corruption cases, issues of abuse of power, and human rights violations. This is a highly veritable technology for a country like Nigeria where protection of whistleblowers is abysmal.

⁵⁹ The Constitution of the Federal Republic of Nigeria, 1999 (as amended) (Constitution).

⁶⁰ Pegasus spyware and its implications on human rights by the Council of Europe (accessible at <https://rm.coe.int/pegasus-spyware-report-en/1680a6f5d8>)

Unfortunately, tools like Pegasus are a danger to encryption as it operates covertly and remotely to uncover confidential information and expose whistleblowers that are unable to protect themselves and their families. The spyware once attached to a device, phone or laptop, begins to monitor the activities of the device without the user's knowledge. The spyware usually has access to passwords, accounts, calls, emails, geolocation data, and even encrypted communications.

In 2021, it was reported that the Nigerian National Assembly for instance, approved the whopping sum of N4.8 Billion Naira to the National Intelligence Agency (NIA) to monitor and spy on its citizens WhatsApp chats, text messages and phone calls.⁶¹ The NIA would spend N2,938,650,000 on the Thuraya interception solution, while the WhatsApp interception solution would gulp N1, 931,700,000.

The government of Nigeria allocated 2.2 billion naira (\$6.6 million) in its 2018 budget for a “Social Media Mining Suite,” having already ordered the military to watch for antigovernmental contents online. An example is the arrest of human rights activist Ibrahim Garba Wala, known as IG Wala, who was sentenced in April 2022 to 12 years imprisonment for criminal defamation, public incitement, and unlawful assembly, for charges stemming from Facebook posts alleging corruption in the National Hajj Commission.⁶²

It is noted that some governments have introduced legislation expressly authorizing the use of spyware under the guise of protecting national security and public safety. One of such law is the Lawful Interception of Communications Regulations⁶³ of the Nigerian Communications Commission (NCC). The regulation was made pursuant to the provisions of Section 70 of the Nigeria Communications Act, which empowers the NCC to make and publish regulations in relation to, amongst other things, the licenses granted or issued under the Act. It is also provided under sections 147 and 148 of the Act that the NCC is empowered to order interception of communications during a public emergency or in the interest of public safety.

⁶¹ <https://investorsking.com/2021/07/12/national-intelligence-agency-receives-n4-87-budget-to-track-conversations/#:~:text=The%20National%20Assembly%20has%20approved,is%20part%20of%20the%20N895>.

⁶² <https://freedomhouse.org/report/freedom-on-the-net/2019/the-crisis-of-social-media/social-media-surveillance> (accessed 05/05/2022)

⁶³ Lawful Interception of Communications Regulation of 2019 (Accessed at <https://ncc.gov.ng/docman-main/legal-regulatory/regulations/839-lawful-interception-of-comunications-regulations-1/file>)

The regulation was enacted for the purpose of providing the legal and regulatory framework for the lawful interception, collection, and disclosure of intercepted communications in Nigeria. Its aim is to specify the nature and types of communications that can be intercepted whilst prescribing penalties for non-compliance with its provisions. The NCC by virtue of its Nigerian Communications Act mandates operators in the telecommunications space to install equipment with interception capability that allows law enforcement agencies on the occurrence of any public emergency or in the interest of public safety to access communication data.⁶⁴

The regulation provides that communications can be intercepted lawfully with or without a warrant. By virtue of Section 7 of the regulation, a Licensee can approach the Court for the issuance of a warrant to intercept communications. The section provides as follows:

7.—(1) Subject to these Regulations, a Licensee shall act upon a warrant issued by a Judge authorising or requiring the Licensee to whom it is addressed to comply with the provisions of the warrant, to secure any one or more of the following— (a) intercept any communication as described in the warrant ; (b) disclose, in such a manner as may be described in the warrant of such intercepted communication ; or (c) assist foreign authorities in accordance with an international mutual assistance agreement ; provided that there is no other lawful means of investigating the matter for which the warrant is required. (2) Except as provided in these Regulations, a Judge shall not issue a warrant unless— (a) the warrant is necessary in compliance with paragraph (3) of this regulation ; and (b) such information can only be obtained by lawfully intercepting such Communication as specified in the warrant. Is within any of the following grounds— (a) it is in the interest of the national security as may be directed by the persons listed in regulation 12(1) (a) or (b) of these Regulations ; (b) for the purpose of preventing or investigating a crime ; (c) for the purpose of protecting and safeguarding the economic wellbeing of Nigerians ; (d) in the interest of public emergency or safety ; or (e) giving effect to any international mutual assistance agreements, which Nigeria is a party.

The same regulation also provides for the interception of communications without warrant in Section 8 which provides that:

8. The interception of communication of any person shall be lawful where— (a) one of the parties to the communication has consented to the interception, provided that an incontrovertible proof of such consent is available ; (b) it is done by a person who is a party to the communication, and has sufficient reason to

⁶⁴ See Section 10 of the 2019 Regulation

believe that there is a threat to human life and safety ; and (c) in the ordinary course of business, it is required to record or monitor such communication.

It should be noted that by virtue of Section 45 of the 1999 Constitution of the Federal Republic of Nigeria (as amended), the right to privacy is not absolute and can be limited in circumstances listed under that provision. Section 45 provides:

45. (1) Nothing in sections 37, 38, 39, 40 and 41 of this Constitution shall invalidate any law that is reasonably justifiable in a democratic society

(a) in the interest of defence, public safety, public order, public morality or public health; or

(b) for the purpose of protecting the rights and freedom of other persons

(2) An act of the National Assembly shall not be invalidated by reason only that it provides for the taking, during periods of emergency, of measures that derogate from the provisions of section 33 or 35 of this Constitution; but no such measures shall be taken in pursuance of any such act during any period of emergency save to the extent that those measures are reasonably justifiable for the purpose of dealing with the situation that exists during that period of emergency:

Provided that nothing in this section shall authorise any derogation from the provisions of section 33 of this Constitution, except in respect of death resulting from acts of war or authorise any derogation from the provisions of section 36(8) of this Constitution.

(3) In this section, a " period of emergency" means any period during which there is in force a Proclamation of a state of emergency declared by the President in exercise of the powers conferred on him under section 305 of this Constitution.

Ordinarily, Section 45 permits a law or regulation to curtail the enjoyment of the right to privacy once it is reasonably justifiable in a democratic society, in the interest of defence, public safety, public order, public morality or public health. This has been the justification put forward for the existence of this provision. However, the regulation also makes provision for interception where warrant is not obtained. It provides for situations where *“one of the parties to the communication has consented to the interception...”*

This is referred to as consensual interception of communication. There have been arguments for the consensual interception of communication. The views have expressed that consensual interception, without warrant, may be appropriate in criminal cases involving circumstances where the credibility of informants are in question as to the veracity of the information they have provided, and in situations involving victims of crimes where the conversation is between them and the perpetrators.⁶⁵ It is believed that in cases as this recording of conversation would serve the purpose of incontrovertible reliable evidence since it would prevent the informant from denying the existence of such a conversation. In line with this argument also is the issue of organized criminal activity which requires cogent and sufficient evidence for the prosecution of offenders. In most cases, law enforcement may rely on covert interception of communications, which may

⁶⁵ American Bar Association *“ABA PROJECT ON STANDARDS FOR CRIMINAL JUSTICE: STANDARDS RELATING TO ELECTRONIC SURVEILLANCE, 126 (1971)*

include undercover activities. The arguments may be made that it was reasonably and legally impossible to obtain a warrant in such a circumstance. Hence this may be accepted as a permissible case depending on the fact of each case.

However, such provisions may leave room for abuse without the discretion of the Court, which should be the umpire to decide the legitimacy of an interception and also to exercise such discretion within the purview of the rule of law and constitutionality. It is very critical for the Courts to consider if having access to another person's communication is appropriate just because one of the parties to a communication consent to it. Doesn't that amount to prioritization of one person's right over another? The fact is that any legislation that requires the interference with a human right like that of privacy must pass through judicial review otherwise that legislation leaves room for the mismanagement of state powers and the violation of privacy rights. Therefore, where there is no judicial oversight there is potential for abuse of power.

The argument against interception of communications without a warrant was presented before the Court in the case of *United States v. Kline*⁶⁶, where the Judge, Gerhard Gesell, stated as follows:

A Government agent can plant a broadcasting transmitter in a person's home, car or office without Court approval and transmit conversation of a consenting informer so long as the informer's presence is known and accepted by the other occupants even though they are completely unaware of and indeed affirmatively misled as to the informer's purpose. This is an enormously dangerous and insidious power to place in the unsupervised hands of the public and the police. There are no restrictions as to time, place or circumstances. Without court supervision, abuses will continue unchecked. We are becoming a society that must exist in constant hazard from official snooping. Whatever incidental good flows from this invasion of privacy is submerged by the growing appearance of police surveillance so typical of totalitarian states.

In 2021, the Constitutional Court of South Africa⁶⁷ was presented with the case of a South African journalist who found out that his communication had been

⁶⁶ *United States v. Kline* 366 F. Supp. 994, 996-97 (D.D.C. 1973)

⁶⁷ The case of AMABHUNGANE CENTRE FOR INVESTIGATIVE JOURNALISM NPC AND ANOTHER V MINISTER OF JUSTICE AND CORRECTIONAL SERVICES AND OTHERS; MINISTER OF POLICE V AMABHUNGANE CENTRE FOR INVESTIGATIVE JOURNALISM NPC AND OTHERS CCT278/19 & CCT279/19 (Accessed at <https://www.concourt.org.za/index.php/judgement/383-amabhungane-centre-for-investigative-journalism-npc-and-another-v-minister-of-justice-and-correctional-services-and-others-minister-of-police-v-amabhungane-centre-for-investigative-journalism-npc-and-others-cct278-19-cct279-19>)

monitored and intercepted by law enforcement. He argued before the High Court of North Gauteng that the Regulation of Interception of Communications and Provision of Communication-Related Information Act (RICA) did not provide for any system of notification, even after the acts of surveillance had taken place, to inform the subject of surveillance that they had been subject to surveillance, which meant that a subject would not normally learn of the surveillance and could not challenge the lawfulness of such action. The Act permitted the surveillance of individuals once an *ex parte* (“for one party”) application, is presented before a Court, which meant that the subject of such a warrant would not be given an opportunity to counter arguments made against the state agency’s request. The High Court Judge after considering the arguments held as follows:

“that RICA was unconstitutional, finding that the failure to provide for any notification to the subject; the lack of safeguards to protect against the negative effect of *ex parte* applications and the risk of surveillance of journalists and lawyers... The High Court also held that the management of data under RICA was unconstitutional and that the bulk surveillance undertaken by the National Communication Centre was unlawful.”⁶⁸

The matter was further presented before the Constitutional Court. The Court acknowledged the importance of the right to privacy, which is tied to dignity. It also accepted that state surveillance is important to investigate and combat serious crime, guarantee national security, and maintain public order. The question the court asked was whether RICA was doing enough to reduce the risk of unnecessary intrusions to people’s rights. It held that the Act did not provide adequate safeguards to protect the right to privacy. The court found that limiting the right to privacy in those circumstances was unjustifiable and unreasonable and found that RICA is unconstitutional.⁶⁹

Similarly, the European Court of Human Rights was approached to determine the legality of surveillance legislation in Russia in the case of Roman Zakharov v. Russia.⁷⁰ The case was brought by Roman Zakharov, who complained that the

⁶⁸ Global Freedom of Expression case analysis found at <https://globalfreedomofexpression.columbia.edu/cases/amabhungane-centre-for-investigative-journalism-v-minister-of-justice-and-minister-of-police-v-amabhungane-centre-for-investigative-journalism/>

⁶⁹ <https://www.michalsons.com/blog/biometrics-and-data-protection-law-around-the-world/42094>

⁷⁰ Zakharov V. Russia-47143/06 Judgment of 4 December 2015
<https://hudoc.echr.coe.int/fre#%22itemid%22:%22002-10793%22>

Russian law did not have sufficient safeguards against arbitrariness and abuse by authorities and that this violated his right to respect for private life.

The Court considered that to carry out surveillance, law enforcement should receive judicial authorization because there is a need for an independent body to oversee the implementation of such surveillance. The Court stressed that while Russia's interception of communications pursued the legitimate aims of protecting national security and public safety, the prevention of crime and the protection of the economic well-being of the country, it needed to have adequate and effective guarantees against abuse.

It stated that the data retention regime in Russia that allows it to automatically store irrelevant data for six months could not be considered justified under Article 8 of the EU Convention on human rights. It also reiterated that the scope and duration of surveillance should be targeted and necessary in a democratic society, and it must not be excessive. It held that Russia's laws governing surveillance did not provide adequate safeguards against abuse by state agents and others and that citizens should be made aware of surveillance legislation that can be used against them. According to the Court, *"...the domestic legal provisions governing the interception of communications did not provide adequate and effective guarantees against arbitrariness and the risk of abuse. The domestic law did not meet the "quality of law" requirement and was incapable of keeping the "interference" to what was "necessary in a democratic society"*.

In addition to the above, the AU Declaration on surveillance⁷¹ has clearly emphasized that "states shall not engage in or condone acts of indiscriminate and untargeted collection, storage, analysis or sharing of a person's communications". Targeted surveillance, on the other hand, must be "authorised by law" and has to be "premised on specific and reasonable suspicion that a serious crime has been or is being carried out or for any other legitimate aim".

The least expected for the surveillance or interception of communication to be justifiable is that such surveillance must be authorized by an independent, impartial and competent judicial authority, certifying that the request is necessary and

⁷¹ Resolution on the deployment of mass and unlawful targeted communication surveillance and its impact on human rights in Africa - ACHPR/Res.573 (LXXVII) 2023 (Accessible at <https://achpr.au.int/en/adopted-resolutions/573-resolution-deployment-mass-and-unlawful-targeted-communication>)

proportionate. This was the opinion of the UN Special Rapporteur on freedom of opinion and expression.⁷²

Data Protection and Data Privacy

Data Protection involves the legal safeguards that are provided for the protection of data stored in computers. It could also be referred to as legal regulation/control/governance over the access to, processing of and use of data stored in computers. Data protection is in fact the legal mechanism that ensures privacy of personal information.⁷³

Data privacy generally means the ability of a person to determine for themselves when, how, and to what extent personal information about them is shared with or communicated to others. This involves the protection of sensitive information from unlawful intrusion. This personal information can be one's name, location, contact information, or location. It is a discipline intended to keep data safe against improper access, theft or loss.

Generally, personal information is information about a natural person, an identifiable living person, which includes data peculiar to that person, in the forms of identity- name, signature, facial structure, address, phone number, thumb impressions (prints), date of birth and emails; this includes other identifiers such as government issued IDs (NIN, Passport, vehicle license, voters card, etc), IP address, mobile device ID, location data, cookie identifier, video record of a person, photograph, and medical records.

The UN General Comment No.16 on article 17 of the ICCPR describes the protection of personal information as follows⁷⁴:

“The gathering and holding of personal information on computers, data banks and other devices, whether by public authorities or private individuals or bodies, must be regulated by law. Effective measures have to be taken by States to ensure that information concerning a person’s private life does not reach the hands of persons who are not

⁷² A/HRC/35/22: Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression on 30th March 2017 (Accessible at <https://www.ohchr.org/en/documents/thematic-reports/ahrc3522-report-special-rapporteur-promotion-and-protection-right>)

⁷³ The Extent to the Right to Privacy and Data Protection in Nigeria by Esher and Makarios Law (Accessible at <https://eshherandmakarioslaw.com/assets/resources/d1de87b4d97b68c5d88843fe2bdcf937.pdf>)

⁷⁴ UN Human Rights Committee (HRC) General Comment 16 on the right to privacy The Right to Respect of Privacy, Family, Home and Correspondence, and Protection of Honour and Reputation, 8 April 1988, HRI/GEN/1/Rev.9 (Vol. I). (Accessible at <https://www.globalhealthrights.org/wp-content/uploads/2013/10/General-Comment-16-of-the-Human-Rights-Committee.pdf>)

authorized by law to receive, process and use it, and is never used for purposes incompatible with the Covenant. In order to have the most effective protection of his private life, every individual should have the right to ascertain in an intelligible form, whether, and if so, what personal data is stored in automatic data files, and for what purposes. Every individual should also be able to ascertain which public authorities or private individuals or bodies control or may control their files. If such files contain incorrect personal data or have been collected or processed contrary to the provisions of the law, every individual should have the right to request rectification or elimination.”

The NDPA defines Personal Data as *“any information relating to an individual, who can be identified or is identifiable, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or one or more factors specific to the physical, physiological, genetic, psychological, cultural, social or economic identity of that individual.”*

This identifiable individual is also known as the Data Subject. The NDPA defines a Data Subject as *“an individual to whom personal data relates.”*

There is also the Data Controller, who is a legal entity, either private or public, either individual or company that determines the use or processing of personal data. This Data Controller controls the means and purpose for which personal information can be used, processed or accessed. This person is legally bound to ensure that the processing of personal information is done in compliance with internet privacy laws, such as the Nigeria Data Protection Act and other data protection legislations.

According to the NDPA, a Data Controller *“is an individual, private entity, public Commission or agency or any other body who or which, alone or jointly with others, determines the purposes and means of the processing of personal data.”* The Act defines a Data Processor as *“an individual, private entity, public authority, or any other body, who processes Personal Data on behalf of or at the direction of a Data Controller or another Data Processor.”*

There is also a Data Protection Authority (DPA), which usually is a regulatory body to monitor and enforce the provisions of a data protection law within a country or region.

Data privacy is also a branch of data security concerned with the proper handling of data consent, notice, and regulatory obligations. More specifically, practical data privacy concerns often revolve around:

1. Whether or how data is shared with third parties.
2. How data is legally collected or stored.
3. Regulatory restrictions.

The California Consumer Privacy Act (CCPA) defines personal information as information that identifies, relates to, describes, is reasonably capable of being associated with, or could reasonably be linked (directly or indirectly) with a particular person or household such as a real name, postal address, unique personal identifier, online identifier, email address, account name, social security number, driver's license number, license plate number, passport number, or other similar identifiers.

The following sanctions and remedies can be imposed for breach of data privacy:

Companies, activists, associations, and others can be authorized to exercise opt-out rights on behalf of California residents.

Companies that become victims of data theft or other data security breaches can be ordered in civil class action lawsuits to pay statutory damages between \$100 and \$750 per California resident and incident, or actual damages, whichever is greater, and any other relief a court deems proper, subject to an option of the California Attorney General's Office to prosecute the company instead of allowing civil suits to be brought against it.

A fine up to \$7,500 for each intentional violation and \$2,500 for each unintentional violation.

1. Privacy notices must be accessible and have alternative format access clearly called out.
2. Liability may also apply in respect of businesses in overseas countries who ship items into California.

The Nigeria Data Protection Act, 2023, was enacted among other things, to safeguard the fundamental rights and freedoms, the interests of data subjects, as guaranteed under section 37 of the Constitution and other relevant provisions. The NDPA retained and did not repeal the existing NDPR and its Implementation Framework. These documents are now to be read in conjunction with the NDPA; however, where there is any conflict in their provisions, the provisions of the NDPA are to prevail.

Every organization whose activities involve collecting and processing personal data of natural persons must comply with the minimum standards provided by law. The rights of the “Data Subjects” must be protected and the "Data Controllers" or "Data Processors" must comply with the laydown principles and obligations required by law. Section 34-38 of the Nigerian Data Protection Act 2023 provides for the rights of the Data Subjects. They are listed below as follows:

1. The right to obtain from a data controller, without constraint or unreasonable delay confirmation as to whether the data controller or a data processor operating on its behalf, is storing or otherwise processing personal data relating to the data subject.
2. The right to know the purposes of the processing, the categories of personal data concerned, the recipients to whom the personal data have been or will be disclosed.
3. The right to know where possible the period for which the personal data will be stored, or, if not possible, the criteria used to determine that period.
4. The right to a copy of data subject’s personal data in a commonly used electronic format, except to the extent that providing such data would impose unreasonable costs on the data controller, in which case the data subject may be required by the data controller to bear some or all of such costs ;
5. The right to correction or, if correction is not feasible or suitable, deletion of the data subject’s personal data that is inaccurate, out of date, incomplete, or misleading;
6. The right to erasure of personal data concerning the data subject, without undue delay where the data is no longer necessary.
7. The right to restriction of data processing pending the resolution of a request, objection by the data subject under the Act, or the establishment, exercise, or defence of legal claims.
8. The right to withdraw consent, a data subject shall have the right to withdraw, at any time, consent to the processing of personal data under this

Act and the data controller shall ensure that it is as easy for the data subject to withdraw, as to give consent.

9. The right to object, a data subject shall have the right to object to the processing of personal data relating to the data subject.
10. The right not to be subjected to automated decision making, a data subject shall have the right not to be subject to a decision based solely on automated processing of personal data, including profiling, which produces legal or similar significant effects concerning the data subject.
11. The right to safeguard the Data Subject rights, the data controller shall implement suitable measures to safeguard the data subject's fundamental rights, freedoms and interests, including the rights to obtain human intervention on the part of the data controller; express the data subject's point of view; and contest the decision.
12. The right to data portability, the Commission may make regulations establishing a right of personal data portability. This Right shall entitle the data subject to receive, without undue delay from a data controller, personal data concerning the data subject in a structured, commonly used, and machine readable format; transmit the personal data obtained to another data controller without any hindrance; and where technically possible, have the personal data transmitted directly from one data controller to another.

Processing of data

This is a method or the way in which data or personal information is collected, stored, retrieved, consulted, disclosed or shared. For processing of data to take place, there are certain principles that must be respected.

There are no general or unified instruments governing processing of data, however, different countries determine what amounts to data processing by the enactment of a data protection legislation. However, in 2022, the United Nations Special Rapporteur on the Right to Privacy released a report which served as guidance as to the harmonization of legislations in respect of identifying and defining the principles relevant to data protection. The report exposes and clarifies certain principles that must guide the use of personal data. It recognised the principles of legality, lawfulness and legitimacy, consent, transparency, purpose, fairness,

proportionality, minimization, quality, responsibility, and security in the context of data protection legislation should govern data privacy. In details, these principles are described as follows:

- a. **Consent and Confidentiality:** The consent of the data subject must be obtained, and such data must be kept confidential and not exposed to a third party.
- b. **Data Minimisation:** Collection of only data that is necessary to achieve a stipulated purpose. Thus, collection must be adequate and relevant.
- c. **Fairness and lawfulness:** Personal information must be processed fairly and lawfully. That is, must comply with stipulated conditions and caveats.
- d. **Collection and Storage for Specific Purposes:** Personal information must be collected and stored for a specific purpose (disclosed to the DS). It can't be obtained for a particular purpose and processed for another purpose.
- e. **Accuracy:** Personal information must be accurate and up-to-date and if not, ensure that this is corrected.
- f. **Storage Limitation:** Personal information must not be stored longer than necessary.
- g. **Security and non-transferability to countries without adequate protection:** Personal information, personal data must be given adequate security- Installation of appropriate technical tools to safeguard them; it must not be transferred to countries without an adequate level of protection of the rights and freedoms of data subjects.
- h. **Transparency and accountability:** Processing must be transparent, and the controller must be accountable for any use.

The NDPA defines processing *“as any operation or set of operations which is performed on Personal Data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise*

making available, alignment or combination, restriction, erasure or destruction, and does not include the mere transit of data originating outside Nigeria.”

Extraterritorial processing of data

This involves the Cross-border transfer of data. This involves the sharing of personal information between or amongst national jurisdictions. It encompasses any act of transmitting, sharing, or storing such data in countries outside its original country of collection, whether for business, regulatory, or technological purposes.

However, the collection, storage, and processing of personal data raises issues of personal data vulnerability. This is because transfer of information has become a more seamless process which enables individuals to share their personal data across international borders. The ease in the transfer of data raises critical issues of privacy and security, which can easily be breached especially as people continue to relate in the increasing fast paced and shrinking world. The ever-developing emerging technologies -such as Ai, IoT, ChatGPT and the likes also poses huge future problems.

Thus, issues like individuals’ privacy and security, confidentiality, legal compliance, and protection of data becomes more critical, especially when that data is transferred across borders as this data includes sensitive information such as financial details, health records, and personal identifiers that, if compromised, can generate data breaches and different forms of cybercrimes, such as, fraud, security hacker, ransomware, identity theft, phishing, malware, cyber espionage, etc.

A lot of jurisdictions have put limitations in place to control this process. Reasons for this include national security, protection from misuse of citizens’ personal information, and strengthening domestic economic capabilities in an increasingly technological world. These laws ensure that data sharing is conducted in a secure manner, with the subjects’ consent, so that they may be protected from cybersecurity risks.

The NDPA provides for a similar, but more comprehensive approach, to cross-border data transfers compared to the NDPR, which relied largely on inferences from the Implementation Framework.

A likely conflict may be the requirement of the approval of the Attorney General of the Federation for cross-border data transfer requests, including the adoption of countries listed on the Whitelist as countries with appropriate level of adequacy provision.

According to Section 2(2) of the NDPA, the NDPA will apply to businesses established in other jurisdictions where the businesses are involved in the processing of the Personal Data of Data Subjects in Nigeria.

The Act permits the transfer of personal data to another country only if there is adequate level of protection in that country, and the data controller or data processor is required to record the basis of such transfer and the adequacy of protection. Section 41-44 of the NDPA.

A data controller and data processor are under obligation to provide to the Commission a general description of the risks, safeguards, security measures and mechanisms to ensure the protection of the personal data.

Sections 41 of the NDPA provides that Personal Data can be transferred outside Nigeria where the recipient of the Personal Data is subject to a law, binding corporate rules, contractual clauses, code of conduct, or certification mechanism that affords an adequate level of protection with respect to the Personal Data in accordance with the NDPA.

The Nigeria Data Protection Commission has the responsibility to determine the capability or sufficiency of the data protection mechanisms in place in the recipient country by issuing guidelines that would measure compliance.

In this vein, the NDPC has the power to make regulations requiring Data Controllers and Data Processors to notify it of the measures in place to ensure adequacy of protection when transferring a Data Subject's Personal Data to a foreign country.

In addition, a level of protection is adequate if it upholds the principles that are substantially similar to the conditions for processing of personal data in the NDPA.

Thus, adequate level of protection as provided for by the Act means the capability or sufficiency of the data protection mechanisms in place in the recipient country. That is:

1. Personal data must be processed in a fair, lawful, and transparent manner.

2. Collection of data must be for specific, explicit, and legitimate purposes, and not be further processed in any way that is inconsistent with the original intent.
3. Personal data should be adequate, relevant, and limited to the minimum necessary for the purposes for which it was collected or processed.
4. The retention period for personal data should not be longer than necessary to achieve its lawful purposes.
5. Data must be kept complete, not misleading, and up to date.

Consistent with the central objective of the Act, businesses are required to process data in a manner that ensures appropriate protection against unauthorized or unlawful processing, access, loss, destruction, damage, or data breaches.

Apart from this, the Act laid down criteria for adequacy in Section 42 as follows:

- a. availability of enforceable data subject rights and the ability of a data subject to enforce such rights through administrative or judicial redress, and the rule of law;
- b. existence of any appropriate instrument between the Nigeria Data Protection Act and a competent authority in the recipient jurisdiction that ensures adequate data protection;
- c. access of a public authority to personal data;
- d. existence of an effective data protection law;
- e. existence and functioning of an independent, competent data protection, or similar supervisory authority with adequate enforcement powers; and
- f. adequacy of international commitments and conventions binding on the relevant country and its membership of any multilateral or regional organizations.

It should be noted that the adequacy protection has exceptions. The Act provides for conditions under which personal data may be transferred abroad in the absence of adequate protection. Section 43 provides these exceptions as:

- a. the Data Subject has provided and not withdrawn the consent to such transfer after having been informed of the possible risks of such transfers for the Data Subject due to the absence of adequate protection;

- b. the transfer is necessary for the performance of a contract to which a Data Subject is a party or in order to take steps at the request of a Data Subject, prior to entering into a contract;
- c. the transfer is for the sole benefit of a Data Subject; and
 - i. it is not reasonably practical to obtain the consent of the Data Subject to that transfer; and
 - ii. if it were reasonably practicable to obtain such consent, the Data Subject would likely give it;
- d. the transfer is necessary for important reasons of public interest;
- e. the transfer is necessary for the exercise or defence of legal claims; or
- f. the transfer is necessary to protect the vital interests of a Data Subject or of other persons, where a Data Subject is physically or legally incapable of giving consent.
- g. a general description of the risks, safeguards, security measures and mechanisms to ensure the protection of the personal data.

An important aspect of data privacy is that the right to privacy facilitates the enjoyment of the right to freedom of expression, in that, it allows individuals to share anonymous posts, which is highly beneficial for whistleblowers and journalists who need to protect their sources (and to make protected disclosures and enables journalists and activists to communicate securely beyond the reach of unlawful government interception).

FREEDOM OF EXPRESSION AND INFORMATION

The right to freedom of expression is a fundamental human right which is contained in article 19 of the Universal Declaration of Human Rights (UDHR) and it states: *“everyone has the right to freedom of opinion and expression, the rights includes freedom to hold opinions without interference and to seek, receive and impart information and ideas through any media and regardless of frontiers”*.

This right comprises of three core tenets: the right to hold opinions without interference (freedom of opinion); the right to seek and receive information

(access to information); and the right to impart information (freedom of expression).

The UN Human Rights Committee's (UNHRC) General Comment No. 34 on the ICCPR notes that the right to freedom of expression includes, for example, political discourse, commentary on one's own affairs and on public affairs, canvassing, discussion of human rights, journalism, cultural and artistic expression, teaching, and religious discourse.⁷⁵ It also embraces expression that may be regarded by some as deeply offensive.⁷⁶ The right covers communications that are both verbal and non-verbal, and all modes of expression, including audio-visual, electronic and internet-based modes of communication.⁷⁷

Article 19(2) of the ICCPR provides that the right to freedom of expression applies regardless of frontiers and through any media of one's choice. General Comment No. 34 further explains that article 19(2) includes internet-based modes of communication.⁷⁸

As earlier noted, the UN Human Rights Council has (UNHRC) affirmed that:⁷⁹

“[T]he same rights that people have offline must also be protected online, in particular freedom of expression, which is applicable regardless of frontiers and through any media of one's choice, in accordance with articles 19 of the Universal Declaration of Human Rights and the International Covenant on Civil and Political Rights.”⁸⁰

This was followed by the affirmation of the African Commission on Human and Peoples' Rights which recognised and called on states to respect and to take legislative and other measures to guarantee, respect and protect citizens' rights to freedom of information and expression through access to internet services.⁸¹

The exercise of this right is essential for guaranteeing human rights, democracy and the rule of law. Without free expression and free media, violations of human

⁷⁵ OHCHR, General Comment No. 34 at para 11. (2011) (accessible at:

<https://www2.ohchr.org/english/bodies/hrc/docs/GC34.pdf>).

⁷⁶ *Ibid* at para 11. For further discussion on this, see Nani Jansen Reventlow, 'The right to 'offend, shock or disturb', or the importance of protecting unpleasant speech' in Perspectives on harmful speech online: A collection of essays, Berkman Klein Center for Internet & Society, 2016 at pp 7-9 (accessible at: <http://nrs.harvard.edu/urn-3:HUL.InstRepos:33746096>).

⁷⁷ *Ibid* General Comment No. 34 at para 12.

⁷⁸ General Comment No. 34 above at n 4 at para 12.

⁷⁹ UNHRC, 'Resolution on the promotion, protection and enjoyment of human rights on the internet', A/HRC/32/L.20 (2016) at para 1 (accessible at: <https://digitallibrary.un.org/record/845728?ln=en>).

⁸⁰ See Media Defence *Module 1: Key principles of international law and freedom of expression (Accessible at <https://www.mediadefence.org/ereader/publications/introductory-modules-on-digital-rights-and-freedom-of-expression-online/module-1-key-principles-of-international-law-and-freedom-of-expression/>)*

⁸¹ ACHPR, 'Resolution on the right to freedom of information and expression on the internet in Africa', ACHPR/Res.362, (2016) (accessible at: <https://www.achpr.org/sessions/resolutions?id=374>).

rights may remain hidden with the propensity to give rise to impunity and continuous violations.

Freedom of expression is guaranteed in section 39 and 22 of the 1999 Constitution of the Federal Republic of Nigeria (as amended). Section 39 provides 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.”*

It is the duty of the government to provide a conducive environment that will enable the citizens’ exercise this right. Section 22 provides that *“The press, radio, television and other agencies of the mass media shall at all times be free to uphold the fundamental objectives contained in this chapter and uphold the responsibility and accountability of the Government to the people”*. A clear Interpretation of this section will mean that the press and the media have the duty to hold the government responsible and accountable to ensure the enjoyment and full realization of this right.

The right as envisaged under Section 39 of the Constitution comprises of:

- the right to hold opinions;
- the right to receive and share information;
- The right to express opinion in form and through all platforms including speech, art, music and other forms of creative communication.
- Online freedom of speech

The right to hold opinions

By the provision of section 39 (1) of the constitution, everyone have the right to hold or have opinion about any issue and the government, its agencies or any other person shall not compel or force others to change or silence their opinions or thoughts except in the situations where the law permits such limitations.

The right to receive and share information

By the provision of section 39 (1) of the Constitution every person has the right to request certain classes of information in the custody of the government and its agencies and to share such information with others without any form of intimidation.

Freedom of information Act (2011) provides the process to be followed by anyone who wants to access public information. This an Act to make public records and information more freely available, provide for public access to public records and

information, protect public records and information to the extent consistent with the public interest and the protection of personal privacy, protect serving public officers from adverse consequences of disclosing certain kinds of official information without authorization and establish procedures for the achievement of those purposes and; for related matters.(Preamble to the Act).

The right to free speech

By the provision of section 39 (1) this include expressing ideas to others in various means, including having conversations and speeches at protests that criticize government actions or personal speech expressing oneself. The government has the responsibility to protect free speech and by the provision of section 22 the press and the media has the duty to hold the government accountable towards this responsibility.

The right to express opinion in all form and through all platforms including speech, art, music and other forms of creative communication

The right to freedom of expression includes the right of citizens to express themselves in whatever form or ways they choose to this will include speech, music, arts and on whatever platforms, social media, newspapers, billboards, podcasts, online articles, blogs, vlogs, videos, animations or films.

The right to freedom of the press

The term “press” refers to television stations such as the Nigerian Television Authority owned and managed by the government, there are television stations owned by private individuals like Channels, Arise TV among others, newspapers companies such as Punch Newspaper, Guardian Newspaper and online news outlets including blogs, news websites and vlogs. To ensure that people have the right information, the press must be free to publish information on events happening in the country without fear of sanction or harassment by the government. This means, for example, that the government unlawfully attacks freedom of expression when they sanction the press for publishing information about the activities of the government.

For example, during the 2023 general elections the National Broadcasting Commission sanctioned about 25 broadcasting stations and issued warning to

about 16 broadcasting stations for alleged misconduct during the 2023 General elections.⁸²

In East Africa, the East African Court of Justice⁸³ upheld the right to freedom of expression in the case of **BURUNDI JOURNALISTS UNION V THE ATTORNEY GENERAL OF THE REPUBLIC OF BURUNDI**⁸⁴

The EACJ was called upon to determine if a Press Law which required accreditation of journalists before exercising their profession was not a violation of freedom of expression. The Court cited the provisions of Article 6(d) and 7(2) of the Treaty to hold that government of Burundi's Press Law No. 1/11, mandating an arbitrary accreditation scheme that compels journalists to obtain a press card before exercising their profession, violated freedom of expression.⁸⁵ *The Court held that "there is no doubt that freedom of the press and freedom of expression are essential components of democracy"*⁸⁶

The Court stated that *"under Articles 6(d) and 7(2), democracy must of necessity include adherence to press freedom"* and a *"free press goes hand in hand with the principles of accountability and transparency which are also entrenched in articles 6(d) and 7(2)"*⁸⁷

⁸²<https://punchng.com/election-nbc-sanctions-25-broadcast-stations-gives-16-final-warning/>)

⁸³ The EAC although not having a specific human rights mandate like the Ecowas Court, makes reference to human rights in terms of good governance in Articles 6(d) and 7 (2) of EAC Treaty (Accessible at <https://investmentpolicy.unctad.org/international-investment-agreements/treaty-files/2487/download>). Article 6(d) provides that "The fundamental principles that shall govern the achievement of the objectives of the Community by the partner states shall include: ... (d) good governance including adherence to the principles of democracy, the rule of law, accountability, transparency, social justice, equal opportunities, gender equality, as well as the recognition, promotion and protection of human and peoples' rights in accordance with the provisions of the African Charter on Human and Peoples' Rights." While Article 7(2) provides that Member States should abide by the principles of rule of law, democracy, social justice and the maintenance of universally accepted standards of human rights. A combined reading of these have culminated in courageous interpretations of good governance to the preservation of human rights. See **East African Court of Justice – a custodian of Internet freedom in the Great Lakes Region** by Christopher Yaw Nyinevi Yohannes & Eneyew Ayalew on November 28, 2022 (Accessible at <https://www.afronomiclaw.org/category/analysis/emerging-role-african-sub-regional-courts-protecting-human-rights-internet>)

⁸⁴ Reference No 7 of 2013 (15 May 2015), (Accessible at <https://globalfreedomofexpression.columbia.edu/cases/burundian-journalists-union-v-attorney-general/>) ; See also European Court of Human Rights, *Lingens v Austria* App no 9815/82 (8 July 1986), paras 41 and 42; and Inter-American Court of Human Rights, *Herrera-Ulloa v Costa Rica* Series C No 107 (2 July 2004), para 117

⁸⁵ Id. Paragraph 123

⁸⁶ Id, para 80

⁸⁷ Id. Para 83

Also, in the case of **MEDIA COUNCIL OF TANZANIA V. ATTORNEY GENERAL**, the applicants challenged the Media Services Act, 120 of 2016 (the Act) in the East African Court of Justice. They sought the Court’s decision on “whether “the Act in its current form is an unjustified restriction on the freedom of expression which is a cornerstone of the principles of democracy, rule of law, accountability, transparency and good governance, which are obligations mandated on the country under the EAC Treaty”⁸⁸ They argued that the Act infringed articles 6(d), 7 and 8 of the Treaty for the Establishment of the East African Community. The Media Council submitted that the Act contains several problems. It argued that the Act restricted different types of news or content without reasonable justification; it introduced a mandatory accreditation for journalists and gave power to the Board of Accreditation to withdraw accreditation; it criminalized defamation, false news and rumours and seditious statements; and it conferred on the Minister absolute power to prohibit importation of publications and sanction media content⁸⁹

The government however argued that the criminal offences and the power given to the Minister under the Act did not violate freedom of expression. He argued that the right to freedom of expression is not absolute, that the accreditation requirements “provide the rights and obligations of a media house and the manner in which they should conduct themselves” and serve as “an oversight and control mechanism over the journalism profession for scrutiny, statistics and growth” It concluded that the Act was justifiable on the grounds that it sought to give effect to the protection of the right to freedom of expression in article 18 of the Tanzanian Constitution by protecting the rights and interests of individuals and of the public.

The Court citing its Judgement in *Burundian Journalists Union v. Attorney General of the Republic of Burundi*, stated that “there is no doubt that freedom of the press and freedom of expression are essential components of democracy”⁹⁰ The Court delved into the question of the applicability of Articles 6 (d)⁹¹, 7(2)⁹² and 8⁹³ of the Treaty and analysed the provision of Section 7(3) of the Act, which mandated media houses to refrain from publishing information that undermine the national security or lawful investigation, does not impede due process of law or endanger any person; does not constitute hate speech; does not disclose Cabinet

⁸⁸ Id. Para 5

⁸⁹ Id. Para 12

⁹⁰ Id. 58. See also *R v. Oakes 1986 ISCR 103* and *CORD v. Kenya HC Petition no 628 of 2014*

⁹¹ Quoted supra.

⁹² Quoted supra.

⁹³ This provides that member states should “abstain from any measures likely to jeopardise the achievement of [the Treaty’s] objectives or the implementation of the provisions of this Treaty”.

proceedings; does not facilitate or encourage the commission of an offence; does not involve an unwarranted invasion of an individual’s privacy; does not infringe lawful commercial interests; does not cause substantial harm to the Government to manage the economy; or does not infringe the holder of the information’s ability to consider whether to provide the information and their professional privilege or position in legal proceedings. The Court applied the three-part test as provided under Article 19(3) of the ICCPR stated as follows:

“(a) is the limitation one that is prescribed by Law? It must be part of a Statute, and must be clear, and accessible to citizens so that they are clear on what is prohibited: (b) Is the objective of the law pressing and substantial? It must be important to the society; and (c) Has the State, in seeking to achieve its objectives chosen a proportionate way to do so? This is the test of proportionality relative to the objectives or purpose it seeks to achieve”⁹⁴

It also applied the judicial reasoning in the case of *Konaté v. Burkina Faso*, which was decided by the African Court⁹⁵ and concluded that the Media Act failed to meet the requirements that the law must not be vague, unclear or imprecise and that means the law did not meet the criteria “prescribed by law”. It also held that “the word ‘undermine’ which forms the basis of the offence, is too vague to be of assistance to a journalist or other person, who seeks to regulate his or her conduct”⁹⁶; and further held that the Respondent “failed to establish either that there was a legitimate aim being pursued ... or indeed that the said limitations are proportionate to any such aim”⁹⁷

The EACJ unanimously held that several of the provisions in the Tanzania’s Media Services Act violated the Treaty for the Establishment of the East African Community as they infringed the right to freedom of expression.

THE THREE-PART TEST

The three-part test is a test provided for under Article 19 (3) of the International Covenant on Civil and Political Rights (ICCPR). The article 19 provides:

1. Everyone shall have the right to hold opinions without interference.

⁹⁴ Id.60

⁹⁵ African Court on Human and Peoples’ Rights, *Konaté v Burkina Faso* App no 004/2013 (5 December 2014)

⁹⁶ Case analysis by the Columbia Global Freedom of Expression accessed at <https://globalfreedomofexpression.columbia.edu/cases/media-council-of-tanzania-v-attorney-general/>

⁹⁷ Id. Para 75

2. 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 in print, in the form of art, or through any other media of his choice.

3. The exercise of the rights provided for in paragraph 2 of this article carries with it special duties and responsibilities. It may therefore be subject to certain restrictions, but these shall only be such as are provided by law and are necessary:

(a) For respect of the rights or reputations of others;

(b) For the protection of national security or of public order (ordre public), or of public health or morals.

Under most international treaties, grounds upon which the right to freedom of expression may be restricted are that the restriction must be provided by law, serve a legitimate aim (respect of the rights and reputations of others, protection of national security or of public order, or of public morals or health) and meet a high standard of necessity.

By virtue of Article 19(3), a limitation or restriction on the right to freedom of expression will only be justifiable where it is (i) provided by law, (ii) serves a legitimate interest, and (iii) is necessary and proportional in a democratic society. Therefore, any government or institution restricting this right must satisfy the tests which are cumulative in application.

RESTRICTIONS MUST BE PROVIDED BY LAW

The first test states that a restriction must be provided by law, that is, any measure for restricting or limiting the right to freedom of expression must be such that is “pursuant to a law that is formulated with sufficient precision to enable an individual to regulate his or her conduct accordingly; it must be made accessible to the public; may not confer unfettered discretion for the restriction of freedom of expression on those charged with its execution; and Laws must provide sufficient guidance to those charged with their execution to enable them to ascertain what sorts of expression are properly restricted and what sorts are not.”⁹⁸

The explanation of the UN Human Rights Council in General Comments 34⁹⁹ provides clarity as to the expectation of this criterion as follows:

- a. The law may include laws of parliamentary privilege and laws of contempt of court. Since any restriction on freedom of expression constitutes a serious curtailment of human rights, it is not compatible with the Covenant for a

⁹⁸ UN Human Rights Committee, *General Comment No 34: Article 19: Freedoms of opinion and expression* UN Doc CCPR/C/GC/34 (12 September 2011), para 25

⁹⁹ *Supra*

restriction to be enshrined in traditional, religious or other such customary law.

- b. Laws restricting the rights enumerated in article 19 must also themselves be compatible with the provisions, aims and objectives of the Covenant.
- c. Laws must not violate the non-discrimination provisions of the Covenant.
- d. Laws must not violate the non-discrimination provisions of the Covenant. Laws must not provide for penalties that are incompatible with the Covenant, such as corporal punishment.
- e. The State party must demonstrate the legal basis for any restrictions imposed on freedom of expression. The State party should provide details of the law and of actions that fall within the scope of the law.

The Committee identified legitimate grounds for restrictions as provided under Article 19 as follows:

- a. For the respect of the rights or reputations of others. The term “rights” includes human rights as recognized in the Covenant and more generally in international human rights law. For example, it may be legitimate to restrict freedom of expression in order to protect the right to vote under article 25, as well as rights article under 17. Such restrictions must be constructed with care: while it may be permissible to protect voters from forms of expression that constitute intimidation or coercion, such restrictions must not impede political debate, including, for example, calls for the boycotting of a non-compulsory vote. Such restrictions must be constructed with care: while it may be permissible to protect voters from forms of expression that constitute intimidation or coercion, such restrictions must not impede political debate, including, for example, calls for the boycotting of a non-compulsory vote. Thus, it may, for instance, refer to individual members of a community defined by its religious faith or ethnicity.
- b. For the protection of national security or of public order (ordre public), or of public health or morals. Extreme care must be taken by States parties to ensure that treason laws and similar provisions relating to national security, whether described as official secrets or sedition laws or otherwise, are crafted and applied in a manner that conforms to the strict requirements of upholding freedom of expression, which is a necessary condition for the realization of the principles of transparency and accountability that are, in turn, essential for the promotion and protection of human rights. Such laws are not compatible, for instance, when they are invoked to suppress or withhold from the public information of legitimate public interest that does

not harm national security or to prosecute journalists, researchers, environmental activists, human rights defenders, or others, for having disseminated such information. Nor is it generally appropriate to include in the remit of such laws such categories of information as those relating to the commercial sector, banking and scientific progress.

RESTRICTIONS MUST PURSUE A LEGITIMATE AIM

The second test states that any restriction on freedom of expression must be necessary for a legitimate purpose. This means that such restrictions must have due regards to the aims provided under Article 19(3) of the ICCPR, Article 27(2) of the African Charter, and the countries' Constitution.

By virtue of Article 27(2) of the African Charter justification for a restriction or limitation must be necessarily based on the simple fact that it is done having due regards for the rights of others, including collective security, morality and common interest.

The rights and freedoms of each individual shall be exercised with due regard to the rights of others, collective security, morality and common interest.

RESTRICTIONS MUST BE NECESSARY IN A DEMOCRATIC SOCIETY

The third test is of two folds. One of end, it requires that any restriction on freedom of expression must be that which is obtainable in a democratic society, meaning that the strict tenets of democracy, including the rule of law and due process must be enjoy complete compliance for any State to justify a restriction. Annexed to this part is the second fold which requires that any measure adopted to restrict or limit the freedom of expression must necessarily be proportionate to the legitimate aim which it claims to pursue. This means that a restriction, according to the Committee, must not be “overboard”. It states:

- a.** The Committee observed in general comment No. 27 that “restrictive measures must conform to the principle of proportionality; they must be appropriate to achieve their protective function; they must be the least intrusive instrument amongst those which might achieve their protective function; they must be proportionate to the interest to be protected...The principle of proportionality has to be respected not only in the law that

frames the restrictions but also by the administrative and judicial authorities in applying the law”

- b. The principle of proportionality must also take account of the form of expression at issue as well as the means of its dissemination. For instance, the value placed by the Covenant upon uninhibited expression is particularly high in the circumstances of public debate in a democratic society concerning figures in the public and political domain.
- c. When a State party invokes a legitimate ground for restriction of freedom of expression, it must demonstrate in specific and individualized fashion the precise nature of the threat, and the necessity and proportionality of the specific action taken, in particular by establishing a direct and immediate connection between the expression and the threat.
- d. a State party, in any given case, must demonstrate in specific fashion the precise nature of the threat to any of the enumerated grounds in par 3 that has caused it to restrict freedom of expression

In furtherance to the above clarification by the Committee, the African Commission on Human and Peoples' Rights in the case of **ZIMBABWE LAWYERS FOR HUMAN RIGHTS & ASSOCIATED NEWSPAPERS OF ZIMBABWE V ZIMBABWE**,¹⁰⁰ enunciated that at every point in time when the measure of proportionality is being considered under Article 19(2) of the ICCPR and Article 9 of the African Charter, five guiding questions must be asked:

“Were there sufficient reasons to justify the action? Was there a less restrictive alternative? Was the decision-making process procedurally fair? Were there any safeguards against abuse? Does the action destroy the essence of the rights guaranteed by the Charter?”¹⁰¹

Therefore, for a claim to a right of freedom of expression especially the right to search and receive information (see Article 9(1) and (2) of the African Charter on Human and People’s Rights) freely to succeed, the applicant must establish that.

¹⁰⁰ African Commission on Human and Peoples' Rights, *Zimbabwe Lawyers for Human Rights & Associated Newspapers of Zimbabwe v Republic of Zimbabwe* Communication No 284/03 (3 April 2009)

¹⁰¹ *id.*, para 176

(1) the right to freedom of expression has been interfered with or disrupted. For example, shutdown or restricting internet access interferes with freedom of expression.

(2) the interference or disruption, as the case maybe, were not sanctioned or done in accordance with the law. For example, is there a law in force that provides a mandate to shutdown internet access or is there any subsequent legislation to justify the shutdown of internet access?

(3) the interference does not pursue a legitimate interest. As the African Commission on Human and People's Rights have noted in a plethora of cases that "*the reasons for possible limitation must be based on legitimate public interest and the disadvantages of the limitation must be strictly proportionate to and absolutely necessary for the benefits to be gained.*"¹⁰² In other words, common interest is key.

(4) That the measures taken to interfere with the freedom of expression is not proportionate to the legitimate interest claimed to be pursued. In this, the claim must establish the fact that the measures taken in interfering is disproportionate and has a chilling effect on public discussions on matters of general interest. That in fact, the interference is not necessary in a democratic society.

In *MEDIA RIGHTS AGENDA, CONSTITUTIONAL RIGHTS PROJECT, MEDIA RIGHTS AGENDA, CONSTITUTIONAL RIGHTS PROJECT V. NIGERIA AFRICAN COMMISSION ON HUMAN AND PEOPLES' RIGHTS*,¹⁰³ the ACHPR dissected the salient issues for determination as follows:

66. According to Article 9.2 of the Charter, dissemination of opinions may be restricted by law. This does not mean that national law can set aside the right to express and disseminate one's opinions; this would make the protection of the right to express one's opinions ineffective. To allow national law to have precedence over the international law of the Charter would defeat the purpose of the rights and freedoms enshrined in the Charter. International human rights standards must always prevail over contradictory national law. Any limitation on the rights of the Charter must be in conformity with the provisions of the Charter.

¹⁰² *Media Rights Agenda, Constitutional Rights Project, Media Rights Agenda, Constitutional Rights Project v. Nigeria African Commission on Human and Peoples' Rights* Communication Nos. 105/93, 128/94, 130/94 and 152/96

¹⁰³ *Supra*. See also the case of *Faurisson v. France* Communication No. 550/1993 of 8 November 1996; *Murphy v. Ireland* European Court of Human Rights Application No. 44179/98; *Barfod v. Denmark* Application No. 11508/85, Judgement of 22 February 1989 and *von Hannover v. Germany*, Application No. 59320/00, Judgement of 24 June 2004.

67. In contrast to other international human rights instruments, the African Charter does not contain a derogation clause. Therefore limitations on the rights and freedoms enshrined in the Charter cannot be justified by emergencies or special circumstances.

68. The only legitimate reasons for limitations to the rights and freedoms of the African Charter are found in Article 27.2, that is that the rights of the Charter “shall be exercised with due regard to the rights of others, collective security, morality and common interest.”

69. The reasons for possible limitations must be founded in a legitimate state interest and the evils of limitations of rights must be strictly proportionate with and absolutely necessary for the advantages which are to be obtained.

70. Even more important, a limitation may never have as a consequence that the right itself becomes illusory.

73. In the present case, the government has provided no evidence that seizure of the magazine was for any other reason than simple criticism of the government. The article in question might have caused some debate and criticism of the government, but there seems to have been no information threatening to, for example, national security or public order in it. All of the legislation criticized in the article was already known to members of the public information, as laws must be, in order to be effective.

THE RIGHT TO ONLINE EXPRESSION

Online expression refers to sharing information, opinions or ideas through the internet. This includes using social media platforms like Facebook, WhatsApp, Instagram, TikTok and Twitter.

People share their opinions and advocate for causes through the internet especially the various social media channels and this enables people to have quick access to information on the internet without needing to leave the comfort of their homes.

There are instances when the Nigeria government has online freedom of expression of Nigerians. For example, In March 2022, the Carnegie Endowment for International Peace reported the government sometimes used platform-based blocking of internet service providers to shut down websites. Reports from prior years stated internet providers sometimes blocked websites at the request of the Nigerian Communications Commission, particularly websites advocating independence for Biafra in the Southeast region. On August 5, Minister of Information Lai Mohammed asked Google to block YouTube videos from terrorist organizations, specifically mentioning IPOB. Civil society organizations and journalists expressed concern regarding the broad powers provided by the law. Some local and state governments used the law to arrest journalists, bloggers, and critics for alleged hate speech. In July, the CPJ reported the arrest of two

employees of Bauchi-based Wikkitimes for criminal conspiracy, defamation, and cyberstalking after publishing a news report criticizing a local politician. Police held the reporters overnight and then released them on bail. Authorities dropped the cyberstalking charges but indicted the journalists on the criminal conspiracy and defamation charges.¹⁰⁴

From the above definition of the various principles of freedom of information contained in section 39 of the Constitution, one can infer that the government has a duty to respect, promote, protect and fulfil freedom of expression of the Nigerian citizens. This includes:

- A duty to refrain from restricting or interfering with citizens right to enjoy the right to freedom of expression.
- A duty to protect all citizens and groups in Nigeria from any intimidation or harassment to reduce their freedom of expression.
- A duty to ensure government agencies comply with international standards and that the laws which have been made to protect the right to freedom of expression conform with international laws and standards.
- A duty to take positive action to ensure people enjoy their rights without any interference.

This is the responsibility of the Nigerian government, its agencies and all the public bodies that form part of it.¹⁰⁵

The right to freedom of expression is one of those rights seen as very essential and fundamental to the development of a civilized society. It is the foundation for the enforcement of other rights, encroachment of which is made known by expression. A major determinant of a nation's respect for the rights of its people is the extent to which they can express themselves.

In IGP V. ANPP, the court of appeal described freedom of expression as the bone of democracy.

It is important to note that this right is not absolute. Though the public has a right to accurate information and fair comments, this must be balanced against other

¹⁰⁴ https://www.state.gov/wp-content/uploads/2023/03/415610_NIGERIA-2022-HUMAN-RIGHTS-REPORT.pdf

¹⁰⁵ https://nigeria.action4justice.org/legal_areas/right-to-freedom-of-expression-2/right-to-freedom-of-expression/

claims in the society which may often conflict except when overridden by public interest.

Thus, Section 39 (3) of the 1999 Constitution provides:

"Nothing in this section shall invalidate any law that is reasonably justifiable on a democratic society –

1. For the purpose of preventing the disclosure of information received in confidence, maintaining the authority and independence of courts or regulating telephone, wireless broadcasting, television or the exhibition of cinematograph films, or
2. Imposing restrictions upon persons holding office under the government of the federation or of a state, members of the armed forces of the federation or members of the Nigerian Police force or other government security services or agencies established by law.

Thus, in the light of these constitutionally permitted grounds, the following restrictions have been imposed by law;

Information received in confidence

Various issues come under this head:

State Privilege:

This has been defined as "the right of the state through its agents or functionaries to withhold evidence which it considers injurious to public interest or revealed in open court.

Official Secrets:

Provisions relating to the disclosure of official secrets are provided for under the Criminal Code and The Official Secrets Act.

Section 97 of the Criminal Code provides the mode of punishment for any person who being employed on the public service, publishes or communicates any fact which is meant to be secret.

Similarly, Section 1 (1) of the Official Secrets Act makes it an offence for anyone to transmit classified matters to anyone who is not authorized on behalf of the government to transmit it.

Contempt of Court

It is a limitation on the right to freedom of expression, exercised by the court in the course of the administration of justice. This is to ensure the absence of improper interference and obstructions of the court processes.

The exercise of this power stems from the authority of judges to control what happens in or around their court and is part of the inherent powers and sanctions of the Court under Section 6 (6) (a) of the 1999 Constitution.

Perjury

The offence of perjury affects the right to freedom of expression & the press and is directed towards the maintenance of the authority and independence of the courts.

Obscene and harmful publications

The basis for restriction here is in the interest of public morality. Under Section 2 of the Children and Young Person (Harmful Publications) Act, it is an offence to publish any book or magazine which is a kind likely to fall into the hands of children or young persons which portrays the commission of crimes, the acts of violence or cruelty, or incidence of a repulsive or horrible nature.

An article or matter is only obscene if its likely audience will be depraved or corrupted by it. The test of obscenity is whether the effect of the article in question upon that person is such as to deprave or corrupt him.

In *R V. Clayton*, on a charge of selling obscene photographs to 2 policemen, the court held that the charge against the accused person could not hold since the persons they sold the photographs to were not persons likely to be depraved or corrupted by it.

Sedition

This limitation is perhaps one of the most objectionable, perhaps because it infringes on freedom of expression in the political context. The offence of sedition is provided for in the Criminal & Penal Code.

In *DPP V. Chike Obi* where the appellant referred the Federal Supreme Court to the point whether or not the law of sedition contravened his right to freedom of expression guaranteed under Section 23 of the 1963 Constitution. The Supreme Court held that the law was "reasonably justifiable in a democratic society" and therefore was constitutional.

Defamation

Another way in which the right to freedom of expression is limited under the law relating to defamation of character. As was succinctly put by Lord Denning:

In *Tony Momoh V. The Senate House of Assembly*, the fact of such limitation on free speech was recognized. Section 45's general derogation clause also makes this limitation constitutional. For the purpose of protecting the rights & freedoms of other persons, which here is a person's right to a good reputation or a good name. Apart from the above stated grounds, Section 45 (1) of the 1999 Constitution also generally makes provisions for further restrictions: In the interest of defence, public safety, public order, public morality or public health and for the purpose of protecting the rights and freedoms of other persons.¹⁰⁶

FREEDOM OF ASSOCIATION AND ASSEMBLY

Freedoms of assembly refers to the right of individuals and groups to come together for a common purpose, either to express their views publicly, exchange ideas or hold a peaceful protest. The right to freedom of assembly can be enjoyed by every person; individuals, groups, associations (whether registered or unregistered), religious bodies, legal entities, and trade unions. It also extends to children, refugees, stateless persons, temporary visitors, migrants, and foreign nationals. Everyone regardless of ethnicity, gender, nationality, religion, language, social or marital status has this right.¹⁰⁷

The right to freedom of peaceful assembly and association is provided for in article 20 of the Universal Declaration of Human Rights as follows that:

1. Everyone has the right to freedom of peaceful assembly and association.
2. No one may be compelled to belong to an association.

The right to freedom of peaceful assembly and association is provided for in article 10 and 11 of the African Charter on Human Right as follows that:

Every individual shall have the right to free association provided that he abides by the law. Subject to the obligation of solidarity provided for in Article 29, no one may be compelled to join an association. Every individual shall have the right to assemble freely with others. The exercise of this right shall be subject only to necessary restrictions provided for by law, in particular those enacted in the interest of national security, the safety, health, ethics and rights and freedoms of others.

¹⁰⁶ <https://www.learnnigerianlaw.com/learn/human-rights/expression>

¹⁰⁷ https://nigeria.action4justice.org/legal_areas/freedom-of-assembly/right-to-freedom-of-assembly/

The right to freedom of assembly and association is provided for in article 11 of the European Convention on Human Right as the right to take part in peaceful meetings and to set up or join associations including trade unions.

Section 40 of the 1999 Constitution of the Federal Republic of Nigeria (As Amended) recognizes the right to peaceful assembly and freedom of association including the right to belong to a political party as follows:

Every person shall be entitled to assemble freely and associate with other persons, and in particular he may form or belong to any political party, trade union or any other association for the protection of his interests:

Provided that the provisions of this section shall not derogate from the powers conferred by this Constitution on the Independent National Electoral Commission with respect to parties to which that Commission does not accord recognition.

The right of peaceful assembly includes the right to hold meetings, sit-ins, strikes, rallies, events or protests, both offline and online. The right to freedom of association involves the right of individuals to interact and organize among themselves to collectively express, promote, pursue and defend common interests. This includes the right to form trade unions. Freedom of peaceful assembly and of association serve as a vehicle for the exercise of many other rights guaranteed under international law, including the rights to freedom of expression and to take part in the conduct of public affairs.

In Nigeria Section 40 of the Constitution and the Public order Act (CAP, 382 LFN, 2004) is the primary legislation regulating the right to assembly in Nigeria. Section 40 of the Constitution provides as follows: “Every person shall be entitled to assemble freely and associate with other persons, and in particular he may form or belong to any political party, trade union or any association for the protection of his interests”. The Public Order Act in section 1 (3) makes it mandatory for individuals or groups to apply for and obtain police permit or approval to hold rallies and peaceful assemblies. It also states that for the purpose of proper and peaceful conduct of public assemblies, meetings and processions, the Governors of each state are empowered to direct the conduct of all assemblies, meetings and processions on public road or places of public resort in their states and prescribe the route by which and the time at which any procession may pass.

However, in 2007 this section of the Act was declared by the court as unconstitutional in the case of Inspector General of Police V. All Nigeria people's party & Ors. ((2007) LPELP-8932 (CA)), Justice Adekeye held that:

“The public Order Act should be promulgated to complement sections 39 and 40 of the Constitution in context and not to stifle it or cripple it. A rally or placard carrying demonstration has become a form of expression of views on current issues affecting government and the governed in a sovereign state. It is a trend recognized and deeply entrenched in the system of governance in civilized countries – it will not only be primitive but also retrogressive for Nigeria if Nigeria continues to require a pass to hold a rally. We must borrow a leaf from those who have trekked the rugged path of democracy and are now reaping the dividend of their experience”.

Although the position of the court has not yet been reflected in legislation changes, Notification is no longer required unless the organizers of the protest require police protection and the government has a duty to respect, promote, protect and fulfil the right to freedom of assembly and association. This includes:

- A duty to refrain from restricting or interfering with citizens the right to freedom of assembly.
- A duty to protect all citizens and groups in Nigeria from any intimidation or harassment to reduce their freedom of assembly.
- A duty to ensure government agencies comply with international standards and that the laws which have been made to protect the right to freedom of assembly must conform with international laws and standards.
- A duty to take positive action to ensure people enjoy their rights without any interference.

This is the responsibility of the Nigerian government, its agencies and all the public bodies that form part of it, such as the police, ministries, local authorities, etc¹⁰⁸

The right to freedom of assembly and association is unfettered only while in the course of enjoying this right; other citizens' right to enjoy that same right is not infringed.

The government has limited the freedom of assembly and association through its actions, or other subsidiary legislations.

For example, Section 102 of the 1960 Criminal Procedure Code (applicable in the northern states) permits the use of force by police officers to disperse unlawful

¹⁰⁸ https://nigeria.action4justice.org/legal_areas/freedom-of-assembly/right-to-freedom-of-assembly/

assemblies or riots. The extent of the force allowed to achieve this is not defined. (coloured)

Section 73 of the 1916 Criminal Code (applicable in the southern states) allows “all such force as is reasonably necessary” to overcome resistance to dispersal. The section further holds that a police officer dispersing an unlawful assembly or riot:

“ not be liable in any criminal or civil proceeding for having, by the use of such [reasonably necessary] force, caused harm or death to any person”

The Police Force Order 237, titled Rules of Guidance in the use of Firearms by the Police, provides that: A police officer may use firearms when “necessary to disperse rioters or to prevent them from committing serious offences against life and property”. It further provides that 12 or more people must remain riotously assembled beyond a reasonable time after the reading of the proclamation before the use of firearms can be justified.

Paragraph 6 of the order provides that:

Fire should be directed at the knees of the rioters. Any ringleaders at the forefront of the mob should be singled out and fired on. Only the absolute minimum number of rounds necessary to suppress the riot should be used. Never under any circumstances will warning shots be fired over the head of rioters.

The human Rights Committee in its 2019 Concluding Observations on Nigeria expressed its concern:

That the Constitution allows for a broad use of lethal force, including for the defence of property and that the provisions of the Code of Criminal Procedure, the Administration of Justice Act, and police order 237 authorize the use of force without adequately restricting the nature of the force and setting out the principles of necessity or proportionality.

The Committee further raised concern:

About allegations of the excessive use of force against demonstrators, including the alleged killing of more than 150 members and supporters of the indigenous people of Biafra during Operation python Dance, on the occasion of non-violent gatherings between August 2015 and November 2016; and the alleged killing of 350 supporters of the movement in Nigeria in response to their barricading of roads blocking the passage of a military convoy in December 2015.

On the 21 October 2020, Amnesty International announced that at least 12 persons had been killed the previous day at Alausa and Lekki Toll gate in Lagos, Nigeria and hundreds of others were severely injured when police and soldiers opened fire

with live ammunition at unarmed protesters. According to Amnesty, CCTV cameras have been dismantled to prevent the collection of evidence.

According to Freedom House's 2019 report on Nigeria:

“The right to peaceful assembly is constitutionally guaranteed. However, federal and state governments frequently ban public events perceived as threats to national security, including those that could incite political, ethnic, or religious tension. Right groups have criticized federal and state governments for prohibiting or dispersing protests that are critical of authorities or associated with controversial groups like Islamic Movement of Nigeria and the separatist group Indigenous people of Biafra (IPOB). In 2018, soldiers responded to rock-throwing protesters from the Islamic Movement of Nigeria in Abuja, who were protesting the continued detention and charges against Ibrahim El-Zakzaky, by opening fire and killing as many as 45 people. In response to criticism of the shootings, the army’s official Twitter account posted a video of US then president President Donald Trump arguing in the context of US border security that stones thrown at the military should be considered firearms. President Buhari (the then Nigerian president) declined to condemn the shootings and the military continued to defend the actions of its security forces.”¹⁰⁹

According to the Nigeria Human Rights Report, the Nigerian government occasionally banned and targeted gatherings when it concluded their political, ethnic, or religious nature might lead to unrest. The army, national police, and other security services sometimes used excessive force to disperse protesters. Police forces engaging in crowd control operations generally attempted to disperse crowds using nonlethal tactics, such as firing tear gas, before escalating their use of force. On May 31, a peaceful protest occurred in the Osun State capital of Osogbo in response to an April 3 killing, Police allegedly opened fire on the protesters, wounding Toba Adedeji, correspondent for The Nation newspaper. Authorities conducted no investigation.¹¹⁰

The Supreme Court in the case of **EMEKA VS. OKORAFOR & ORS (2017) LPELR- 41738 (SC)**, where Eko JSC stated at pages 141 para D-E as follows:

“The right under section 40 of the Constitution, the right to assembly and freely associate with others, works both ways. The others you want to associate with must be prepared to associate with you. None can be imposed by order of Court, on the other. The right to freedom

¹⁰⁹ <https://www.thecable.ng/an-overview-of-the-endsars-protest-in-nigeria-legal-issues-and-matters-arising>

¹¹⁰ https://www.state.gov/wp-content/uploads/2023/03/415610_NIGERIA-2022-HUMAN-RIGHTS-REPORT.pdf

of association also connotes the right of the others to freely associate or dissociate from whosoever.”

See the cases of **Mbanefo vs. Molokwu (2009) 11 NWLR (pt. 1153) 431, Osagwe & Ors vs. Registrar of Trade Unions (1985) LPELR -2792 (SC), Taraba State Government & Anor vs. Shaku & Ors (2019) LPELR – 48130 (CA), Abdullahi vs. Sabuwa & Ors (2015) LPELR – 25954 (CA).**

In the case of MEDICAL AND HEALTH WORKERS UNION OF NIGERIA (MHWUN) & 4 ORS V. PROF. MIKE OZOVEHE OGIRIMA & 4 ORS.¹¹¹

the Claimants filed a suit on the 4th of July 2014, challenging the propriety of the Defendants embarking on strike action. According to them, the 2nd Defendant not being a registered Trade Union lacked the power to embark on industrial action in the nature of strike to press for the welfare of its members. The Applicant also argued that the 2nd Defendant has no legal right to disrupt the career progression of its members who are in the employment of the 3rd Defendant. The court considered the issues presented and held as follows:

The 4th relief is for a Declaration that it is only trade union organizations that can declare trade disputes, down tools, embark on strike, work to rule and or protest. The response of the learned Counsel to the 1st & 2nd Defendants is that his clients were registered as association in the exercise of the right conferred by section 40 of the Constitution. It is difficult not to agree with that line of submission. I had stated earlier that I neither found nor was I told that both 1st and 2nd Defendants were trade unions. The right to freedom of association is a constitutional one which can neither be waived nor abridged. Section 40, Constitution of the Federal Republic of Nigeria, 1999, as amended provides thus –

“Every person shall be entitled to assemble freely and associate with other persons, and in particular he may form or belong to any political party, trade union or any other association for the protection of his interests”.

Once individuals come together under an association the right becomes available to be enjoyed. The Court of Appeal in *Alhaji Umar Abdullahi v. Gambo Sabuwa & ORS (2015) LPELR-25954(CA)* pointed out clearly that the right to assemble freely and associate with other persons entrenched in Section 40 of the 1999 Constitution gives every citizen a right to choose the Association he wants to belong and he cannot be mandated to belong to any Association against his choice and that this right cannot be derogated from by anyone relying on *Agbai v. Okogbue (1991) 7 NWLR (Pt 204) 391, Nkpa v. Nkume (2001) 6 NWLR (Pt 710) 543, Musa v. Independent National Electoral Commission (2002) 11 NWLR (Pt*

¹¹¹ SUITNO: NICN/IB/95/2014 (Accessible at <https://nicnadr.gov.ng/judgement/details.php?id=8047>)

778) 223, *Attorney General, Federation v. Abubakar* (2007) 10 NWLR (Pt.1041) 1.

There appears to be a misconception by the learned Counsel to the Claimants that only Trade Unions can protest or go on strike. If the members of an association are to be able to protect their interests within the confines of section 40 of the Constitution, then the right to protest, down tools or declare strike must never be denied them. These are rights geared toward the protection of the right of members of the association. To grant this relief as sought is to abridge the constitutional rights of the 1st and 2nd Defendants. I refuse and dismiss the relief accordingly not having been proved.

The 5th relief is for an Order of this Honourable Court deeming the industrial action embarked upon by the 1st and 2nd Defendants members since Tuesday the 1st day of July 2014 as illegal, unconstitutional, unprofessional and ultra vires. This relief is predicated on the 4th relief for a declaration that it is only trade union organizations that can declare trade disputes, down tools, embark on strike, work to rule and or protest. Having refused and dismissed that relief, this head of claim is also bound to be refused and dismissed. I so do without hesitation.

MODULE 6

AN INTRODUCTION TO INTERNET SHUTDOWNS

Internet shutdown refers to measures taken by governments to interfere with access to the internet in order to restrict or censor opinions, dialogue, debate, online organizing, and information dissemination in general.

AccessNow defines¹¹² internet shutdowns as an intentional disruption of internet or electronic communications, rendering them inaccessible or effectively unusable, for a specific population or within a location, often to exert control over the flow of information.

Internet shutdowns usually occur when the government instructs communications companies to render the internet infrastructure inoperable. The implications of this are immediately felt in the economy of the country followed by other human rights issues, such as freedom of expression, assembly, association, etc. The fact is that restricting Internet access results in tremendous individual and societal harm while impairing journalistic activities.

In 2018, AccessNow tracked 196 internet shutdowns worldwide. In 2019, several States within the ECOWAS Community and African region have imposed Internet shutdowns, and this is a phenomena that has occurred in countries such as Sierra Leone, Egypt, Lebanon, Cameroon, Guinea, Zimbabwe, China, Myanmar, Chad, Ethiopia, Bahrain, Democratic Republic of Congo and India, etc.

Internet shutdowns have implications for civil and political as well as socioeconomic rights. They directly violate the rights to freedom of expression, access to information, association, peaceful assembly, political participation, mental and physical health and education. Additionally, vulnerable groups are often most likely to suffer disproportionate hardships during internet shutdowns.

Internet shutdowns have implications for civil and political as well as socioeconomic rights. They directly violate the rights to freedom of expression, access to information, association, peaceful assembly, political participation, mental and physical health and education. Additionally, vulnerable groups are often most likely to suffer disproportionate hardships during internet shutdowns.

¹¹² AccessNow (Accessible at <https://www.accessnow.org/campaign/keepiton/>)

Several reasons have been offered by governments for justifying internet shut down. Amongst others, National security, Communal violence, public unrest or instability, Disinformation, Cheating prevention during exams Elections, Protests, Ongoing conflict in a region, Major holidays or public events, Visits from public figures, Major exams, etc. Some of these are very serious and challenging problems facing governments and societies worldwide but shutting down the internet often causes more harm than good.

In Nigeria for instance, in 2021, the Nigerian Communications Commission released communications for the shutdown of all telecommunications services in the States of Zamfara, 13 out of 34 local government areas of Katsina, 14 out of the 23 local government areas of Sokoto state, and Kaduna State. These governments claimed that the pervading security situation following the activities of bandits necessitated the immediate shutdown of all telecommunications services in those States. They explained that the measure was ordered to stem kidnappings and killings carried out by armed groups, who allegedly use their mobile phones to prepare coordinated attacks and demand ransom payments. However, these shutdowns came at huge costs for the telecommunications companies who were obligated to comply with the instructions of the NCC. The shutdowns prevented both new and old subscribers from patronizing the telecoms companies or purchasing services during the shutdowns.

This was reported by the Cable Nigeria, a reliable source of information in Nigeria¹¹³, to have cost¹¹⁴ huge losses to the country's telecommunications companies as follows:

MTN lost about 5.1 million subscribers, dropping from 63.9 million to 58.8 million between January and December 2021.

Airtel Nigeria lost 2.5 million subscribers between January and December 2021, while 9mobile lost 1.13 million subscribers within the same period.

Globacom, on the other hand, lost about 470,000 subscribers within the same period, according to data on the Nigerian Communications Commission (NCC) website.

International human rights instruments such as the ICCPR, ICESCR and the African Charter on Human and Peoples' Rights recognize and protect the rights impacted by internet shutdowns. Apart from breaching rights, internet shutdowns

¹¹³ TheCableNg "Network shutdowns, NIN-SIM policy... how regulations impacted telecoms sector in 2021" (Accessed at <https://www.thecable.ng/network-shutdowns-nin-sim-policy-how-regulations-impacted-telecoms-sector-in-2021>)

¹¹⁴ A Guardian Newspaper publication of 12 August 2021: "Experts Weigh Costs as FG plans to unban Twitter" (Accessible at <https://guardian.ng/news/experts-weigh-costs-as-fg-plans-to-unban-twitter/>)

are reported to carry a lot of economic and reputational implications for ICT companies acting at the behest of governments.

For instance, on 5th June 2021 the Nigerian government ordered the suspension of twitter services, a social media platform operating in Nigeria, for 222 days. The shutdown, which impacted about 104.4 million internet users in the country, was recorded to by British firm, Top10VPN to cost¹¹⁵ the country around \$366.9million before it was lifted in October 2021. The firm used a NetBlocks **Cost of Shutdown Tool™** (COST)¹¹⁶ to arrive at the estimates.

Nigeria was not the first country to have ordered some form of shutdown in Africa. The Collaboration on International ICT Policy for East and Southern Africa, CIPESA, noted that “Internet Freedom Predators Are Also Press Freedom Predators: The countries that have ordered internet disruptions are among the most lowly ranked in Africa on the 2018 World Press Freedom Index including Algeria, Congo-Brazzaville, Burundi, Cameroon, Central African Republic, Chad, DR Congo, Ethiopia, Equatorial Guinea, Gabon, Gambia, Mali, Uganda, and Zimbabwe.” These countries were ranked as authoritarian governments under the Democracy Index published by the Economist Intelligence Unit (EIU)¹¹⁷

In this vein, the case of internet shutdown was filed before the Community Court of Justice of ECOWAS sometime in 2018 for consideration. This was in the case of **AMNESTY INTERNATIONAL, TOGO V THE REPUBLIC OF TOGO ECW/CCJ/APP/61/18.**

The Republic of Togo shutdown the internet on the 5th to 10th and 19th to 21st of September 2017. The government relied on two existing laws to do this: the Law on the Information Society and the Law of 2011. The shutdowns followed widespread protests by citizens over an attempt by the President to amend the

¹¹⁵ A British firm Top10VPN (Accessible <https://www.top10vpn.com/research/cost-of-internet-shutdowns/2022/>)

¹¹⁶ A tool described as a data-driven online service that enables anyone – including journalists, researchers, advocates, policy makers, businesses, and others – to quickly and easily produce rough estimates of the economic cost of Internet disruptions. (Accessible at <https://netblocks.org/projects/cost>)

¹¹⁷ According to CIPESA, “The Democracy Index is based on five categories: electoral process and pluralism; civil liberties; the functioning of government; political participation; and political culture. The Democracy Index defines authoritarian regimes as those where state political pluralism is absent or heavily circumscribed; formal institutions of democracy have little substance; and elections are not free and fair. In addition, there is disregard for abuses and infringements of civil liberties, and criticism of the government is repressed.” (Accessed at https://cipesa.org/wp-content/files/briefs/report/Despots-And-Disruptions_March-20.pdf)

Constitution of the republic with a view to extending his term in office. International media reported the protests.

Following the shutdowns and attendant restrictions, eight applicants, including a journalist, approached the ECOWAS Court. Among other things, they claimed that the internet shutdown prevented journalists from doing their work and therefore, violated their right to freedom of expression and to journalistic activities. Other claims related to NGOs that could not do their work on account of the disruptions to different forms of electronic communications. Amnesty International Togo was an NGO applicant.

The Republic of Togo had argued that the action by the government was justified in this circumstance because the government *realized that the protests had the potential of degenerating into a civil war and therefore it was imperative to protect the national security of the state.*

Some international organizations applied to submit Amicus Briefs before the Court. The Republic of Togo objected to the applications of the amici on grounds, amongst others, that the amicus curie application was in breach of the Rules of the Court. They also argued that the amici curiae, comprising AccessNow, Article 19, Internet Freedom Foundation, Paradigm Initiative for Information Technology, United Nations Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression & others, were experts on the subject of internet and access, therefore, it was not for them to apply to the Court but for the Court to use its inherent power to appoint them and define their mission as prescribed under Article 45 of the Court's Rules. The Court however rejected the arguments of the government and allowed the amici curiae interventions on grounds that it has the inherent jurisdiction to allow the amici.

The Court held in favour of the applicant as follows: That the respondent was in violation of Article 9 of the African Charter and by shutting down the internet, it violated the applicants' rights to freedom of expression. The Court also directed Togo (the respondent state) to take all necessary measures to guarantee non-occurrence of this situation in the future and to enact and implement laws, regulations and safeguards in order to meet its obligations with respect to the right to freedom of expression in accordance with international human rights instruments. The Court also awarded compensations and costs.

Providing some context to its conclusions, the court stated that the arguments by the respondent state that it had acted in defence of national security had "merit and has been internationally recognized as a valid defence to derogate from certain

rights, the fundamental basis of the exercise of the power of derogation is that it must be done in accordance with the law” and in other words, there must exist a national legislation guaranteeing the exercise of the right whilst providing the conditions under which it derogated from.

It is not in question that every government must protect its citizens against any forms of violence or insecurity. However, in so doing it must ensure to protect and respect the rights of its citizens as constitutionally guaranteed. The government in exercising its right to protect its citizens and their properties must ensure to perform these tasks in conformity with the rule of law and compliance with international human rights standards. As established in international law and treaties, any restrictions on the right to freedom of expression, for instance, is limited to circumstances, where those restrictions are set out in law, serve a legitimate interest, and are necessary and proportionate in a democratic society. Following its decision in the Amnesty Togo case, the Community Court of ECOWAS was approached to decide the legality of the suspension of Twitter in the ***SERAP AND OTHERS V NIGERIA*** (the Twitter Ban case).¹¹⁸ The Court held that because access to the internet facilitates freedom of expression, ‘denial of access to the internet or services provided via the internet... operates as denial of the right to freedom of expression and to receive information’. It therefore overruled Nigeria’s objection to its jurisdiction. On the merits, *it reasoned that access to social media like Twitter is essential for exercising freedom of expression; therefore, access to social media including Twitter should be regarded as a component of freedom of expression and protected from unlawful, arbitrary, or disproportionate restrictions*. It therefore concluded that Nigeria’s ban of Twitter without the backing a law or court order violated freedom of expression under the African Charter and the ICCPR.

¹¹⁸ The consolidated Case of four applications- The cases of Suit **No. ECW/CCJ/APP/23/21**, filed by Mr. Femi Falana (SAN), on behalf of Socio-Economic Rights and Accountability Project (SERAP), a Lagos-based NGO, and 176 Nigerians; Suit **No. ECW/CCJ/APP/24/21**, filed by Chief Malcolm Omirhobo, a Lagos-based human rights lawyer; Suit **No. ECW/CCJ/APP/26/21**. Filed by Mr. Patrick Elohor, President of the NGO, One Love Foundation; and Suit **No. ECW/CCJ/APP/29/21** filed by Mrs. Mojirayo Ogunlana-Nkanga on behalf of Media Rights Agenda and four other non-governmental organizations as well as four journalists (Accessible at <https://mediarightsagenda.org/media-rights-agenda-others-win-suit-over-twitter-ban-as-ecowas-court-rules-nigerian-governments-action-unlawful-2/>)

Access to information is an integral part of the right to freedom of opinion and expression, enshrined in a wide number of international and regional human. Therefore, a violation of the right to expression is a violation of the right to information.

In a recent case also before the ECOWAS Court, **ASSOCIATION DES BLOGUEURS DE GUINÉE (ABLOGUI) AND OTHERS V THE STATE OF GUINEA** ECW/CCJ/JUD/38/23/22 (31 October 2023)¹¹⁹, the

The applicants filed an application at the ECOWAS Court alleging that the respondent violated their rights to information and freedom of expression when the State of Guinea restricted access to the internet and social media platforms throughout the country on 18 October 2020 (during the presidential elections), where there was limited connectivity to the internet and social media, between October 23-27, 2020, the internet was completely inaccessible in the country, and from October 27 until December 2020, where Facebook was blocked. The applicants argued that the restrictions hindered their ability to carry out their professional activities and negatively impacted the general public who relied on the internet and social media platforms like Facebook to receive vital news, including how to participate in the presidential elections. The applicants prayed the Court to declare the restriction of the internet services and blocking of Facebook services across Guinea violations of the right to freedom of information and expression under the ACHPR, ICCPR, and the Revised ECOWAS Treaty, and urged the Court to order the respondent to take all necessary measures to put an end to said violations.

The Court considered the main issue, which was whether Guinea's restriction on internet and social media access violated the applicants' right to freedom of expression and access to information. The Court reiterated that access to information is an extension of freedom of expression and stated that both Article 9 of the ACHPR and 19 of the Universal Declaration of Human Rights (UDHR), refer to access to information in conjunction with freedom of expression. It opined that access to information should be "*guaranteed to as wide a public as possible by all means including the media (event, fact, judgment, figures, documents) and internet which disseminates information more quickly and on a global level.*"

Recalling its decision in the Togo case¹²⁰, the Court stated that freedom of expression is not an absolute right and can be restricted, exceptionally, through

¹¹⁹ <http://www.courtecowas.org/wp-content/uploads/2023/12/JUDGMENT-ABLOGUI-V-GUINEA-ENG.pdf>

¹²⁰ supra

measures *provided by law that serve a legitimate interest and are necessary and proportionate*. It is on this basis that it analysed the blocking of Facebook and held that restricting the internet and Facebook was not a measure provided by law and that Guinea failed to argue in favour of its legitimate purpose. The Court further stated that *even if the restriction served a legitimate purpose, it was nevertheless disproportionate since restrictions should be aimed at specific content, and general operating bans on certain sites and systems are not compatible with Article 19 (3) of the ICCPR*.

The Court stated that the Court “*is of the opinion that the Internet plays an important role in the development of a country because websites contribute to improving access to news through real-time dissemination of information.*”¹²¹ It held that “*the blocking of internet access by the Respondent State violated the Applicants’ right to freedom of expression.*”¹²²

Therefore, it is now settled law that restrictions of Internet access without a strict legal framework regulating the scope of the ban and affording the guarantee of access to courts to prevent possible abuses amounts to a violation of freedom of expression.¹²³

In addition, it is unequivocal that the right of access to information is an invaluable component of democracy which facilitates participation in public affairs. It is a right that is necessary for the realisation of other human rights, including the right to participate in government directly or through freely chosen representatives, as guaranteed by Article 13 of the African Charter. Thus, the right to inextricably linked to elections, as an essential part of electoral process that empowers the electorate to be well informed about political processes with due regard to their best interests: to elect political office holders; to participate in decision-making processes on the implementation of laws and policies; and to hold public officials accountable for their acts or omissions in the execution of their duties.

This was the reasoning of the African Commission when it released a set of *Guidelines on Access to Information and Elections in Africa*, where it noted that “No democratic government can survive without accountability and the basic postulate of accountability is that people should have information about the

¹²¹ ECOWAS Court of Justice, *Association des Blogueurs de Guinée (ABLOGUI) and others v The State of Guinea*, Judgment no. ECW/CCJ/JUD/38/23/22 (31 October 2023), paragraph 60.

¹²² *Id* Page 21

¹²³ ECOWAS Court of Justice, *Association des Blogueurs de Guinée (ABLOGUI) and others v The State of Guinea*, Judgment no. ECW/CCJ/JUD/38/23/22 (31 October 2023); See also ECtHR, *Yildirim v Turkey*, App No. 3111/10 (18 December 2012).

functioning of government.¹²⁴ It notes that regulatory bodies should refrain from shutting down the internet during electoral processes. In exceptional cases where shutdowns may be permissible under international law, such limitations need to be authorised by law, serve a legitimate aim, and be necessary and proportional in a democratic society. It stated *“For elections to be free, fair and credible, the electorate must have access to information at all stages of the electoral process. Without access to accurate, credible and reliable information about a broad range of issues prior, during and after elections, it is impossible for citizens to meaningfully exercise their right to vote in the manner envisaged by Article 13 of the African Charter.”*¹²⁵

RIGHT TO THE INTERNET

Internet access in the strict sense is not a fundamental right, however, there is a growing call for the right to the internet and several arguments for access to the internet as a human right abounds. One of such is that internet service provides a platform, such as social media or online websites, to enhance the exercise of freedom of expression. Some aspects of these arguments address the essentiality of the internet to people’s existence, such as how internet shutdown makes it hard for people to connect with their families, sustain their livelihoods, protect their relationships and maintain their mental health. There is a denial of citizen’s access to their families, communities, businesses, such as the cases for banks, telecommunication companies, schools and other online academic activities. The effect of this denial of access to the internet is that citizens right to expression, assembly and association are being violated. Moreover, this right to the internet has been made clear by the United Nations when it stated in its 2019 Report of the UN Secretary-General’s High-level Panel on Digital Cooperation that, “universal human rights apply equally online as offline – freedom of expression and assembly, for example, are no less important in cyberspace than in the town square”.¹²⁶

¹²⁴ Guidelines on Access to Information and Elections in Africa 2017 (Accessed at <https://achpr.au.int/index.php/en/special-mechanisms-reports/guidelines-access-information-and-elections-africa-2017>) and <https://achpr.au.int/en/node/894>

¹²⁵ Id.

¹²⁶ UN Secretary – General’s High-Level Panel, *Report on digital interdependence*, available at: <https://www.un.org/en/pdfs/DigitalCooperation-report-for%20web.pdf> p16

The right to an Internet connection, to communicate on the Internet is tacitly recognized by many countries as a fundamental right of modern times, when using the Internet. As a vehicle of communication, information dissemination and economic development, citizens not only communicate and conduct business correspondence but also have the right to access electronic public services, voting tools, access to necessary services that can be provided remotely, for example, during the Covid-19 pandemic, when countries declared lockdown, schools, universities carried out the educational process remotely, churches for the exercise of right to religion operated via social media platforms, many employees worked from home, some unemployed found remote jobs and performed their duties using the Internet, while the entertainment industry found expansion to the extent of enjoying paid activities on platforms like Twitter and YouTube. In such conditions, depriving people of access to the Internet is a deprivation of basic constitutional rights, which, considering the development of digital technologies in their offline mode now operates vigorously in the online mode.

Generally, restricting access to the internet is considered a violation of citizen's right to information and freedom of expression.¹²⁷ Certain legal issues were highlighted before different courts for its analysis, and one major question for the Court is whether deliberate requests by governments to the ISPs to do any act to restrict the internet is justifiable in any circumstance?

The right to the internet has thus become a sustained discourse in the international space. No international instrument or treaty or regional laws have clearly spelt out the right to the internet. However, some courageous Courts have found a way to pronounce the necessity of the internet to human lives and in the case of a regional Court like the Community Court of ECOWAS, held that 'the internet is essential and a derivative right to the right to the freedom of expression'.

Some national courts have also had positive bold approach to the idea of the right to the internet and below are pronouncements that should be considered significant to the discourse leading to the eventual adoption of the right in the future.

The case of **FAHEEMA SHIRIN R.K. V. STATE OF KERALA**¹²⁸ is important as an example in this instance. In that case a 3rd year student sued her university and others challenging her expulsion from the hostel following her disobedience to the rules of the hostel, which imposed a restriction on the use of mobile phones

¹²⁷ See Amnesty International Togo & Ors. Vs. The Republic of Togo (supra)

¹²⁸ WP(C).No.19716 OF 2019(L) 19th September 2019

from 10:00 pm to 6:00 am and then from 6pm to 10pm. At the time the rule was being enforced, the Applicant and other students had appealed that the restriction on use of mobile phones and laptops within the hours declared were inconvenient and a limitation for them. She made this complaint to the Deputy Warden, the Matron and the Principal. The principal subsequently had a meeting with the Applicant's parents where she informed them that Applicant must comply with the rules or vacate the hostel. The students were also asked to indicate their willingness to comply with the rules which the Applicant wrote stating her objections to the rules. She was subsequently expelled from the hostel. This affected her from attending classes because she had to drive 150km every day to get to the school. She therefore brought a suit at the High Court of Kerala.

The Applicant argued amongst others that the limitations imposed by the hostel management on the use of cell phones during disciplinary compliance violated the petitioner's fundamental rights; was discriminatory as it was only imposed in the women's hostel, in violation of Clause 5 of guidelines issued by the University Grants Commission (UGC), which prohibits gender discrimination and affected the quality of education accessible to female students, thus violating the Convention on Elimination of all forms of Discrimination Against Women (CEDAW), the Beijing Declaration and the Universal Declaration of Human Rights. The Applicant asserted that the restrictions were arbitrary and hampered access to quality education to female students limiting their growth and potential. She also stated that this amounted to a denial of her right to acquire knowledge through the internet, in addition that the prohibition on the use of mobile phones was a deprivation of the access to the source of knowledge detrimental to the quality of education available to women. She submitted that the right to access internet forms a part of freedom of speech and expression guaranteed under Article 19(1)(a) and the restrictions imposed do not come within reasonable restrictions covered by Article 19(2) of the Constitution of India in a scenario when the Government has proclaimed steps for making internet accessible to all citizens recognizing the right to internet as a human right. That the rule contradicted the State's recognition that the right to access the internet was human right, and its policy to make the internet accessible to all citizens through its "mobile first approach for e-governance services" under the Digital Kerala Vision. The restriction further undermined digital learning programs being implemented by the State and Education Department which made it possible for students to read their lessons on their smart phones and tablets. She claimed that the imposition of the rules and her expulsion thereof amounted to a breach of her constitutional right to privacy and personal autonomy, guaranteed under Article 21 of the Constitution of India; violated her constitutional right to freedom of expression, and her right to education. She relied

on extensive case law in *Ministry of Information and Broadcasting v. Cricket Association of Bengal & Anr*¹²⁹, *Shreya Singhal v. Union of India*¹³⁰, *N.D Jayal v. Union of India*¹³¹, *PUCL v. Union of India*¹³², *National Legal Services Authority v. Union of India*¹³³, *Shafin Jahan v. Asokan K.M & Ors*¹³⁴. and the judgment of the Kerala high Court in *Anjitha K. Jose & Anr. v. State of Kerala & Ors*¹³⁵ to buttress her arguments.

The Respondent claimed that the restrictions were imposed following the request of some parents. It admitted that the Applicant's parents did not agree to the restriction, but claimed that they acted within their authority as representatives of an educational institution to enforce discipline, which was integral to their role to cultivate and guide the student's pursuit of education which the Applicant's parents were aware of when they signed the general application form at the time she was admitted. They argued that the college had a full-fledged library of more than 30,000 books, which students could use and also in addition to access the internet to gain information only between 6 p.m. and 10 p.m. They stated that an arbitrary limitation cannot be claimed.

The Court considered both arguments and held that the right to access the Internet has been recognized as a fundamental right which forms part of the right to privacy and the right to education, as provided for in Article 21 of the Constitution. It found that disproportionate access to the Internet in an information society generates and propagates socio-economic exclusions. The Court relied on international conventions as follows:

1. The Convention on the elimination of all forms of communication against women and all previous resolutions of the commission on human rights and on the right to freedom of opinion and expression, including, resolution 23/2 adopted by the Human Rights Council of the UN General Assembly on 24th June, 2013 on the role of freedom of opinion and expression in women's empowerment, council resolution 20/8 of 5 July 2012 on the promotion of protection and enjoyment of human rights on the Internet, which called upon States to promote women's freedom of opinion and

¹²⁹ (1995) 2 SCC 161

¹³⁰ *Shreya Singhal v. Union of India*, WRIT PETITION (CRIMINAL) NO.167 OF 2012.

¹³¹ (2004) 9 SCC 362

¹³² *PUCL v. Union of India*, AIR 1997 SC 568, JT 1997 (1) SC 288, 1996 (9) SCALE 318, (1997) 1 SCC 301, 1996 Supp 10 SCR 321, 1997 (1) UJ 187 SC.

¹³³ (2014) 5 SCC 438

¹³⁴ (2018)16 SCC 368

¹³⁵ 2019(2) KHC 220

- expression online and off-line, as well as facilitate equal participation in access to and use of the internet;
2. The resolution adopted by the UN General Assembly on 14th July 2014, which emphasized that access to information on the internet created vast opportunities for affordable and inclusive education globally, thereby being an important instrument facilitating the promotion of right to education, and called upon States to promote and facilitate access to the internet and develop information and communication facilities and technologies in all countries and which can be an important role in facilitating the promotion of the right to education.

The Court noted that the internet created opportunities and advantages to online learning, and mobile phones facilitated the exchange of ideas, group discussions, to read news online, undergo online courses, and downloading of data or e-books. It also noted that the students were adult, old enough and capable of taking responsibility for their studies and should be given the freedom to use their mobile phones to access the internet “to acquire knowledge from all available sources” in order to “achieve excellence and enhance [the] quality and standard of education” irrespective of the widespread misuse of electronic devices – including laptops. It held that while the Hostel authorities are expected to enforce regulations, those regulations must be in alignment with modern needs and not undermine students’ access to educational resources; that the total restriction on the use of mobile phones and the direction to surrender it during certain hours was absolutely unwarranted. It emphasized that “a rule of instruction which impairs the said right of the students cannot be permitted to stand in the eye of the law” and that the international community has since recognised¹³⁶ that the right to access the Internet was “a fundamental freedom and a tool to ensure right to education,” and the rules in the instant case infringed on fundamental freedom as well as the privacy rights of students which could “adversely affect the future and career of students who want to acquire knowledge and compete with their peers.”¹³⁷

In an internet shutdown case before the Supreme Court of India, in the case of *Anuradha Bhasin v. Union of India*¹³⁸, the Court considered the arguments by a journalist that due to internet suspension in Jammu and Kashmir, she was unable to publish her newspaper and this violated the freedom of press. The Applicant challenged the constitutional validity of the restrictions on public movements and

¹³⁶ UN Human Rights Council declaration

¹³⁷ *Shirin R.K. v. State of Kerala* (Accessible at

<https://globalfreedomofexpression.columbia.edu/cases/shirin-r-k-v-state-of-kerala/>)

¹³⁸ *Anuradha Bhasin v. Union of India*, 2020 Writ Petition (Civil) No. 1031 of 2019 combined with Writ Petition (Civil) No. 1164 of 2019. Also 2020) 3 SCC 637, 2020 SCC OnLine SC 25, AIR 2020 SC 1308; See also *Foundation of Media Professionals v. Union Territory of Jammu and Kashmir & Anr* WP (C) Diary No. 10817 of 2020

suspension of internet services under Article 32 of the Constitution¹³⁹ and also argued that blanket internet suspension order violated the freedom to carry on any trade, business and profession guaranteed by Article 19(1)(g) of the Indian Constitution.

In a twist, the Court while recognizing that restriction of physical movement along with shutting down of all internet communications violated Article 19 of the constitution since the right to Internet is a part of Article 19 (1a) which is a fundamental right of the constitution, held that due to immediate threat or due to any security concern, temporary ban on services is acceptable but suspension of internet services for an indefinite period is not acceptable since the balance between the national security and human rights should always be maintained.

According to the Court, Article 19(1)(a) embodies the fundamental right of speech and expression, and this right includes the right to make any expression through the medium of the internet. The Court observed that nowadays, the internet has become one of the most important sources for disseminating information. Through the medium of the internet, information can be provided to millions of people in the blink of an eye. Thus, the freedom to make any speech or expression through the medium of the internet is an important facet of Article 19(1)(a), and the government cannot impose undue restrictions on this valuable freedom. The Court observed that the development of technology seldom corresponds to similar developments in law. The law must evolve itself and imbibe the developments in technology. The internet is also a very important tool for trade and business. Some trades are exclusively dependent on the internet, and the right to carry on trade and commerce through the internet is constitutionally protected under Article 19(1)(g).

The Court also discussed the doctrine of proportionality and observed that the doctrine has been etched in the Indian Constitution by the use of the word ‘reasonable’ in Article 19. Article 19 permits the state to impose only reasonable restrictions on freedom of speech and expression. This principle implies that the legislature or the administrator should strive to achieve a proper balance between the purpose of the legislative or administrative order and the adverse effect that the legislation or order is likely to have on the rights and liberties of the concerned persons.¹⁴⁰

¹³⁹ Accessible at <https://indiankanoon.org/doc/981147/>

¹⁴⁰ Case analysis by *Shashwat Kaushik* (Accessible at <https://blog.iplers.in/anuradha-bhasin-v-union-of-india-case-analysis/#:~:text=in%20the%20world,-Anuradha%20Bhasin%20v.,blanket%20ban%20on%20internet%20services>)

The position above was also mirrored in the Nigerian case before the Federal High Court in the case of **INC. TRUSTEES OF LAWS AND RIGHTS AWARENESS INITIATIVE AND ATTORNEY GENERAL OF KADUNA STATE**¹⁴¹ where the Applicant sought amongst others the “DECLARATION that access to the Internet is a digital right i.e. fundamental right guaranteed under chapter 4 of the Constitution of the Federal Republic of Nigeria, 1999 (as amended) but exercised and enjoyed online and on digital platforms,” the Court stated as follows:

“While expounding these provisions, the Court of Appeal had this to say: “My Lords, the right to freedom of expression and the press as recognized and guaranteed by law, is geared towards the safeguarding of the right of the citizen to impart and information as permitted by law. It, therefore, exists to protect the right to seek and receive information for the purpose of disseminating such ideas and purpose and ideas as well as the right to freely express for the information opinions orally or through publications. The real essence of this right, therefore, is to guarantee to each citizen the right within the purview of the law to express himself freely without unjustifiable interference” see the case of *Shuaibu & Ors. v Utomwen & Ors*”¹⁴²

The Court stated in furtherance to the above that:

“These provisions upon which these decisions are anchored should answer the Applicants questions in the affirmative that access to the internet is a fundamental right as it is a medium to right of freedom of expression as constitutionally guaranteed under Section 39 of the Constitution as amended. However, to these provisions there is a caveat. In Section 45 of the 1999 Constitution, it is provided in the following terms...”

The Court went ahead to cite the case of *Aviomoh vCOP & Anor.*¹⁴³ where the Court held that:

“...So, when Section 39(1) of the Constitution entitles a person to freedom of expression, it is not a blanket right. It must not be utilized or invoked in such a way, that it offends public safety, order, morality and health, and it must not be injurious to the rights and freedoms of other persons. Once a person lives in a community, his rights stop where the rights of other members of the community begin. He has to behave according to the norms of that society; otherwise his conduct will be injurious to the wellbeing and continued existence of that community...The Constitution recognises the fact that if such a person acts to the detriment of others, he can be liable in a civil action, but the issue goes beyond the right of an injured individual to act and the whole society has to be

¹⁴¹ Suit No. FHC/KD/CS/80/2022 (unreported)

¹⁴² Id. Page 6 Para 1

¹⁴³ (2014) LPELR-23039(CA)

involved to protect itself. Hence, criminalising such conduct of the individual. That is why Section 45 (1) of the Constitution was promulgated”.

The Court therefore held as follows that:

“Thus whereas right of access to internet is generally guaranteed by our Constitution as a medium of free expression, these rights can be curtailed under certain situations such where the security of the society is in danger...I do not think I need to be supplied with any law before I agree that in Kaduna State, like any other State, the Governor is the Chief security officer of the State. This is an inherent constitutionally enshrined position. The Governor as the Chief Security officer is therefore in the best position to assess the security situation of the state and take appropriate measures even if it entails temporary inconvenience to the members of the public...In my view, it would be ridiculously insensitive of this court to interfere with the decision of the Respondent. This court ought to take, and it hereby takes judicial notice of the precarious situation in Kaduna State as well as some other parts of the country. I do not therefore think that the Applicant’s action is meritorious. It is accordingly dismissed.”

From the above positions from different Courts there is no doubt that national legislations need to be enacted to establish and protect the right to the internet as a fundamental right because of its peculiarities. There is a need for internet access to be provided within constitutional protection. The internet is critical to the enjoyment of fundamental freedoms that are crucial to a functioning democracy and a thriving civic space. The civic space as we know it becomes healthy when such fundamental freedoms like the freedom of expression, association and assembly are promoted and protected under the State’s obligations to fulfil, protect and promote.

Additionally, the Internet provides access to communication for all users around the world by providing them a virtual platform. Internet is a mode of access to the education for students who take online exams and do online diploma and other courses and thus it is fundamental to facilitate its advancement. Telecoms companies, mobile Internet Service and Broadband Internet providers give a life support system to the people from all over the world. Thus, the Internet though a source of information, communication and access to social media, portrays a significant role for businesses and occupations. It is important for workers who work remotely as well as small and individual owned enterprises which sell their product services online giving them a means for their survival.

Protecting democracy requires that we must infuse a human rights approach to providing and expanding access to the internet. In the same vein restrictions must also be subjected to strict proof of compliance with the rule of law. The freedom of

expression helps democracy function better when citizens can exercise their rights to impart and disseminate information without hindrances. We must also consider that democracy requires the rule of law. The rule of law is central to democracy. The rule of law is fuelled by pertinent principles, such as legality, legal certainty, transparency, accountability, and judicial protection by an independent judiciary, among others. Thus, the role of the judiciary in all of this cannot be disregarded.

It is necessary that access to the internet be held to be an integral part of human rights that require the protection of the law. This will make the violation of internet access in a democratic society an actionable violation. The rationale is that internet access is an element of human rights which states are under obligation to provide protection for in accordance with the law of the constitution in the same way that the constitution guarantees freedom of expression. Thus, any restriction on freedom of expression must be considered within the context of a democratic society.

The need for a universal access to the internet remains a top priority at the international stage as the UN Secretary General made the call for achieving universal connectivity by 2030 in his roadmap for digital cooperation¹⁴⁴. According to him,

“In order to ensure that every person has safe and affordable access to the Internet by 2030, including meaningful use of digitally enabled services, in line with the Sustainable Development Goals, the United Nations will: a) Support efforts to establish a baseline of digital connectivity that individuals need to access the online space, as well as a definition of “affordability”, including universal targets and metrics; b) Convene a global group of investors and financing experts to consider the development of a financing platform and find other new models for investment in connectivity, in particular, in hard-to-reach and rural areas; c) Promote new and potentially transformative models to accelerate connectivity, such as the GIGA initiative of ITU and the United Nations Children’s Fund; d) Promote the development of enabling regulatory environments for smaller-scale Internet providers, along with local and regional assessments of connectivity needs; e) Accelerate discussions on connectivity as part of emergency preparedness, responses and aid, including working through the inter-agency Emergency Telecommunications Cluster...To address the challenges and opportunities of protecting and advancing human rights, human dignity and human agency in a digitally interdependent age, the Office of the United Nations High Commissioner for Human Rights will develop system-wide guidance on human rights due diligence and impact assessments in the use of new technologies, including through engagement with civil society, external experts and those most vulnerable and affected. ***I also call upon Member States to place human rights at the centre of regulatory frameworks and***

¹⁴⁴ Report of the Secretary-General Roadmap for Digital Cooperation 2020-Achieving Universal Connectivity (Accessible at https://www.un.org/en/content/digital-cooperation-roadmap/assets/pdf/Roadmap_for_Digital_Cooperation_EN.pdf)

legislation on the development and use of digital technologies. In a similar vein, I call upon technology leaders urgently and publicly to acknowledge the importance of protecting the right to privacy and other human rights in the digital space and take clear, company-specific actions to do so.”

Some countries have legislations targeted at access to the internet as a human right. These include:

Estonia: In February 2000, the Estonian Parliament sanctioned the new Telecommunications Act, including Internet Access an essential Human Right.

Greece: In 2001, Greece changed its Constitution and embedded Article 5A encouraging the option to get track individuals web movement, and then finally declared Access to the Internet a Fundamental Human Right.

Finland: In 2010, Communications Market Act, which expressed that widespread help additionally incorporated a utilitarian Internet association and had articulated Access to the Internet a Fundamental Human Right via amendment.

Costa Rico: In 2010, The Apex Court of Costa Rico had declared access to Internet a basic human right. Under Article 33 of the Constitution of Costa Rico Access to the Internet is a Fundamental Human Right.

Spain: In November 2009 the Spanish citizens was entitled to have access to the Internet because of the Act 2/11 of March 2004 which states that sustainable economy should affix x broadband access to its universal service.

Canada: In 2016, Canadian Radio Television and Telecommunications Commission pronounced Internet access a fundamental assistance.

In conclusion, as the world continue to seek ways to harmonise efforts on the right to the internet owing to the rapidly evolving digital landscape, it is important that policy, legislation, laws and governance objectives must include multistakeholder perspectives, including the inputs from civil society, This is because omitting diverse contributions could have grave consequences such as laws that can undermine civil liberties and criminalize activities inherent to the exercise of human rights, including the rights to privacy and free expression. It is unfortunate that some African countries attempt or enact laws to authorize broad State censorship, website blocking and online surveillance.¹⁴⁵

¹⁴⁵ Nigeria Cybercrimes Act 2015 and the Lawful Interception of Communications Regulation.

In Egypt for example, the law on cybercrime, mandates that Internet service providers keep and store users' data, including phone calls, text messages, and browsing and application history, for a period of 180 days, and that they make the data accessible to law enforcement upon requests or be penalised. Service providers that fail to comply with the data storage requirement may face punishments ranging from 5 million to 10 million Egyptian pounds (LE), while companies that do not submit information to government authorities upon request may be imprisoned for up to three months and face fines between LE200,000 and LE1 million. The law states that in more urgent cases, such requests can be made directly to the National Telecom Regulatory Agency. Service providers that do not adhere to a censorship request face fines ranging from LE500,000 to LE1 million and a one-year prison term.

In a world where our lives are gradually being removed from the physical space, it is critical that laws and policies must be based on fundamental rights. Legislations and regulations must be drafted in such a way as to enable us to satisfy our virtual basic needs and flourish while offering protection against the abuse of power. Laws that are enacted without necessary human rights safeguards are autocratic in nature and would amount to a violation of both domestic and international legal obligations of the State to protect the rights of individuals to privacy, freedom of thought, freedom of the press, and expression.

MODULE 7

THE CONCEPT OF NATIONAL SECURITY AND DIGITAL RIGHTS

This module will do an overview of the concept of national security.

National is one of the justifications that governments rely on for the restriction of fundamental rights. Many countries' Constitutions carry an omnibus provision that empowers government to legitimately suspend fundamental rights. The national security consideration is usually left at the discretion of the government, and it's been noted by several institutions at the international, regional and national level to be susceptible to abuse.

In an era where digital rights have become as relevant as offline rights, national security is frequently relied upon as a justifiable reason for limiting digital rights or for an interference with access to the internet, as well as other interferences with the right to freedom of expression. While this may, in appropriate circumstances, be a legitimate aim, it also has the potential to be relied upon to quell dissent and cover up state abuses. The covert nature of many national security laws, policies and practices, as well as the refusal by states to disclose complete information about the national security threat, tends to exacerbate this concern. Furthermore, courts and other institutions have often been deferent to the state in determining what constitutes national security.

National Security is sanctioned as a defence for governments' violations of the rights to freedom of expression, assembly, association and even privacy. This is backed by international, regional and national instruments, such as the International Covenant on Civil and Political Rights (ICCPR)¹⁴⁶ and the African Charter on Human and Peoples' Rights (ACHPR).¹⁴⁷ These instruments rightly approve circumstances of insecurity, such as banditry, terrorism, war, or when the corporate existence of a sovereign States is at stake as legitimate moments to limit some human rights.

Article 4 of the ICCPR states:

¹⁴⁶ International Covenant on Civil and Political Rights (1966) at articles 19, 21 and 22 (accessible at: <https://www.ohchr.org/en/professionalinterest/pages/ccpr.aspx>).

¹⁴⁷ African Charter on Human and Peoples' Rights (ACHPR), at articles 3, 11, 12, 27 (1981) (accessible at: <https://au.int/en/treaties/african-charter-human-and-peoples-rights>).

"In a time of public emergency which threatens the life of the nation and the existence of which is officially proclaimed, the States Parties to the present Covenant may take measures derogating from their obligations under the present Covenant to the extent strictly required by the exigencies of the situation, provided that such measures are not inconsistent with their other obligations under international law and do not involve discrimination solely on the ground of race, colour, sex, language, religion or social origin."¹⁴⁸

In this regard, the United Nations Rights Committee clarified the provision of Article 4 in General Comments 29¹⁴⁹ which permits derogation of rights during a situation of critical emergency. It states as follows:

- a. Article 4 of the Covenant is of paramount importance for the system of protection for human rights under the Covenant. On the one hand, it allows for a State party unilaterally to derogate temporarily from a part of its obligations under the Covenant. On the other hand, article 4 subjects both this very measure of derogation, as well as its material consequences, to a specific regime of safeguards.
- b. Measures derogating from the provisions of the Covenant must be of an exceptional and temporary nature. Before a State moves to invoke article 4, two fundamental conditions must be met: the situation must amount to a public emergency which threatens the life of the nation, and the State party must have officially proclaimed a state of emergency. The latter requirement is essential for the maintenance of the principles of legality and rule of law at times when they are most needed. When proclaiming a state of emergency with consequences that could entail derogation from any provision of the Covenant, States must act within their constitutional and other provisions of law that govern such proclamation and the exercise of emergency powers;
- c. Not every disturbance or catastrophe qualifies as a public emergency which threatens the life of the nation, as required by article 4, paragraph 1. During armed conflict, whether international or non-international, rules of international humanitarian law become applicable and help, in addition to the provisions in article 4 and article 5, paragraph 1, of the Covenant, to prevent the abuse of a State's emergency powers. The Covenant requires that even during an armed conflict measures derogating from the Covenant are allowed only if and to the extent that the situation constitutes a threat to the life of the nation. If States parties consider invoking article 4 in other situations than an armed conflict, they should carefully consider the justification and why such a measure is necessary and legitimate in the circumstances.
- d. A fundamental requirement for any measures derogating from the Covenant, as set forth in article 4, paragraph 1, is that such measures are limited to the extent strictly required by the exigencies of the situation. This requirement relates to the duration, geographical

¹⁴⁸ ICCPR above n 2 at article 4.

¹⁴⁹ United Nations Human Rights Council, 'General Comment No. 29, states of emergency (article 4)' at para. 2 (2001) (accessible at: <https://digitallibrary.un.org/record/451555?ln=en>).

coverage and material scope of the state of emergency and any measures of derogation resorted to because of the emergency. Derogation from some Covenant obligations in emergency situations is clearly distinct from restrictions or limitations allowed even in normal times under several provisions of the Covenant.²

- e. Nevertheless, the obligation to limit any derogations to those strictly required by the exigencies of the situation reflects the principle of proportionality which is common to derogation and limitation powers. Moreover, the mere fact that a permissible derogation from a specific provision may, of itself, be justified by the exigencies of the situation does not obviate the requirement that specific measures taken pursuant to the derogation must also be shown to be required by the exigencies of the situation.
- f. Article 4, paragraph 2, of the Covenant explicitly prescribes that no derogation from the following articles may be made: article 6 (right to life), article 7 (prohibition of torture or cruel, inhuman or degrading punishment, or of medical or scientific experimentation without consent), article 8, paragraphs 1 and 2 (prohibition of slavery, slave-trade and servitude), article 11 (prohibition of imprisonment because of inability to fulfil a contractual obligation), article 15 (the principle of legality in the field of criminal law, i.e. the requirement of both criminal liability and punishment being limited to clear and precise provisions in the law that was in place and applicable at the time the act or omission took place, except in cases where a later law imposes a lighter penalty), article 16 (the recognition of everyone as a person before the law), and article 18 (freedom of thought, conscience and religion). The rights enshrined in these provisions are non-derogable by the very fact that they are listed in article 4, paragraph 2.

In its latest General Comment, No. 37, specifically on the right of peaceful assembly, issued in July 2020, the Committee stated that: “State parties must not rely on derogation from the right of peaceful assembly if they can attain their objectives by imposing restrictions in terms of article 21.”

At the regional level, States parties do not have the same derogation provision stated in the African Charter, but this has not restricted them from adopting national legislations or regulations where derogations are provided for.

In Nigeria, the 1999 Constitution of the Federal Republic of Nigeria provides for derogation under Section 45. It states:

- 45. (1) Nothing in sections 37, 38, 39, 40 and 41 of this Constitution shall invalidate *any law that is reasonably justifiable in a democratic society-*
 - a. In the interest of defence, public safety, public order, public morality or public health
 - b. For the purpose of protecting the rights and freedom of other persons”

By virtue of this provision, Courts have pronounced, for instance, that the right to freedom of expression is not absolute but subject to some permissible

constitutional restrictions. This was the case in ASARI DOKUBO V FEDERAL REPUBLIC OF NIGERIA¹⁵⁰, where Hon. Rhodes-Vivour JCA (as he then was) held that:

“My Lords, where National Security is threatened or there is the real likelihood of it being threatened Human Rights or individual rights of those responsible take second place. Human rights or individual rights must be suspended until National security can be protected or well taken care of”.

This was also the opinion of the Court in ACHIMU V HON. MINISTER FOR INTERNAL AFFAIRS¹⁵¹ per Mustapha J. when he held that:

“the right conferred by Section 39 of the 1999 Constitution is not absolute as it is circumscribed by the provision of Section 45 (1) of the same constitution which provides that the right to family life can be interfered with in the interest of defence, public safety, public order, public morality, public health or for the purpose of protecting the rights and freedom of other persons....See: THE PUNCH NIGERIA LTD. V. ATTORNEY-GENERAL OF THE FEDERATION (Supra), THE GUARDIAN NEWSPAPER LTD V ATTORNEY-GENERAL OF THE FEDERATION (1999) 9NWLR (PT.618) 187

The import of this is that “National Security” is a significantly important objective having justification to limit human rights.

However, some States go overboard in their application of national security to hound journalists, bloggers, human rights defenders, civil society organizations, political oppositions, etc. This fact was also envisaged by the UN Human Rights Community.

In Nigeria, for instance, under the excuse of National Security, the Buhari led government mandated the media to only publish suppressed information. The President Muhammadu Buhari reiterated this at a legal gathering in August 2018 when he boldly said that “...*the Rule of Law must be subjected to the supremacy of the nation’s security and national interest...*”

Several reports abound of record-high impunity of attacks on the press since 2015 and how security forces in countries like Nigeria now use Cyber Crimes and Terrorism laws to hound journalists in the name of national security.¹⁵² A reason is

¹⁵⁰ (2007) 12 NWLR (Pt. 1048) 320 at 358-359; (2007) LPELR 958 (SC).

¹⁵¹ (2005) 2 F.H.C.L.R 401

¹⁵² **Nigeria: Endangered voices: Attack on freedom of expression in Nigeria** October 14, 2019 Index Number: AFR 44/9504/2019 (Accessible at <https://www.amnesty.org/en/documents/afr44/9504/2019/en/>) See also the blogpost by John Campbell **Buhari's Attacks on the Press in Nigeria Continue Unabated** (11 December 2019) <https://www.cfr.org/blog/buharis-attacks-press-nigeria-continue-unabated>

to perpetuate media censorship and deny citizens vital information of public interest.

In this respect, the UN Special Rapporteur on Freedom of Expression, Frank LaRue, expressed that:

“The use of an amorphous concept of national security to justify invasive limitations on the enjoyment of human rights is of serious concern. The concept is broadly defined and is thus vulnerable to manipulation by the State as a means of justifying actions that target vulnerable groups such as human rights defenders, journalists or activists. It also acts to warrant often unnecessary secrecy around investigations or law enforcement activities, undermining the principles of transparency and accountability.”

Principle XIII(2) of the Declaration of Principles on Freedom of Expression in Africa provides that the right to freedom of expression should not be restricted on public order or national security grounds ***“unless there is a real risk of harm to a legitimate interest and there is a close causal link between the risk of harm and the expression”***.

The crux of the national security permission is that it must not be arbitrarily applied. It must be provided by law, the measure taken must be necessary and proportional in an open and democratic society.

In **CHIKE OBI V DIRECTOR OF PUBLIC PROSECUTION**¹⁵³, the Nigerian Supreme Court held that its role was not merely to “rubberstamp the acts of the Legislature and the Executive, that the court must be the arbiter of whether or not any particular law is reasonably justifiable”.

In this vein also, the Supreme Court in **OLAWOYIN V ATTORNEY GENERAL OF NORTHERN NIGERIA**¹⁵⁴, held that a restriction upon a fundamental right before it may be considered justifiable must (a) *be necessary in the interest of public morality and (b) not to be excessive or out of proportion to the object which it is sought to achieve.*

This clearly states that that even in the application of the national security defence, the restriction to any digital right, for instance, must not be excessive or out of proportion to the object which it is sought to achieve. This also means that the application of Section 45 of the 1999 Constitution of the federal republic of Nigeria (as amended) does not envisage the derogations from the rights under

¹⁵³ (No.2) (1961) All NLR 458

¹⁵⁴ [1961] 1 All NR

sections 39-41 without due regards to the three part test of provided by law, legitimate aim, necessary in a democratic society and also proportionate. The crux of Section 45 is that the provisions of sections 39-41 can only be abrogated in consonance with a law that is reasonably justifiable in a democratic society.

Thus applying these tests means that, that the restriction or limitation on the right to freedom of expression be according to a “law that is reasonably justifiable in a democratic society” prescribes that such a restriction or limitation must be strictly necessary to achieve a legitimate aim and that it be proportionate to the interest to be protected; that measures to be taken in derogating from these rights must be the least intrusive instrument amongst those which might achieve this interest;¹⁵⁵

In fact, derogation must be proportional and necessary in a democratic society for it to be justified. This was the decision of the African Commission on Human and Peoples’ Rights in its *Declaration of Principles on Freedom of Expression in Africa, ACHPR/Res.62(XXXII)02 (23 October 2002), Principle II (2). The African Commission stated*¹⁵⁶ that:

“Freedom of expression should not be restricted on public order or national security grounds unless there is a real risk of harm to a legitimate interest and there is a close causal link between the risk of harm and the expression.”

Also in *MEDIA RIGHTS AGENDA, CONSTITUTIONAL RIGHTS PROJECT V NIGERIA*¹⁵⁷ the African Commission on Human and Peoples Rights noted that **restrictions on freedom of expression should be based on a legitimate public interest and the disadvantages of limitation should be strictly proportionate to and absolutely necessary to achieve the desired benefit.**

In its Principles and Guidelines on Human and Peoples’ Rights while Countering Terrorism in Africa, the African Commission stresses that, while the spread of terrorism may be intensified by the use of the internet and social media, these ‘are tools which can be used to combat the spread of terrorism and should not be viewed as a threat in itself’

¹⁵⁵ UN Human Rights Committee, *General Comment No 27: Article 12: Freedom of Movement* UN Doc CCPR/C/21/Rev.1/Add.9 (2 November 1999), para-14.

¹⁵⁶ Declaration of Principles on Freedom of Expression in Africa (adopted by the African Commission during its 32nd Ordinary Session, 17-23 October 2002, Banjul, The Gambia, Principle XIII (2)

¹⁵⁷ *Supra (Communication No. 105/93-128/94-130/94-152/96, para 69)*

This was also the view of the UN Special Rapporteur on the promotion and protection of human rights while countering terrorism in 2011 when he enunciated that maintaining connectivity may mitigate public safety concerns and help restore public order.¹⁵⁸ Also, in General Comments 34¹⁵⁹ The UNHRC explained that the media plays an important role in informing the public about acts of terrorism, and it should be able to perform its legitimate functions and duties without hindrance.¹⁶⁰

Lastly, in *Constitutional Rights Project and Civil Liberties Organisation v Nigeria*,¹⁶¹ Following the annulment of the 1993 presidential elections, political opponents, activists and journalists, who protested the annulment were arrested and detained, many without charges, and publications were seized and banned.¹⁶² The matter was brought before the African Commission which had to determine whether the government had breached fundamental human rights in the annulment of the elections and their subsequent actions. The Commission rejected the government's argument that the measures taken were appropriate and enforced der to prevent a certain situation from arising. It found that the decrees created by the government, tailored specifically to certain individuals or legal entities, were likely to amount to unequal treatment before the law and this amounted to a breach of Article 1 of the African Charter which requires all member states to respect the Charter by recognizing the rights, freedoms and duties contained in it. The commission also held that no situation could justify such a wholesale interference with freedom of expression. It stated that competent authorities should not enact provisions which limit the exercise of this freedom. The competent authorities should not override constitutional provisions or undermine fundamental rights guaranteed by the constitution and international human rights standards"¹⁶³ It held that by banning and seizing certain publications and unlawfully detaining the protesters was a clear breach of freedom of expression and there wasn't a justification.

¹⁵⁸ UN Human Rights Council, '2017 Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression' at para. 14 (2017) (accessible at: <https://www.undocs.org/A/HRC/35/22>).

¹⁵⁹ Supra

¹⁶⁰ UN Human Rights Council, 'General Comment no. 34 at para 46 (2011) (accessible at <https://www2.ohchr.org/english/bodies/hrc/docs/gc34.pdf>).

¹⁶¹ <https://globalfreedomofexpression.columbia.edu/cases/constitutional-rights-project-and-civil-liberties-organisation-v-nigeria/>

¹⁶² African Commission on Human and Peoples' Rights, Communication No. 102/93 (1998) (accessible at: <https://africanlii.org/afu/judgment/african-commission-human-and-peoples-rights/1998/2>).

¹⁶³ Para. 57 (ACHPR/A\101/93:18).

From the foregoing, national security will continue to pose challenges for human rights whether offline and online and it is the Courts that would have to step in to create and mandate a balance so that there can be the supremacy of the rule of law over blatant violations of rights.

MODULE 8

ONLINE HUMAN RIGHTS VIOLATIONS

Several other issues affect the digital environment. Apart from governments' infractions, individuals also pose huge problems for others in the virtual environment. These issues include, online violence and harassment, Online crimes, online gender-based violence, Equality and freedoms in the digital environment, Identity in the digital environment, Profiling, discrimination, Child protection.

Every human has the freedom to be online. No one must be deprived of the right to the internet, to live freely and to exercise all their rights online.

This means that people online can confidently exercise their rights as provided for under Articles 17, 19 and 20 of the Universal Declaration of Human Rights (UDHR) and in Articles 19, 21 and 22 of the International Covenant on Civil and Political Rights (ICCPR), that is, the rights to the protection of the law from unlawful interference with their privacy or attacks to their honour and reputation, peacefully assemble online, to associate with others and to freely express themselves, “to seek, receive and impart information and ideas of all kinds either orally, in writing or in print, in the form of art, or through any other media of their choice or by holding opinions without interference.”

These rights are inalienable, and no one must be deprived of them except in exceptional circumstances where the considerations are national security, public morality, public order, public health, and public safety. However, these restrictions will only be valid where they meet the three cumulative thresholds- that they provided by law, pursue a legitimate aim/interest, and measures resorted to are proportionate and necessary in a democratic society.

However, there has been an increased use of digital media as a tool of repression, harassment, and violence against in the online environment, primarily against celebrities, activists, and journalists. This is referred to as online violence.

Online violence is expressed in the forms of cyberbullying, harassment, cybersexism, unwanted sexual remarks, non-consensual posting of sexual media materials, threats, trolling, doxing, cyberstalking, discriminatory memes and skits, etc.

Online Safety

Billions of people around the world rely on digital services for education, work and social interaction. The internet needs to be a safe and secure space for all persons, businesses, civil society groups and governments. A safe and secure online experience is very important for global businesses, civil society groups and individuals alike. The internet enables the exercise of so many rights which are ultimately beneficial for everyone.

However, increasingly, safety issues have become a major problem. There are persistent challenges to combatting several issues, such as misinformation, false news, disinformation, child sexual abuse, trafficking and exploitation, terrorism and hate speech, and content related to self-harm and suicide.

Online repression, harassment, threats, and ridiculing of individuals through written messages, phone calls, and releasing of offensive pictures and videos over social media are known as cyberstalking or cyberharassment. These acts usually take different forms and are clear hindrances to other's full enjoyment of their rights online.

The Forms of Online Gender Based Violence

According to the Violence Against Persons Prohibition (VAPP) Act 2015, *“violence means any act or attempted act, which causes or may cause any person physical, sexual, psychological, verbal, emotional or economic harm whether this occurs in private or public life, in peace time and in conflict situations.”*

1. Doxing: the intentional revelation of a person's private information online without their consent, often with malicious intent.
2. Trolling: when someone posts or comments online to provoke people. In other cases, they may not agree with the views of another person or group online, so they try to discredit, humiliate or punish them. In some cases, they say things they don't even believe, just to cause drama. Trolls often post under a fake name or anonymously, so they can say things without being held responsible. This can make them feel more powerful.
3. Identity theft: This could also be regarded as identity piracy or identity infringement. This happens when one person (criminal) uses (steals) another person's personal information for their own gain, which usually is financial.
impersonation, catfishing...
4. Data breaches

5. Malware and viruses
6. Phishing and scam emails
7. Sextortion, and sexploitation
8. Fake websites
9. Online scams
10. Romance scams
11. Inappropriate content
12. Child pornography
13. Cyberbullying, cyberstalking and cyber threats
14. Faulty privacy settings
15. Suppression of information:
journalists are usually targets of this form. Journalists report that they have received different forms of violence in the line of their work, including threats of sexual assault and physical violence, abusive language, harassing private messages, threats to damage their professional or personal reputations, digital security attacks, misrepresentation via manipulated images and financial threats.
16. Threats of Political repression of expression
This usually involves state sponsorship of bots, anonymous and publicly identified individuals to harass women who have taken political positions.
17. Impersonation, Hacking, spamming, tracking and surveillance
Using of deep fake technologies, Artificial Intelligence and emerging technologies. Surveillance can be from both state and non-state actors.

Online Gender Based Violence (OGBV)

OGBV is targeted abuse and bias over the internet against people, disproportionately against those who identify as female.

It should be noted that all genders experience harassment online. However, women and gender minorities experience harassment of a sexual nature at higher rates¹⁶⁴.

¹⁶⁴ <https://www.unwomen.org/en/news/stories/2020/7/take-five-cecilia-mwende-maundu-online-violence>

Most threats and harassment against women spread sexualized hate. According to the Media Defence¹⁶⁵,

“Research has found that fake online accounts with feminine usernames incurred an average of 100 sexually explicit or threatening messages a day, while masculine names received only 3.7 messages.”

The Human Rights Council of the UN General Assembly recognised this huge dichotomy between women and men’s online presence in its July 2016 resolution¹⁶⁶ and it expressed as follows:

“that many forms of digital divides remain between and within countries and between men and women, boys and girls, and recognizing the need to close them, **Stressing** the importance of empowering all women and girls by enhancing their access to information and communications technology, promoting digital literacy and the participation of women and girls in education and training on information and communications technology, and encouraging women and girls to embark on careers in the sciences and information and communications technology...”

Most threats and harassment against women spread sexualized hate. Women and gender minorities experience harassment of a sexual nature at higher rates. Some threats are directed towards body shaming of their victims.

Some of this form of violence is not limited to women but also extends to other vulnerable groups such as intersex, cross dressers, asexual, bisexual, gay, queer, and lesbian.

The effect of OGBV is that it:

1. Discourages women from participating in online spaces, including social media and other forums thereby increasing the digital gender gap.
2. Self-censorship
3. Mental health
4. Reputational Damage and Insecurity
effects include mental health issues such as fear, panic attack, suspicion, distrust, low self-esteem, insomnia, depression, psychosis, increased stress, acting out violently and long-lasting emotional trauma even after the act has stopped.

¹⁶⁵ <https://www.mediadefence.org/resource-hub/resources/gender-online-harassment-factsheet/>

¹⁶⁶ See UN Resolution Supra

THE LEGAL FRAMEWORKS TO ADDRESS ONLINE VIOLENCE

The 1999 Constitution of the Federal Republic of Nigeria (as amended):

Sections 33-Right to life,

Section 34-Right to dignity,

Section 37-Right to privacy,

Section 38-Right to Religion, conscience and Thought, and

Section 39-Right to Freedom of Expression

Child Rights Act 2003 and laws (26 states)- Child pornography:

Section 8-privacy,

Section 11-dignity,

Section 31-unlawful sexual intercourse

Criminal Code:

Section 376 -Publishing defamatory matter with intent to extort,

Section 218-Defilement of girls under thirteen,

Penal Code:

Section 396-398 -Criminal intimidation by an anonymous communication,

Section 399- Intentional insult with intent to provoke breach of the peace,

Section 400-Word, gesture or act intended to insult the modesty of woman.

VAPP Act 2015:

Section 14- Emotional, Verbal and Psychological Abuse,

Section 17- Stalking,

Section 18- Intimidation,

The CyberCrimes (Prohibition, Prevention,etc) (Amendment) Act, 2024Section 23-

Child pornography and related offences,

Section 24- cyberstalking.

The Constitution

1. Section 34 provides that:

(1) Every individual is entitled to respect for the dignity of his person, and accordingly

– (a) no person shall be subject to torture or to inhuman or degrading treatment;

(b) no person shall be held in slavery or servitude; and (c) no person shall be required to perform forced or compulsory labour.

(2) for the purposes of Subsection (1) (c) of this section, "forced or compulsory labour" does not include - (a) any labour required in consequence of the sentence or order of a court; of the armed forces of the Federation or the Nigeria Police Force in pursuance of their duties as such;

(c) in the case of persons who have conscientious objections to service in the armed forces of the Federation, any labour required instead of such service;

(d) any labour required which is reasonably necessary in the event of any emergency or calamity threatening the life or well-being of the community; or

(e) any labour or service that forms part of – (i) normal communal or other civic obligations of the well- being of the community. (ii) such compulsory national service in the armed forces of the Federation as may be prescribed by an Act of the National Assembly, or (iii) such compulsory national service which forms part of the education and training of citizens of Nigeria as may be prescribed by an Act of the National Assembly

2. Right to Private and Family life:

Section 37 provides that the privacy of citizens, their homes, correspondence, telephone conversations and telegraphic communications is hereby guaranteed and protected.

3. Right to freedom of thought, conscience and religion

Section 38 provides that:

(1) Every person shall be entitled to freedom of thought, conscience and religion, including freedom to change his religion or belief, and freedom (either alone or in community with others, and in public or in private) to manifest and propagate his religion or belief in worship, teaching, practice and Observance

(2) No person attending any place of education shall be required to receive religious instruction or to take part in or attend any religious ceremony or observance if such instruction ceremony or observance relates to a religion other than his own, or religion not approved by his parent or guardian. (3) No religious community or denomination shall be prevented from providing religious instruction for pupils of that community or denomination in any place of education maintained wholly by that community or denomination. (4) Nothing in this section shall entitle any person to form, take part in the activity or be a member of a secret society.

4. Right to freedom of expression and the press.

2) Section 39 provides that:

(1) Every person shall be entitled to freedom of expression, including freedom to hold opinions and to receive and impart ideas and information without interference.

(2) Without prejudice to the generality of subsection (1) of this section, every person shall be entitled to own, establish and operate any medium for the dissemination of information, ideas and opinions: Provided that no person, other than the Government of the Federation or of a State or any other person or body authorised by the President on the fulfilment of conditions laid down by an Act of the National Assembly, shall own, establish or operate a television or wireless broadcasting station for, any purpose whatsoever. (3) Nothing in this section shall invalidate any law that is reasonably justifiable in a democratic society -

(a) for the purpose of preventing the disclosure. of information received in confidence, maintaining the authority and independence of courts or regulating telephony, wireless broadcasting, television or the exhibition of cinematograph films; or (b) imposing restrictions upon persons holding office under the Government of the Federation or of a State, members of the armed forces of the Federation or members of the Nigeria Police Force or other Government security services or agencies established by law.

The Vapp Act

Emotional, Verbal and Psychological Abuse

1) Section 14 (1) provides that a person who causes emotional, verbal and psychological abuse on another commits an offence and is liable on conviction to a term of imprisonment not exceeding 1 year or to a fine not exceeding N200,000.00 or both. 2) Section 14(2) provides that a person who commits the act of violence provided for in subsection (1) of this section commits an offence and is liable on conviction to a term of imprisonment not exceeding 6 months or to a fine not exceeding N100,000.00 or both. 3) Section 14(3) provides that a person who incites, abets, or counsels another person to commit the act of violence as provided for in subsection (1) of this section commits an offence and is liable on conviction to a term of imprisonment not exceeding 6 months or to a fine not exceeding N100,000.00 or both.

4) Section 14(4) provides that a person who receives or assists another who, to his or her knowledge, committed the offence provided for in subsection (1) of this section is an accessory after the fact and is liable on conviction to a term of imprisonment not exceeding 6 months or a fine not exceeding N100,000.00 or both.

Stalking

Section 17(1) provides that a person who stalks another commits an offence and is liable on conviction to a term of imprisonment not exceeding 2 years or to a fine not exceeding N500,000.00 or both.

2) Section 17(2) provides that a person who attempts to commit the act of violence provided for in subsection (1) of section commits an offence and is liable on conviction to a term of imprisonment not exceeding 1 year or to a fine not exceeding N200,000.00 or both.

3) Section 17(3) provides that a person who incites, aids, abets, or counsels another person to commit the act of violence as provided for in subsection (1) of this section commits an offence and is liable on conviction to a term of imprisonment not exceeding 1 year or to a fine not exceeding N200,000.00 or both.

4) Section 17(4) provides that a person who receives or assists another who, to his or her knowledge, committed the offence provided for in subsection (1) of this section is an accessory after the fact and is liable on conviction to a term of imprisonment not exceeding 1 year or to a fine not exceeding N100,000.00 or both.

Intimidation

1) Section 18(1) provides that a person who intimidates another commits an offence and is liable on conviction to a term of imprisonment not exceeding 1 year or to a fine not exceeding N200,000.00 or both.

2) Section 18(2) provides that a person who attempts to commit the act of violence provided for in subsection (1) of this section commits an offence and is liable on conviction to a term of imprisonment not exceeding 6 months or to a fine not exceeding N100,000.00 or both. 3) Section 18(3) provides that a person who incites, aids,

Abets, or counsels another person to commits an offence and is liable on conviction to a term of imprisonment not exceeding 6 months or to a fine not exceeding N100,000.00 or both.

4) Section 18(4) provides that a person who receives or assists another who, to his or her knowledge, committed the offence provided for in subsection (1) of this section is an accessory after the fact and is liable on conviction to a term of imprisonment not exceeding 6 months or to a fine not exceeding N100,000.00 or both.

The Child's Right Act

The United Nations Convention on the Right of the Child and African Charter on the Rights and Welfare of a Child were domesticated in Nigeria which led to the enactment of the Child's Right Act (2003) that provides for the rights of children in Nigeria.

Right to private and family life.

Section 8 (1) provides that every child is entitled to his privacy, family life, home, correspondence, telephone conversation and telegraphic communications, except as provided in subsection (3) of this section.

1) Section 8 (2) provides that no child shall be subjected to any interference with his right in subsection (1) of this section, except as provided in subsection (3) of this section.

2) Section 8 (3) provides that nothing in the provision of subsections (1) and (2) of this section shall affect the rights of parents and, where applicable, legal guardians, to exercise reasonable supervision and control over the conduct of their children and wards.

Right to dignity of the child

1)Section 11 provides Every child is entitled to respect for the dignity of his person, and accordingly, no child shall be-

(a) subjected to physical, mental or emotional injury, abuse, neglect or maltreatment, including sexual abuse;

(b) subjected to torture, inhuman or degrading treatment or punishment;

(c) subjected to attacks upon his honour or reputation; or (d) held in slavery or servitude, while in the care of a parent, legal guardian or school authority or any other person or authority having the care of the child.

Unlawful sexual intercourse with a child

1)Section 31 provides that

(1) No person shall have sexual intercourse with a child.

(2) A person who contravenes the provision of Subsection (1) of this section commits an offence of rape and is liable on conviction to imprisonment for life.

(3) Where a person is charged with an offence under this section, it is immaterial that (a) the offender believed the person to be of or above the age of eighteen years; or

(b) the sexual intercourse was with the consent of the child

The Criminal Code

Publishing defamatory matter with intent to extort.

3) Section 376 provides that any person who publishes, or threatens to publish, or offers to abstain from publishing, or offers to prevent the publication of defamatory matter, with intent to extort money or other property, or with intent to induce any person to give, confer, procure, or attempt to procure, to, upon, or for, any person, any property or benefit of any kind. is guilty of a felony and is liable to imprisonment for seven years.

Defilement of girls under thirteen

Section 218 any person who has unlawful carnal knowledge of a girl under the age of thirteen years is guilty of a felony, and is liable to imprisonment for life, with or without caning.

Any person who attempts to have unlawful carnal knowledge of a girl under the age of thirteen years -is guilty of a felony, and is liable to imprisonment for fourteen years, with or without caning.

A prosecution for either of the offences defined in this section shall be begun within two months after the offence is committed. A person cannot be convicted of either of the offences defined in this section upon the uncorroborated testimony of one witness.

The Penal Code

Criminal intimidation by an anonymous communication

1) Section 396 provides that whoever threatens another with an injury to his person, reputation or property or to the person reputation or property of anyone in whom that person is interested, with intent to cause alarm to that person or to cause that person to do any act which he is not legally bound to do or to omit to do an act which that person is legally entitled to do as the means of avoiding the execution of that threat, commits criminal intimidation.

2) Section 397 provides that whoever commits the offence of criminal intimidation shall be punished:

(a) with imprisonment for a term which may extend to two years or with fine or with both; and

(b) if the threat be to cause death or grievous hurt or to cause the destruction of any property by fire or to cause an offence punishable with death or with imprisonment for a term which may extend to seven years or to impute unchastely to a woman, with imprisonment for a term which may extend to seven years or with fine or with both.

3) Section 399 provides that whoever uses insulting or abusive language concerning, or otherwise conducts himself towards, a person or class or group of persons, whether the person or any member of that class or group is present or not, in a manner likely to give the provocation to a person present as to cause the last mentioned person to break the public peace or to commit any other offence shall be punished with imprisonment for a term which may extend to two years or with fine or with both.

Criminal intimidation by an anonymous communication.

1) Section 398 provides that whoever commits the offence of criminal intimidation by an anonymous communication or having taken precaution to

conceal the name or abode of the person from whom the threat comes, shall be punished with imprisonment for a term which may extend to two years in addition to the punishment provided for the offence by section 397 of this Penal Code.

Intentional insult with intent to provoke breach of the peace

1) Section 399 provides that whoever uses insulting or abusive language concerning, or otherwise conducts himself towards, a person or class or group of persons, whether the person or any member of that class or group is present or not, in a manner likely to give the provocation to a person present as to cause the last mentioned person to break the public peace or to commit any other offence shall be punished with imprisonment for a term which may extend to two years or with fine or with both.

Word, gesture or act intended to insult the modesty of woman.

1) Section 400 provides that whoever intending to insult the modesty of a woman utters a word, makes a sound or gesture or exhibits an object, intending that the word or sound shall be heard or that the gesture or object shall be seen by such woman or intrudes upon the privacy of such woman, shall be punished with imprisonment for a term which may extend to one year or with fine or with both.

The CyberCrimes (Prohibition, Prevention, etc) (Amendment) Act, 2024

Child pornography and related offences.

1) Section 23 provides that: (1) Any person who intentionally uses any computer system or network in or for-

(a) producing child pornography;

(b) offering or making available child pornography;

(c) distributing or transmitting child pornography;

(d) procuring child pornography for oneself

or for another person; (e) possessing child pornography in a computer system or on a computer-data storage medium:

commits an offence under this Act and shall be liable on conviction –

(i) in the case of paragraphs (a), (b) and (c) to imprisonment for a term of 10 years or a fine of not more than N20,000,000.00 or to both fine and imprisonment; and

(ii) in the case of paragraphs (d) and (e) of this subsection, to imprisonment for a term of not more than 5 years or a fine of not more than N10,000,000.00 or to both such fine and imprisonment.

(2) Any person who knowingly makes or sends other pornographic images to another computer by way of unsolicited distribution shall be guilty of an offence and upon

conviction shall be sentenced to One year imprisonment or a fine of Two Hundred and Fifty Thousand Naira or both.

(3) Any person who, intentionally proposes, grooms or solicits, through any computer system or network, to meet a child for the purpose of:

a) engaging in sexual activities with the child; (b) engaging in sexual activities with the child where –

(i) use is made of coercion, inducement, force or threats; (ii) abuse is made of a recognized position of trust, authority or influence over the child, including within the family; or Child pornography and related offences.

(iii) abuse is made of a particularly vulnerable situation of the child, mental or physical disability or a situation of dependence; (c) recruiting, inducing,

coercing, exposing, or causing a child to participate in pornographic performances or profiting from or otherwise exploiting a child for such purposes;

commits an offence under this Act and shall be liable on conviction- (i) in the case of paragraphs (a) to imprisonment for a term of not more than 10 years and a fine of not more than N15,000,000.00; and

(ii) in the case of paragraphs(b) and(c) of this

subsection, to imprisonment for a term of not more than 15 years and a fine of not more than N25,000,000.

(4) For the purpose of subsection (1) above, the term “child pornography” shall include pornographic material that visually depicts-(a) a minor engaged in sexually explicit conduct;

(b) a person appearing to be a minor engaged in sexually explicit conduct; and

(c) realistic images representing a minor engaged in sexually explicit conduct.

(5) For the purpose of this section, the term “child” or “minor” means a person below 18 years of age.

Cyberstalking

1) Section 24 provides that any person who knowingly or intentionally sends a message or other matter by means of computer systems or network that -

(a) is grossly offensive, pornographic or of an indecent, obscene or menacing character or causes any such message or matter to be so sent; or

(b) he knows to be false, for the purpose of causing annoyance, inconvenience danger, obstruction, insult, injury, criminal intimidation, enmity, hatred, ill will or needless anxiety to another or causes such a message to be sent:

commits an offence under this Act and shall be liable on conviction to a fine of not more than N7,000,000.00 or imprisonment for a term of not more than 3 years or to both such fine and imprisonment.

2) Section 24 (2) provides that any person who knowingly or intentionally transmits or causes the transmission of any communication through a computer system or network

(a) to bully, threaten or harass another person, where such communication places another person in fear of death, violence or bodily harm or to another person;

(b) containing any threat to kidnap any person or any threat to harm the person of another, any demand or request for a ransom for the release of any kidnapped person, to extort from any person, firm, association or corporation, any money or other thing of value; or

(c) containing any threat to harm the property or reputation of the addressee or of another or the reputation of a deceased person or any threat to accuse the addressee or any other person of a crime, to extort from any person, firm, association, or corporation, any money or other thing of value:

commits an offence under this Act and shall be liable on conviction-

(i) in the case of paragraphs (a) and (b) of this subsection to imprisonment for a term of 10 years and/or a minimum fine of N25,000,000.00; and

(ii) in the case of paragraph (c) and (d) of this subsection, to imprisonment for a term of 5 years and/or a minimum fine of N15,000,000.00.

(3) A court sentencing or otherwise dealing with a person convicted of an offence under subsections (1) and (2) may also make an order, which may, for the purpose of protecting the victim or victims of the offence, or any other person mentioned in the order, from further conduct which-

(a) amounts to harassment; or (b) will cause fear of violence, death or bodily harm; prohibit

the defendant from doing anything described/specified in the order.

(4) A defendant who does anything which he is prohibited from doing by an order under this section, commits an offence and shall be liable on conviction to a fine of not more than N10,000,000.00 or imprisonment for a term of not more than 3 years or to both such fine and imprisonment.

(5) The order made under subsection (3) of this section may have effect for a specified period or until further order and the defendant or any other person mentioned in the order may apply to the court which made the order for it to be varied or discharged by a further order.

(6) Notwithstanding the powers of the court under subsections (3) and (5), the court may make an interim order for the protection of victim(s) from further exposure to the alleged offences.

MODULE 9

ADDITIONAL JURISPRUDENCE ON DIGITAL RIGHTS

PRIVACY CASES

Digital Rights Lawyers Initiative v National Identity Management Commission SUMMARY OF FACTS OF THE CASE

In 2020, the 2nd Appellant—a Nigerian Citizen approached the National Identity Management Commission (NIMC) for the rectification of his date of birth on his National Identification Number (NIN) slip. To grant the 2nd Appellant’s request, NIMC demanded the sum of N15, 000 (Fifteen thousand Naira) as provided by its policy on management of citizens’ identity. The Appellants consequently approached the Federal High Court sitting in Abeokuta, Ogun State challenging the demand for money as violating right to privacy guaranteed by section 37 of the Constitution of the Federal Republic of Nigeria, 1999. At the trial court, the Appellants invited the court to resolve the following questions: 1. Whether or not by section 37 of the constitution of the Federal Republic of Nigeria, 1999 (as amended), the Respondent’s act of demanding for payment for rectification/correction of personal data is likely to interfere with the Applicant’s right to private and family life?

2. Whether or not by the provisions of article 3.1(1)(7)(h) of the Nigeria Data Protection Regulation, 2019 (NDPR), the Applicant can request for rectification/correction of personal data from the Respondent free of charge?

When the trial court upheld NIMC’s objection to its jurisdiction, the Appellants appealed to the Court of Appeal sitting in Ibadan, Oyo State.

DECISION OF THE COURT

Although the court dismissed the appeal, the judgment made some far– reaching resolutions of issues bordering on right to privacy in Nigeria as follows:

The trial court, rightly held that the right to ‘privacy of citizens’ as guaranteed under the section includes the right to protection of personal information and personal data.’

“On the relationship between the NDPR 2019 and section 37 of the CFRN 1999, it is pertinent for me to state that the CFRN 1999 makes provision in chapter IV guaranteeing the various fundamental rights of citizens. But, the nature and scope of those rights and even their limitations are in most instances, furthered by other statutes, regulations or other legal instruments. It is in this instance that the NDPR must be construed as

providing one of such legal instruments that protects or safeguards the right to privacy of citizens as it relates to the protection of their personal information or data which the trial court had rightly adjudged to be part of the right to privacy guaranteed by section 37 of the CFRN.”

OBSERVATION

Although the court dismissed the appeal, its resolution is very instructive and valuable for litigating right to privacy and data protection in the Nigerian courts. The judgment also represents the first appellate court decision on the nature and objectives of the Nigeria Data Protection Regulation (NDPR) as a (subsidiary) legislation that complements the right to privacy guaranteed in the Nigerian Constitution. However, the court’s conclusion that a suit that borders on the exercise of data subject’s right to rectification of personal data has nothing to do with right to privacy leaves so much to be desired especially having established the link between the concept of data protection and notion of privacy. The court identified the relationship and interoperability between the NDPR and right to privacy but later in the judgment altered its position when it agreed with the trial court that rectification of date of birth has nothing to do with right to privacy. This position disturbingly negates the Court of Appeal’s finding that the provisions of the NDPR fall under the right to privacy under the Constitution. As celebrated as this decision appears, it seems to have taken with another hand, what it gives with one hand. If the court can hold that a suit bordering on data subject’s right to rectification of personal data has nothing to do with right to privacy, then one can only hope that this decision does not constitute a readymade shield to subsequent suits seeking to enforce other data subject’s rights in court under the fundamental rights enforcement procedure.

Incorporated Trustee of Digital Rights Lawyers Initiative (DRLI) v Central Bank of Nigeria (CBN)

SUMMARY OF FACTS

On the 6th day of August 2020, a commercial bank (First Bank of Nigerian Plc.) hosted a virtual Financial Technology Summit themed “How Blockchain and Artificial Intelligence will Disrupt Fintech in Nigeria”. During the summit Central Bank’s Director for payment system management, Mr Musa Jimoh announced that “the Central Bank of Nigeria (Respondent herein) has directed commercial banks to share their customers’ data with financial technology (Fintech) companies. DRLI consequently approached the court challenging the directive as a likely interference with customers’ right to privacy guaranteed under Section 37 of the Constitution of the Federal Republic of Nigeria and

relevant provisions of the Nigeria Data Protection Regulation. The Respondent raised a preliminary objection on the following grounds:

1. By the provision of section 53 (1) of the Banks and other Financial Institution Act, Section 52 of the Central Bank of Nigeria (Establishment) Act, 2007, the suit cannot be maintained against the Respondent.
2. By the provision of article 2.2 (e) of the Nigeria Data Protection Regulation 2019 and section 33 (1) (a) of Central Bank of Nigeria (Establishment) Act 2007, the suit did not disclose a reasonable cause of action.

After hearing the parties, the court however upheld the preliminary objection and dismissed the substantive suit.

DECISION OF THE COURT

Notwithstanding the dismissal of the substantive application, the judgment of the court made some pronouncements on right to privacy and data protection in Nigeria as follows:

On the core objectives of the FREP rules;

“Firstly, it must be stated that core objectives of the Fundamental Rights Enforcement Procedure Rules 2009 are stipulated in preamble 3 (c) to wit:

“(c) For the purpose of advancing but never for the purpose of restricting the Applicant’s rights and freedoms, they may make consequential orders as may be just and expedient.”

As such, the above objective is aimed at enhancing access to justice for all persons who desire to enforce their fundamental rights...”

On whether status of limitation affects an application for enforcement of fundamental right;

“...it is no wonder the provision of Order 3 Rule 1 of the FREP Rules 2009. It provides; *“An application for enforcement of Fundamental Right shall not be affected by any limitation statute whatsoever.”*

On whether the Respondent can make validly directive to commercial banks to share data to third party without consent of data subject;

“I find that a community reading of Regulation 2.2 (e) of Nigeria Data Protection Regulation 2019 and Section 2 (d) of the C.B.N. Act 2007 avails the Respondent/Applicant’s directive, unless and until the Applicant/Respondent shows the contrary, which he has not done, due to his failure to expose that Respondent/Applicant’s directive was not done in good faith, I hereby discountenance Applicant/ Respondent’s issues one and two.” Pages 18–19.

On the Power of C.B.N. to share information; “...I hold simpliciter, that Section 33 (1) (a) of the C.B.N. Act 2007, would mean “all Information” received by

Respondent/Applicant could be used in the interest of the society, and same provision is apposite to this suit. See Chief Obafemi Awolowo v. Alhaji Shehu Shagari and 2 Ors (1979) All NLR 120.” Page 20.

On what applicant must show to prove interference with data subject’s rights;
“More so, the deponent left in abeyance how the Respondent/Applicant’s directive will interfere with his right to privacy guaranteed under the Nigeria Data Protection Regulation and section 37 of the Constitution. No doubt, this is a salient fact which ought to have been particularized. The case of Peak Merchant Bank Limited v. C.B.N. & Ors (2017) LPELR 42324 (CA) captures the importance of stating the facts of bad faith as follows;

“The elements and/or particulars that constituted the bad faith is not alleged clearly or definitely (positively) in the statement of claim.” It was held by the Apex court in the case of N.D.I.C. V. C.B.N (supra) in pages 297 that “... in order that the court may have jurisdiction to entertain the type of action now in question, the Plaintiff/Respondent has to show or alleged bad faith in the way the revocation was done and indicate the elements that constitute bad faith... unless bad faith is positively alleged by way of its elements... an allegation without its elements cannot be regarded as positive.” Page 24–25.

OBSERVATION

Although the suit was dismissed, the few pronouncements on data protection gives some form of encouragement that our courts are now giving due cognizance to the notion of privacy under section 37 of the 1999 Constitution of the Federal Republic of Nigeria (As Amended). This can be seen as expressed by the court in the case in view when it held thus; “More so, the deponent left in abeyance how the Respondent/Applicant’s directive will interfere with his right to privacy guaranteed under the Nigeria Data Protection Regulation and Section 37 of the Constitution.”

Incorporated Trustees of Digital Right Lawyers Initiative v. L.T. Solutions & Multimedia Limited

SUMMARY OF FACTS

On the 2nd day of May 2020, LT Solutions Multimedia Limited, through its Twitter handle tweeted that: “over 200 million fresh Nigerian and international emails lists, sorted by age, state, LGA, city, industry etc send a dm or call 08139745545 to get yours”. The privacy policy published on the company’s website showed that the Respondent collects personal data of citizens, but it did not explain how data subject’s consent were sought and obtained among other deficiencies. At the High Court of Ogun State, DRLI

filed an action claiming among other things that: data protection is guaranteed under the right to privacy in section 37 of the CFRN and the Respondent's processing of data of over 200 million Nigerians without legal basis violates the provisions of the NDPR and likely to interfere with their right to privacy.

DECISION OF THE COURT

The Applicant submitted four (4) issues for the determination, but the court re-couched the issues into three (3) and decided the matter on the basis of those issues.

On whether the right to privacy extends to protection of personal data:

The court referred to *Nwali v. Ebonyi State Independent Electoral Commission & Ors*¹⁴ for the proposition that the court has no power to restrict the phrase "privacy of citizens" to specific situations but must interpret it generally, liberally, and expansively. The court also referred to some sector-specific regulations in relation to data protection to establish that the regulations made pursuant to section 37 of the CFRN show that the provisions are to be interpreted expansively and liberally to ensure the privacy of citizens. The court then reproduced the preamble to the NDPR and its objectives and found that:

"In the light of the above, I thus also have no hesitation in holding that the right to privacy extends to protection of a citizen's personal data such [has] been alleged that the Respondent has violated or is threatening to violate as I now go on consider whether the Respondent has indeed violated the Applicant's right to privacy or threatens to violate it." (page 7).

On whether the Respondent failed to comply with the provision of the NDPR:

The court relied on Article 2.5 of the NDPR in resolving this issue. The said Article 2.5 provides thus: "Notwithstanding anything contrary in this Regulation or any instrument for the time being in force, any medium through which personal data is being collected or processes shall display a simple and conspicuous privacy policy that the class of data subject being targeted can understand. The privacy policy shall in addition to any other relevant information contain the following ..." (page 7).

In deciding whether the Respondent complied with the above provision of the NDPR, the court referred to depositions in the affidavit in support of the Applicant's originating motion to the effect that the Respondent was processing the private data of citizens without legal basis and without compliance with the NDPR. The court held that "Since no counter affidavit or any other processes have been filed by the Respondents, it means that the Applicant only needs minimal proof of the facts in respect of the reliefs claimed in this suit."

The court held further thus:

“Firstly, I agree with the Applicant that the Respondent qualifies as a data controller under section 1.3(g) of the NDPR Regulations, as members of the Applicant will also qualify as data subject under section 1.3(k) of the Regulations. I have also painstakingly gone through the facts in support of this Relief, as contained in the above– mentioned paragraphs and Exhibits 2 and 3, and I am also constrained to agree with the Applicants that the Respondent as a Data Controller has failed to comply with the Regulations by its failure to publish a privacy policy as provided under section 2.5 of the Regulations showing the requisite information requested therein.” (page 9).

On whether the Respondent violated the right of the Applicant: “I am however unable to agree with the Applicant that this infraction of the Regulations by simply failing to publish a privacy policy impinges on the privacy rights of the members of the Applicant without a clear and unambiguous deposition that the Respondent as a Data Controller failed to obtain the consent of data subject (such as any of the Applicant’s members) in contravention of the provisions of Section 2.3 of the Regulations relating to the procuring of consent which is reproduced hereunder as follows:

Section 2.3 Procuring Consent

No data shall be obtainable except the specific purpose of collection is made known to the Data Subject. Data Controller is under obligation to ensure that consent of a Data Subject has been obtained without fraud, coercion or undue influence, according ... The point I am struggling to make is that, notwithstanding the fact that I have found that the Respondent failed to comply with the law by publishing its privacy policy, the nature of these proceedings not being criminal or quasi criminal in nature, but one for the determination of whether the right of privacy guaranteed under section 37 of the Constitution has been infringed or is likely to be infringed it behoves the deponent to the Applicant’s affidavit in support to further show clearly how this failure to publish its privacy policy infringed this right to privacy as this failure simpliciter does not show an infringement of the right to privacy without an unambiguous deposition that any data subject’s information has been processed without his (or her) consent. I am thus unable to find that the right to privacy of the Applicant’s members have been infringed or is likely to be infringed.”

On whether the court would order the Respondent to comply with the provisions of the NDPR or find the Respondent liable to pay a fine: “...my earlier position that this is not a criminal or quasi criminal nature robs this Court of the jurisdiction to determine these issues, and perhaps more importantly, this Court as a State High Court will lack the jurisdiction to determine these issues having regard to the fact that these Regulations are made by a body established by an Act of the National Assembly i.e. a Federal legislation and not under a State Law as it is trite that unless a Federal Act permits a State High

Court to determine the infractions under these Regulations such as are applicable by statutory provisions for trials under the Robbery and Firearms Act for trials of Armed Robbery cases, or matters prosecuted under the Economic and Financial Crimes (EFCC) Act and Independent Corrupt Practices Commission (ICPC) Act. It is the Federal High Court that will thus have jurisdiction to determine this issue and I believe more appropriately upon the filing of criminal charges by the relevant government Agency, presumably the NITDA against transgressors of the Regulations which must necessarily arise after the arraignment of such transgressor including plea taking. The Reliefs related to these issues are thus liable to be struck out.”

OBSERVATION

This is the first decision of a court in Nigeria to hold that the rights of data subjects under the NDPR are part of the right to privacy and family life under section 37 of the CFRN. Shortly after this decision, the Federal High Court took a contrary view in Incorporated Trustees of Laws and Rights Awareness Initiative v. The National Identity Management Commission (ITLRAI v. NIMC) that a breach of the rights of a data subject under the NDPR is not necessarily a breach to right to private and family life under section 37 of the CFRN. Hence, an action for the interpretation of the provisions of the NDPR cannot be brought under the FREP Rules. However, the conflicting positions in this judgment and the decision in ITLRAI v. NICM have now been settled by the decision of the Court of Appeal in Incorporated Trustees of Digital Rights Lawyers Initiative & Ors v. National Identity Management Commission¹⁶, wherein the Court of Appeal held that personal data protection as provided in the NDPR generally falls under the fundamental right to privacy guaranteed in section 37 of the CFRN. This remains the law until an appeal from the decision or any other decision to the Supreme Court is decided against the position of the Court of Appeal. One would have thought that the finding of the court that the rights to privacy under the CFRN extends to the rights of data subjects under the NDPR, implies that an action for breach of such would be cognizable under the FREP Rules 2009 which defines “court” as the Federal High Court, High Court of a State or High Court of the Federal Capital Territory, Abuja¹. A controller’s liability for failure to fulfil its duty to clearly publicize its privacy policy is different from its duty to obtain consent of data subjects under the NDPR and same ought not to be fused or confused as done in this judgment. Under the NDPR, the requirement to procure consent for processing of personal data¹⁸ is different from the requirement to publicize clear privacy policy.¹⁹ Even with or without obtaining consent, a breach of the requirement to publicize privacy policy alone, makes the Respondent liable. The holding of the court that the deponent of the affidavit in support of the originating summons ought to have deposed to facts that the Respondent did not obtain the consent of Applicant’s members before processing their data, with respect, lost sight of the earlier finding of the court that the rights of data

subject under the NDPR are part of the right to privacy in section 37 of the CFRN. That pronouncement of the court did more than a mere christening of the rights under the NDPR, it exalted those rights to the prestigious status of fundamental rights guaranteed by the CFRN, and in enforcing fundamental rights, a citizen does not have to wait until the rights are actually violated, a citizen could sue once he alleges that any of his rights has been, is being or likely to be contravened²⁰. 18 Article 2.3 of the NDPR. 19 Article 2.5 of the NDPR. 20 Section 46(1) of the CFRN.

Incorporated Trustees of Digital Rights Lawyers Initiative v. Minister of Industry, Trade and Investment & 2 Ors.

SUMMARY OF FACTS

In 2020, the Federal Government of Nigeria through the Ministry of Industry, Trade and Investment, set up a Micro Small and Medium Enterprise (MSME) Survival Fund. Applications for the grant were made through an online portal hosted as <https://www.survivalfund.gov.ng> through which personal data (including Bank Verification Number (BVN) and other sensitive data of Nigeria citizens that applied for the said federal government funds were processed. In September 2020, some members of DRLI sought to apply for the Survival Fund online and discovered that the 1st Respondent did not comply with the NDPR as they failed to publish a privacy policy or notice on the portal hosted online. Also, the Ministry neither appointed a data protection officer (DPO) nor developed any security measures to protect data, store data securely in the said online application portal. DRLI consequently approached the court on behalf of its members, claiming that the Respondent has violated the provisions of the NDPR and interfered with the right to privacy of its members.

DECISION

In granting all the reliefs sought by DRLI, the court held as follows:

On who is a Data Controller.....

First, I quite agree with Applicant that indeed the 1st Respondent is a data controller by virtue of Regulation 1.3(x) NDPR which defines a data controller as “a person who either alone, jointly with other persons or in common with other person or a statutory body, determines the purpose for and the manner in which persona/ data is processed or to be processed. (p.18)

On when a Data Controller will be held liable for breach of data privacy of a data subject The 1st Respondent did not deny the Applicant's case by providing any evidence to show that the obligations set out above as a data controller were complied with. The Applicant furnished the Court with Exh.3–6 which are photographs of the MSME Survival Fund Program online portal and in them I see that neither of the obligations required of the 1st Respondent were complied with. The 1st Respondent beyond saying generally in Paragraph 9 and 10 of the counter affidavit that the portal was set up and being used with all security measures and statutory provisions regarding the privacy of data being collected, and that the operation of the survival fund were transparent and available to members of the public, it did not provide any details to demonstrate or prove compliance with the privacy protecting and securing measures outlined in the Regulations. All things considered, I hold that the failure of the Respondents, from taking measures towards protecting the data privacy of the citizens, taking into account the vital information required from the data subject such as the Bank Verification Number, names and addresses, poses a threat to the Applicant's members right to private and family life owing to the fact that the objectives of the NDPR as provided in Regulation 1.1 is to safeguard the rights of natural persons to data privacy. (p.20)

OBSERVATION

This decision is an historic one in the sense that, the court pronounced that threat to data privacy of citizen amounts to breach of fundamental right to private and family life. It is the first decision where the Nigerian court would rule on the importance of publication of a privacy policy and its impact on data protection and privacy rights. The court categorically held that the non-publication of the privacy policy among other things violated the provision of the NDPR and interfered with the right to privacy guaranteed under section 37 CFRN.

INCORPORATED TRUSTEES OF DIGITAL RIGHTS LAWYERS INITIATIVE & 2 OTHERS V. NATIONAL IDENTITY MANAGEMENT COMMISSION SUMMARY OF FACTS

Sometime in February 2020, Mr. Atayero (the 2nd Applicant) approached the National Identity Management Commission (NIMC) for the rectification of his date of birth on his National Identification Number (NIN) slip. To grant the 2nd Applicant's request, NIMC demanded the sum of N15, 000 (Fifteen thousand Naira) as provided by its policy management of citizens' identity.

The Applicant consequently approached the High Court sitting in Abeokuta, Ogun State challenging the demand for money before rectification of his personal data as a violation

of their right to privacy guaranteed by section 37 of the Constitution of the Federal Republic of Nigeria, 1999 and Article 3.1 (1) (7) (h) of the Nigeria Data Protection Regulation 2019. The court was invited to resolve the following questions:

1. Whether or not by construction of section 37 of the constitution of the Federal Republic, 1999 (as amended), the Respondent's act of demanding for payment for rectification/correction of personal data is likely to interfere with the Applicant's right to private and family life?

2. Whether or not by the provisions of article 3.1(1)(7)(h) of the Nigeria Data Protection Regulation, 2019 (NDPR), the Applicant can request for rectification/correction of personal data from the Respondent free of charge?

The Court in delivering its judgment per Hon. Justice A.A Akinyemi without delving into the main issue struck out this suit while upholding the objections of the Defendant.

DECISION OF THE COURT

Although the court dismissed the suit on three grounds without delving into the main suit, nonetheless a part of the judgment made some far-reaching resolution of issues bordering on right to privacy in Nigeria as follows:

On the relationship between privacy and data protection, the trial court found that:

“The kernel of both the provision of section 37 of the constitution and these illuminating decisions is, to my mind, that privacy of a citizen of Nigeria shall not be violated. From these decisions, privacy to my mind can be said to mean the right to be free from public attention or the right not to have others intrude into one's private space uninvited or without one's approval. It means to be able to stay away or apart from others without observation or intrusion. It also includes the protection of personal information from others. This right to privacy is not limited to his home but extends to anything that is private and personal to his including communication and personal data.’ (page 8)

OBSEERVATION

Thankfully, the Court in its resolution at page 8 of its judgment identified that the right to personal data is part of the right to privacy as enshrined under section 37 of the Constitution of the Federal Republic of Nigeria 1999 (as amended). Shockingly, the same court went further to say that the demand for payment of N15, 000 for correction of the date of birth of the 2nd Applicant has absolutely nothing to do with his privacy. (see page 12). The court arrived at this decision without attempting to look at the provisions of article 3.1 (8) of the NDPR which gives data subjects the right to obtain from a Controller without undue delay the rectification of inaccurate personal data concerning him or her.

The court also failed to consider that the objective of the NDPR is to safeguard the right to privacy as captured under section 37 of the constitution.

Digital Rights Lawyers Initiative v National Youth Service Corps

SUMMARY OF FACTS

Sometime in 2020, the Respondent coerced Corps members especially the most recent corps members i.e. Batch B Stream 1, to sign Data Subject Consent Forms on the eve of their passing out as a precondition for their final discharge in Oyo State and other states of the Federation. The personal data collected from the Corp members were subsequently published in magazines which bear the names, phone numbers, image photographs and other personal information of the Corp members. DRLI consequently challenged the act as a violation of the certain provisions of the NDPR and section 37 of the Constitution which guarantees right to privacy.

The court was invited to resolve the following questions:

- a. Whether or not by the interpretation of Section 37 of the Constitution of the Federal Republic of Nigeria 1999 (as amended) and articles 1.1 (a), 2.1 (a) 2.2 & 2.3 of the Nigeria Data Protection Regulation 2019, the Respondent's processing of NYSC Corp members personal data in an End of the Year Service Magazine/Photo Album without their freely given consent constitute a violation of the Corp members' right to privacy?
- b. Whether or not by the interpretation of article 1.3 (iii) of the Nigeria Data Protection Regulation 2019, the Respondent's "Data Subject Consent Statement" attached as a condition for Discharge Certificate qualifies as freely given consent?

After hearing the parties, the court dismissed the suit but made some pronouncement on issues bordering on right to privacy.

DECISION OF THE COURT

Although the court dismissed the suit, the trial court made a slight pronouncement on a novel area of data protection in Nigeria especially on data subject's consent as follows:

On locus standi to strategically litigate data protection, the court observed "It pertinent to state that paragraph 3(e) of the Preamble to the Fundamental Rights (Enforcement Procedure) Rules 2009, read as follows;

"The Court shall encourage and welcome public interest litigations in the human rights field and no human rights case may be dismissed or struck out for want of locus standi. In particular, human rights activists, advocates, or groups as well as any non-governmental organizations, may institute human rights application on behalf of any potential applicant.

In human rights litigation, the applicant may include any of the following: (i) Anyone acting in his own interest; (ii) Anyone acting on behalf of another person; (iii) Anyone acting as a member of, or in the interest of a group or class of persons; (iv) Anyone acting in the public interest, and (v) Association acting in the interest of its members or other individuals or groups”

Predicated on the above, the Applicant has instituted this suit on behalf of 2019 Batch C Corp members of the Respondent”. (Pages 16–17)

On nexus between Nigeria Data Protection Regulation 2019 and right to privacy under the constitution:

“Section 37 of the Constitution of the Federal Republic of Nigeria 1999 (as amended) provides:

“The privacy of citizens, their homes, correspondence, telephone conversations and telegraphic communications is hereby guaranteed and protected”.

There is no gain to say that Fundamental rights are constitutionally guaranteed and protected with a specific provision preserving same as specified in the Constitution, which provides that, in case of a breach of that right, the person aggrieved can approach the High Court for redress. See Section 46(1) of the Constitution of the Federal Republic of Nigeria 1999 (as amended). However, it must be said that these fundamental rights entrenched in Chapter IV (Four) of the Constitution are not always absolute in so far as they co-exist with other validly made laws” (e.g. Nigeria Data Protection Regulation 2019)” (pages 17–18).

On whether Section 20 of the National Youth Service Corp Act divest the court to entertain an action for enforcement of fundamental rights of a Corp member:

“It apt to settle the preliminary issue of jurisdiction raised by learned counsel of the Respondent in his submission in opposition to this suit. In the case of UBA v Johnson (2018) LPELR–45073 (CA) the Court of Appeal held as follows:

“Following from all that has been said above, and as it is glaring that it is not the intendment of the FREP Rules that the enforcement by a person of his fundamental right is to be subjected to the fulfilment of any condition precedent whatsoever, once the proceeding is initiated by a process accepted by the trial Court, it becomes obvious that Appellant issue 5 must be and is hereby resolved against them”. In that wise I hold that section 20 of the National Youth Service Corp Act, Cap N84, LFN, 2004 cannot divest this court of the jurisdiction to entertain this suit. (page 18–19)

On when a Controller may be held to have properly obtained Data subjects’ consent under the NDPR “A look at Exhibit 2 not only reveals a consent form, but it also contains

leeway for the 2019 Batch B Stream 1 Corp members to waive their consent at any time, by use of DATA SUBJECT WITHDRAWAL FORM... (page 20)... In the instance of this case, I hold squarely that the Exhibit 2 is not an infringement of Applicant fundamental rights encapsulated in Section 37 of the Constitution of the Federal Republic of Nigeria 1999 (as amended), and the Exhibit 2 have not exposed at all that the applicant were railroaded into a straitjacket all for the sake of their graduation/passing out certificate”. (page 21) “Pointedly I find that Exhibit 2 annexed to the Originating Summons have fully complied with the Nigeria Data Protection Regulation 2019. And crucial to set out is Article 2.3 (2) (c) to wit: “Prior to giving consent, the Data subject shall be informed of his right and method to withdraw his consent at any given time. However, the withdrawal shall not affect the lawfulness of processing based on the consent before its withdrawal”. (page 22)

OBSERVATION

Although, the court dismissed the suit, its resolution on how a data controller can satisfy the provision of the NDPR with respect to data subjects’ consent. While the suit also confirms DRLI’s locus standi to strategically litigate digital rights under the FREP Rules, it is ultimately hoped that it will serve as a caution to the government agencies and other private institutions that process citizens’ personal information without consent or other lawful basis as required by law.

INCORPORATED TRUSTEES OF DIGITS RIGHTS AND LAWS INITIATIVE V HABEEB OLASUNKANMI RASAKI

SUMMARY OF FACTS

This suit was filed by DRLI on behalf Mr. Leslie Aihevba against the Respondent who has printed various WhatsApp conversations of the former over a period of time. Due to the sensitive nature of the conversations, DRLI approached the court to stop the Respondent from further processing (especially sharing and use) of the WhatsApp messages. DRLI submitted the following questions for determination:

- a. Whether or not by the interpretation and construction of paragraph 3(e)(v) of the Preamble to the Fundamental Rights Enforcement Procedure Rules and Section 46 of the Constitution 1999 (as amended) and article 4.8 of the NDPR the Applicant has locus standi to commence action for and on behalf of Mr. Leslie Aihevba.
- b. Whether or not by the construction of article 1.1(a) of the Nigerian Data Protection Regulation 2019 and section 37 of the Constitution (as amended) data protection is guaranteed under right to private and family life.

c. Whether or not the applicant is entitled to the reliefs sought.

The Respondent filed a counter affidavit and written address in opposition, contending inter alia, that the primary relief sought by the Applicant was not cognizable under the Fundamental Rights Enforcement Procedure Rules and the court resolved the suit on this sole issue alone.

DECISION OF THE COURT

The court dismissed the action after making a preliminary finding that the applicant's major reliefs are not enforceable under an action for the enforcement of fundamental rights.

On the nature of Fundamental Rights Enforcement Procedure Actions

“The Fundamental Rights Enforcement Rules may be activated by any person who alleges that any of the Fundamental Rights provided for in the constitution or African Charter of Human and Peoples Rights (Ratification and Enforcement) Act and to which he is entitled, has been, is being, or is likely to be infringed, such a person may apply to the court in the state where the infringement occurs or is likely to occur; for redress. In effect, by section 46(1) of the 1999 constitution, a person whose fundamental right is breached, is being breached or about to be breached may apply to a High Court in that state for redress.”

On nature of Principal relief in a claim for the enforcement of fundamental rights

“It is settled in a plethora of cases that when an application is brought under the Fundamental Rights (Enforcement Procedure) Rules, a condition precedent to the exercise of the jurisdiction of the court is that the enforcement of fundamental rights or the securing of the enforcement of same must be the main claim as well as the ancillary claim. Where the main claim or principal claim is not the enforcement or securing the enforcement of fundamental right, the jurisdiction of the court cannot be properly exercised, and the action will be incompetent.”

On whether action for the interpretation of the Nigeria Data Protection Regulation qualifies as a fundamental rights enforcement action

“I have closely examined the two reliefs being claimed and I cannot agree more with the respondent's counsel that the principal relief is not for the enforcement of the fundamental right, rather, as exemplified and amplified by the two questions posed by the applicant for determination, it is about the interpretation and construction of article 1.1(a) and 4.8 of the Nigeria Data Protection Regulation (NDPR) 2019 and the locus of the applicant to enforce the supposed right to privacy of an individual. Therefore, the claim is not cognizable under the Fundamental Rights (Enforcement Procedure) Rule 2009 and the court has no jurisdiction to entertain it.”

OBSERVATION

This judgment was delivered in January 2021, 6 years after the Court of Appeal conclusively affirmed the status of the right to privacy as a fundamental right in *Nwali v EBSIEC & Ors.* (2014). The court, with greatest respect, did not direct its mind to the earlier jurisprudence of the Court of Appeal, or properly appreciate the succinct issues submitted for determination. At any rate, the ratio of the court herein does not represent the correct position of the law on the status of the NDPR as an instrument that enforces the right to privacy as a fundamental right.

Incorporated Trustees of Digital Rights Lawyers Initiative v. Unity Bank Plc

SUMMARY OF FACTS

DRLI instituted this action for the benefit of job Applicants whose personal data were exposed by Unity Bank on their job portal in 2020 claiming a number of reliefs for the alleged data breach pursuant to relevant provisions of the NDPR. The Respondent filed an objection to the suit on the ground of lack of locus standi and failure to fulfil necessary condition precedent for initiating the suit under the NDPR. The court consequently dismissed the suit on the preliminary objection.

DECISION OF THE COURT

On whether a suit brought pursuant to the NDPR can be filed under fundamental rights enforcement procedure

“It is clear therefore that applicant/respondent must allege that any of his rights contained in chapter four was/ were contravened or infringed upon, is being infringed or is likely to be contravened. Therefore, before any action can be brought under the Fundamental Rights Enforcement Rules, 2009, they must primarily be reliefs that alleged breached of a fundamental right.” (page 17). “Without delving into the merit of the substantive suit of whether section 37 of the 1999 Constitution can apply, assuming without saying that it can apply, all these facts simply show that the enforcement of human right is not the principal relief but ancillary relief in this instant application.” (page 19). “I have carefully perused the facts of this case and the reliefs sought in respect thereof. It is clear to me that the principal or main claim of the applicant relates to the purported exposure of personal data of 53,000 by the respondent in line with the Nigeria Data Protection Regulation 2019. I hereby hold that this instant application is not proper to be brought under Fundamental Rights action.” (pages 20 and 21).

On DRLI's locus standi to institute the action on behalf of the 53,000 data subjects: "However, my concern is that the applicant has not shown sufficient interest to show that he is not just a meddlesome interloper. If and truly, 53,000 personal data of persons were breached, how come none of the said data subject is before the court? assuming but not saying that the instant action is breach of fundamental rights of such huge number of persons as in this case, how come there is no complaint or evidence of the existence of such persons before the court. Moreso, does the act of the purported exposure of data comes within the purview of public interest litigation as envisaged by section 46(1) of the 1999 Constitution and the Fundamental Right Enforcement Procedure Rules? From the facts and the evidence before the court, I do not think so. It is also notable that the applicant is basing this instant application on section 37 of the 1999 constitution as well as several provisions of the Nigeria Data Protection Regulation 2019. However, it should be said that fundamental right actions are sui generis and in a class on its own." (page 23).

On whether the Administrative Redress Tribunal is a condition precedent to the filing of cases under the NDPR "Regulation 4.2 of the NDPR provides thus–

"(1) Without prejudice to the right of a Data Subject to seek redress in a court of competent jurisdiction, the Agency shall set up an Administrative Redress Panel under the following terms of reference;

(2) Investigation of allegations of any breach of the provisions of this Regulation;

(3) Invitation of any party to respond to allegations made against it within seven days;

(4) Issuance of Administrative orders to protect the subject–matter of the allegation pending the outcome of investigation;

(5) Conclusion of investigation and determination of appropriate redress within twenty–eight (28) working days; and

(6) Any breach of this Regulation shall be construed as a breach of the provisions of the National Information Technology Development Agency (NITDA) Act of 2007." (page 24)

"The provision of the above Nigeria Data Protection Regulation 2019 is clear as to how to proceed against a breach, it is not a mere irregularity that can be dispensed with. The arguments of the applicant as to statute of limitation are misconceived and irrelevant. Since the applicant/respondent has failed to comply with the provision of section 4.1(8) of the NDPR, this court is divested of jurisdiction to adjudge this matter. I so hold." (page 25).

OBSERVATION

In this case, the court's decision on the relationship of the right to privacy and data protection is quite conflicting. In Incorporated Trustees of Digital Rights Lawyers

Initiative v. L.T. Solutions & Multimedia Limited, the Ogun State High Court coram Ogunfowora, J., had held that the right to privacy under section 37 of the CFRN includes data protection under the NDPR. The decision of the court on the lack of locus standi on the part of the Applicant is rather curious, especially so because the court recognized and reproduced the provision of section 3(e) of the preamble to the FREP 27 [2021] LPELR–55623(CA). Rules which encourage courts to welcome public interest litigations and not to dismiss or strike out public interest actions on the ground of lack of locus standi. The said paragraph 3(e) of the preamble to the FREP Rules provides for classes of applicants in human rights litigation which are (i) anyone acting in his own interest, (ii) anyone acting on behalf of another person, (iii) anyone acting as a member of, or in the interest of a group or class of persons, (iv) anyone acting in the public interest, and (v) association acting in the interest of its members or other individuals or groups.

The court on one hand, held that “From the foregoing it is obvious that the applicant can have the locus standi to bring this action under (iv) and (v) but on the other hand, the same court surprisingly concluded that: “... the applicant has not shown sufficient interest to show that he is not just a meddlesome interloper.”

More astonishing are the reasons the court relied on. First, that none of the 53,000 data subjects whose rights were violated was before the court, and second, that the act of purported exposure of data did not come within the purview of public interest litigation envisaged in section 46(1) of the CFRN. Contrariwise, in Centre for Oil Pollution Watch v. NNPC29 the Supreme Court recognized that:

“One of the features of this type of litigation is that the victims are often groups of persons who would not ordinarily be in a position to approach the court on their own due to impecuniosity or lack of awareness of their rights.”

It is therefore surprising that the court expected that some of the 53,000 persons, whose rights were allegedly infringed, ought to be before the court. The court’s second reason that data privacy breach litigation does not fall under an action in section 46(1) of the CFRN to bring it within public interest litigation under the FREP has been addressed and overtaken by the Court of Appeal’s decision in Incorporated Trustees of Digital Rights Lawyers Initiative & Ors v National Identity Management Commission (supra) wherein the court clarified the NDPR vis a vis right to privacy.

On condition precedent to enforcing a right under the NDPR in court, I am of the respectful view that, the court was wrong in concluding that the Applicant ought to have reported the alleged breach to the Administrative Redress Panel before instituting the action. The court’s decision is not supported by the express wording of regulation 4.2 (1)

of the NDPR which provides that: “Without prejudice to the right of data subject to seek redress in a court of competence jurisdiction, the agency shall set up an Administrative Redress Panel under the following terms of reference...”

The court was wrong in holding that this provision constitutes a condition precedent for instituting an action to enforce any of the rights under the NDPR, for at least three reasons. First, the regulation employs the phrase “without prejudice and in *Acmel (Nig.) Ltd v. F.B.N. Plc*³⁰, the Court of Appeal held that the words “without prejudice” means without loss of any right, in a way that does not harm or cancel the legal rights or privileges of a party. This shows that, the provision of article 4.2 of the NDPR is not intended to cancel out the right of a party to seek redress before a court until any mechanism is exhausted.

Second, the provision indeed does not provide for a data subject to report any alleged breach to the Administrative Redress Panel, the provision simply empowers the National Information Technology Development Agency (“NITDA”) to set up an Administrative Redress Panel and provides for what the roles of the Administrative Redress Panel would be. It is therefore amazing how the court interpreted a section which empowers the NITDA to establish an Administrative Redress Panel, as a condition precedent for enforcing any right under the NDPR. The provision does not say anything a data subject is to do before instituting an action to enforce his rights under the NDPR.

Third, the position of the law is that for a statute to place a condition precedent to the right of access to court as enshrined in section 6(6) (b) of the CFRN, the statute must be constitutional, legal, and express. In *Unilorin & Anor v. Oluwadare*³¹ the Court of Appeal held that:

“Finally on this point, we must remember that section 6(6)(b) of the Constitution of the Federal Republic of Nigeria, 1999, guarantees uninhibited right to every person to go to court seeking a determination of any question as to his civil rights and/or obligations. It is my view that for any condition precedent to the exercise of that constitutional right to be effective it must be constitutionally, legally, and expressly provided.” From the foregoing, I am of the respectful view that article 4.2 of the NDPR was not intended to be a condition precedent to the enforcement of any right under the NDPR. Conversely, if it was so intended, then it fails the test of expressivity set out in the decision in *Unilorin & Anor v. Oluwadare* (supra).

INCORPORATED TRUSTEES OF LAWS AND RIGHTS AWARENESS INITIATIVE V. NATIONAL IDENTITY MANAGEMENT COMMISSION

SUMMARY OF FACTS

In 2020, the National Identity Management Commission rolled out digital identity cards on Google store and an official of the Federal Government of Nigeria went on social media advising people to download their national identity cards (digital IDs) on the software application. Within 24 hours of the announcement, many Nigerians complained about the porous security features of the digital IDs and data breaches that led to some people being given other citizens' information on their digital IDs. DRLI consequently approached the court principally seeking "A declaration that the Respondent's processing of the digital identity cards via their software application (NIMC app) is likely to interfere with Daniel John's right of privacy as guaranteed under article 1.1(a) of the NDPR 2019 and Section 37 of the Constitution" among other reliefs.

DECISION OF THE COURT

On whether an action can, be brought on behalf of a data subject for breach of the NDPR "Having read and digested the above provisions, I am of the opinion that the Applicant cannot choose and pick which statute is favourable to him while neglecting salient part of the statute. By regulation 4.2(6): Any breach of this Regulation shall be construed as a breach of the provisions of the National Information Technology Development Agency (NITDA) Act of 2007. This provision takes it out of the purview of fundamental right action, therefore only a data subject can legally sue for breach of his data and that can only be done under the Nigeria Data Protection Regulation/NITDA Act, 2007" (see page 16)

OBSERVATION

With respect to the court, this decision represents another unfortunate step to defeat a valid complaint made to the Court. While it is conceded that the Court's decision is based on a number of binding judicial decisions (which are not necessarily apt), it is submitted that the jurisprudence in fundamental rights actions ought to depart from situations where such applications are defeated on technical grounds, such as locus standi (with or without the presence of the complainant whose right has been infringed) to ensuring that decisions in fundamental right matters meet the substantial justice of the case. The latter is the intendment of the FREP Rules 2009. As such, a community reading of the overriding objectives of the Rules contained in paragraph 3 (a) of the preamble will show that the intention is to advance and realise but not to restrict the rights contained in Chapter IV of the Constitution of the Federal Republic of Nigeria, the provisions of the African Charter on Human and People's Rights and other municipal, regional and international bills of rights. The above view is supported by the dictum of Nweze, JSC in *Kalu v. STATE* [2017] 14 NWLR (Pt. 1586) 522, 544–545 where his Lordship stated that issues around fundamental rights should not be subjected to the austerity of tabulated

legalism. In fundamental rights cases, it is enough that an applicant's complaint is understood and deserves to be entertained. Thus, the way the court is approached (including the couching reliefs) ought not to defeat such matters. See Federal Republic of Nigeria v. Ifegwu [2003] 15 NWLR (Pt. 842) 113, per Uwaifo, JSC (as he then was). Conclusively, one would have expected that even if the Court was of the view that a breach of NDPR is only actionable as a breach of the NITDA Act of 2007, the Respondent's action would have been examined in the light of section 37 of the Constitution, since the Applicant brought the suit under both the NDPR and the Constitution. Suit No. IKD/3191GCM/2019. Judgment delivered by the High Court of Lagos State, Ikorodu Division Per Hon. Justice I. O. Akinkugbe on the 24th of October 2021.

HILLARY OGOM NWADEI V GOOGLE LIMITED LIABILITY COMPANY & ANOR

SUMMARY OF FACTS

The Applicant, a Priest and Lawyer was charged to the Lancashire Court of England for assault in 2015 and thereafter convicted and sentenced to 8 months jail term which ended that same 2015. During and after Mr. Nwadei's trial, conviction and jail term, many bloggers and news outlets reported the news, and those reports were frequently accessed on Google search engine. The availability of these news on Google's platform prevented Mr. Nwadei from gaining employment after he left his last job in the United Kingdom. The Applicant consequently instituted an action at the High Court of Lagos State claiming, inter alia, that having completed his 8 months jail term in England, he was therefore entitled to the unfettered enjoyment of his constitutional rights to privacy and the dignity of his human person. He also alleged that the Respondents have threatened his rights to privacy and the dignity of his human person by making the information of his arrest, subsequent trial and conviction available to the whole world on social media four years after the completion of his sentence, and also injunctive orders to restrain the Respondents from further making available on their platforms the information relating to his arrest and conviction. In other words, Mr Nwadei sought to enforce his data protection right to be forgotten. The 1st Respondent challenged the Applicant's action, by a counter-affidavit and written address, wherein they responded that they (Google) did not publish any information about the Applicant and had no control over any information posted about the Applicant and could therefore not edit any information posted by third parties. The 1st Respondent further contended that the information about the Applicant's arrest and conviction already formed part of the public record in England and the Applicant could therefore not expect to have a right of privacy in respect of such information and that any publication of same does not violate his rights to human dignity.

DECISION OF THE COURT

The Court found that the Applicant had placed insufficient evidence before it to support his claims, and therefore dismissed the application. On the need for Applicant to adduce sufficient evidence to prove claim: “It is not sufficient evidence I hold, for the applicant to just state that his rights have been violated, there must be cogent evidence placed before the court to support the reliefs being sought. The evidence being relied upon to support the facts in the supporting affidavit are clearly Exhibits A, B, and C, especially Exhibit A, the alleged offending article circulating on the internet allegedly made available to the world at large by the 1st respondents search Engine, has to be placed before the court to enable the court to reach a just determination. This was not done.”

On importance of Further Affidavit in proving claims

“The applicant by not refuting the 1st respondent’s facts stated in the counter affidavit that they were not responsible for the information posted about his arrest and arraignment by a further affidavit, being a search engine has not shown how the 1st respondent has wronged him I hold by violating the fundamental rights allegedly violated. It is the law that a person cannot sue someone who has done him no wrong. SEE *REBOLD INDUSTRIES LIMITED V MAGREOLA & ORS* (2015) LPELR–24612 (SC) and it is settled law that facts not denied are deemed admitted.”

OBSERVATION

This case presented a very rare opportunity for the Court to examine the data protection “right to be forgotten”, but the failure of the Applicant’s counsel to diligently place proper evidence before the court and to respond to the counter depositions of the respondent robbed the court of the opportunity to explore the concept at all. Curiously, in spite of the fact that the suit was filed in 2019, none of the reliefs claimed referenced the Nigeria Data Protection Regulation (NDPR) under which the right to be forgotten can be conveniently invoked. Although the second relief references ‘right to private life’, the Applicant did not satisfactorily relate it to right to be forgotten and that may explain the court’s disposition as well. Admittedly, Mr. Nwande’s reliefs, on the surface but impliedly speaks to the right to be forgotten, the originating processes did not explore the dynamics of the right in any material respect. Surprisingly, notwithstanding Google’s admission that it could well de-reference such damaging stories, the Applicant failed to address how his case could be accommodated under the broad categories of persons who can enforce the European– styled right to be forgotten as first introduced in the famous decision of *Google Spain v AEPD* case.

INCORPORATED TRUSTEES OF DIGITAL RIGHT LAWYERS INITIATIVE V NIGERIAN INTERBANK SETTLEMENT SYSTEM AND ORS (FHC/KD/CS/2020

In compliance with the Central Bank of Nigeria’s directive to deposit money banks and other financial institutions to establish modalities for providing access to customers’ Bank Verification Numbers, amongst other issues, the Nigerian Inter Bank Settlement System, the primary vehicle through which the directive was to be implemented, established a database for customers’ BVN and modalities for accessing same in violation of the Nigerian Data Protection Regulation 2019—the law that regulates privacy and data protection issues in Nigeria. When the failure was discovered, the Digital Right Lawyers Initiative—a foremost Digital Rights advocacy group in Nigeria, instituted an action at the Federal High Court on behalf of its members and the public who were likely to be affected by the failure to comply with the law. In a judgment delivered on the 10th of December 2021, the Federal High Court dismissed the suit for want of jurisdiction. This review assesses the reasoning behind the court’s decision and provides an analysis on why a different path ought to have been taken by the court.

SUMMARY OF FACTS

The Incorporated Trustees of the Digital Right Lawyers Initiative instituted an action to protect the rights of its members from the anticipated breach of the right of its members to privacy and exposure of Nigerians’ data to unwanted access as a result of the Respondents’ failure to comply with Data Protection laws. In response, the Respondents challenged the jurisdiction of the Applicants to maintain the action. They contended among other issues that the Applicant lacked the locus to maintain the suit and does not have the authority to sue, the suit did not disclose a reasonable cause of action and the Applicant failed to comply with condition precedent by not filing a pre-action notice. The Applicant in response, contended that actions to enforce the fundamental rights of individuals or groups do not require the establishment of locus standi and compliance with pre-action protocols. They also contended that their locus to institute the action is inherent in the fact that the suit was a public interest litigation where locus is not required to be established. The Applicant also contended that since it maintains a nation-wide membership, it did not matter that the suit was not instituted where its registered office is located and more so, the breach could occur in any part of the country.

DECISION OF THE COURT

In determining the objection raised against the competence of the suit, the court, after defining what amounts to locus, held thus “... a closer perusal at (sic) the oral submission of the 2nd Respondent counsel, it was submitted that the applicant is only in court or(sic) a voyage of discovery as the said regulation which the applicant relied on vehemently has

not come into effect and there is nothing before the honourable court to challenge that fact. The applicant did not state the said regulation that the 1st and 2nd Respondents have violated nor did he attach same... it is pertinent to state that the Preliminary objection of the Respondents success (sic) as the applicant has no locus standi within which to stand and institute the action.” With the above pronouncement, the court dismissed the suit.

OBSERVATION

In taking the above decision, the court applied the law wrongly to the case before it. First, as clearly demonstrated in the Applicants’ case, the suit was instituted to prevent an anticipated breach of the rights of Nigerians to data privacy. There need not have been an actual violation of the rights of members of the NGO or Nigerians before the right to institute an action for redress accrues. The law is trite and embedded in the grundnorm that a person who anticipates the violation of his constitutionally guaranteed right can institute an action to protect same.

Again, the court seemed to have confused Cause of Action with Locus: two terms with different meanings under the law. While the former indicates that a person must have a set of facts or circumstances that give the right to sue namely: the existence of a legal right and the violation or expected violation of same, the latter means that one must have the right or “standing” in law to sue. The court, in the case under review seemed to have held that the applicants did not disclose the existence of a legal right which would be wrong in the circumstance for as explicated above, an applicant seeking the enforcement of his fundamental right does not need to wait till the right is violated. In the extant case, the Applicants had demonstrated that the Respondents were involved in the making of a regulation that exposed the data of Nigerians to violation. The Applicant as a public interest litigation did not need to demonstrate any particular interest in the matter before taking action. The court also hinged its decision on the ground that the Nigerian Data Protection Regulation, 2019 which the Applicant complained, was violated was not attached to the Affidavit in support of the Application. In its view, the failure to so do indicated that the Applicant did not show how a violation of the law had occurred. This is in my view a rather befuddling position to take. The law is crystalized in a galaxy of decisions that statutes are not meant to be attached as Exhibits or tendered in court for the court is said to take judicial notice of statutory texts. By the clear wording of section 122 (2) of the Evidence Act, the court is expected to take judicial notice of ‘all laws or enactment and any subsidiary legislation made under them having the force of law...’ It follows that the refusal to attach the regulation ought not to have been a ground to decline jurisdiction as the court has done.

P.P.&P. (Nig.) Ltd.v.Olaghere [2019]2NWLRpg541
NigerianWeeklyLawReports11February2019 CA/L/1046/2011

SUMMARY OF FACTS

The appellants used the photograph of the 1st respondent's personal house as the front cover and inside page of the appellants' 2002 calendar. After getting constructive notice of the publication, the 1st respondent, through his solicitor, wrote a letter of complaint to the appellants. He demanded for withdrawal of the calendars from circulation and for monetary compensation. But the appellants did not respond to the letter.

Consequently, the 1st respondent sued the appellants jointly and severally. He asserted that that the appellants published the pictures of his house without his express or implied permission. He sought the withdrawal of the calendar from circulation. Alternatively, he sought an order directing the appellants to write a letter of apology to him as approved by his solicitor, and to publish the apology in a widely circulated daily newspaper. He also sought an award of N100million (One hundred million Naira) as aggravated and exemplary damages.

In their defence, the appellants pleaded that they engaged the services of an independent contractor to source for the photograph of a property; that the contractor undertook to indemnify them for any encumbrance that might occur afterwards; and that the contractor sourced for the photograph they published. The appellant raised the issue of non-joinder of the independent contractor by the 1st respondent and asserted that was fatal to the 1st respondent's case. However, on the application of the appellants, the *alter ego* of the contractor was joined as a 3rd party in the suit.

The trial court after hearing the case of parties, found in favour of the 1st respondent and awarded a sum of N50million (Fifty million Naira) against the appellants though there was no evidence of actual loss by the 1st respondent or direct gain by the appellants from the publication of the calendar. It also ordered the appellants to publish an apology to the 1st respondent in a widely read daily newspaper.

Dissatisfied with the decision of the trial court, the appellants appealed to the Court of Appeal.

DECISION OF THE COURT

Held (*Unanimously allowing the appeal in part*):

On Whether wrongful to use the photograph of a person's house on a calendar without prior consent of the person -It is wrongful and a breach of the privacy of

an individual to use the photograph of his house on a calendar without his prior consent or authorization. In this case, the appellants breached the privacy of the 1st respondent when they used the photograph of his house on their products calendar without his consent. (P. 568, F-H)

Anozia v. Nnani [2015] 8 NWLR 241 CA/OW/29/2013

SUMMARY OF FACTS

The appellant filed an application at the trial court and sought for an order setting his suit down for hearing and order of court referring the parties for a DNA test. He also sought for an order for arrest of the respondents for failing to react to his suit. In the main suit filed by the appellant, he sought mainly for declaration of the paternity of the 2nd respondent and an order directing the 2nd respondent to change his surname. The respondents denied the claims of the appellant.

After hearing the application of the appellant, the trial court refused to order the 1st respondent to submit to a DNA test. The appellant being aggrieved with the interlocutory decision of the trial court filed a notice of appeal at the Court of Appeal. The respondents filed a notice of preliminary objection and contended that some of the grounds of appeal did not arise from the decision of the trial court.

DECISION OF THE COURT

On whether an adult can be compelled to submit to DNA test –

A court cannot order an unwilling adult or senior citizen to submit to DNA test, in defiance of his fundamental rights to privacy for the purpose of extracting scientific evidence to assist the appellant in the instant case to confirm or disprove his wish that the 2nd respondent - a 57 year old man is his child, of an illicit amorous relationship. (P. 254, paras. F-G)

CASES ON FREEDOM OF EXPRESSION INCORPORATED TRUSTEES OF DIGITAL RIGHTS LAWYERS INITIATIVE V. NATIONAL COMMUNICATIONS COMMISSION

SUMMARY OF FACTS

In 2019, the National Communications Commission (NCC) introduced a (draft) Internet Industry Code of Practice which empowers the NCC to unilaterally issue a takedown

order to Internet Service Providers (ISP) to shutdown certain websites without recourse to court order. DRLI consequently challenged the document in court seeking the following reliefs:

1. A declaration that by section 7.3 of the Respondent's establishment of Internet Industry Code of Practice on take down notice (the "Draft Code") is likely to violate the Applicant's fundamental right to expression and the press guaranteed under Section 39 of the Constitution of the Federal Republic of Nigeria, 1999 (as amended) (the "Constitution").
2. A declaration that the Respondent's plans to unilaterally issue takedown notice to any Internet Access Service providers (IASP) without Court orders is likely to violate the Applicant's fundamental rights to expression and the press guaranteed under Section 39 of the Constitution of the Federal Republic of Nigeria, 1999 (as amended) (the "Constitution").
3. Perpetual injunction restraining the Respondent, its officers and/ or representatives from issuing takedown notices to Internet Services Providers (ISPS) without a Court order.

In response, the NCC filed a Notice of Preliminary Objection challenging the jurisdiction of the Court on the grounds of lack of locus standi, non-disclosure of cause of action, irregular procedure, the main relief sought is not cognizable under fundamental rights enforcement procedure and non-fulfilment of condition precedent.

DECISION OF THE COURT

Although the Court agreed that DRLI possessed the requisite locus standi to commence this suit, the court however dismissed the suit for being speculative, frivolous and an abuse of court process as the Applicant is challenging a draft Code which has neither been gazetted nor passed into law, as such, has no force of law at the time of filing the suit.

OBSEVATION

Although the court struck out the suit, the holding that the Applicant has the locus standi to bring this action is in line with existing judicial authorities and is therefore commendable. However, the decision of the Court declining jurisdiction on the ground that the document is a draft Code, which had not come into force at the time as same has neither been gazetted nor passed into law, is with respect to the court, an interesting and curious one. In arriving at that conclusion, the Court failed to consider the provision of section 46(1) of the Constitution that: "Any person who alleges that any of the provisions of this Chapter has been, is being or likely to be contravened in any State in relation to him may apply to a High Court in that State for redress." (Emphasis supplied) A similar provision is contained in Order 2 Rule 1 of the FREP Rules and has been restated in a plethora of judicial decisions. With respect to the court, the position of our laws is that,

where anticipates that his fundamental right may be interfered with, the person can approach the court for redress and the court can come to the person's aid and make the necessary orders. Had the court considered this position of law, it would have arrived at a different decision. Moreover, a legislative instrument may still have the force of law even where same has not been gazetted and regulatory agencies can issue codes by way of subsidiary legislations and the codes will be binding and enforceable within the relevant industry without being formally enacted by the National Assembly. This position is supported by the decision of the Court of Appeal in the case of Deaconess Felicia Ogundipe v. The Minister of Federal Capital Territory (2014) LPELR–22771 (CA). Given the foregoing, the decision of the court in this case that the draft Code has neither been gazetted or enacted into law, and as such cannot be a ground for a fundamental rights action, with respect to the court, falls short of established legal principles and creates a bad precedent for fundamental right actions.

Diana Ele Uloko v. Inspector General of Police

SUMMARY OF FACTS

On the 11th day of October 2020, the Applicant, Diana Uloko, joined thousands of other Nigerian youths to exercise their fundamental rights to freedom of expression and association by participating in the “End SARS” protest in Abuja. The protests were held nationwide in expression of citizens’ grievances against the numerous atrocities committed by the Nigerian Police Force against young Nigerians in the country. During the protest, the Applicant made use of her Samsung mobile phone to record the protest and post pictures of same on social media to report the events. Whilst this was on-going, some officers of the Nigerian Police Force disrupted the protest and ambushed many protesters. In the process, while the Applicant’s sister was apprehended and manhandled by the Police, the Applicant took out her phone to broadcast the harassment of her sister on social media, but the phone was seized by a Police Officer who destroyed her phone by smashing it with a stick. The Applicant was also injured during this incident. Aggrieved by the actions of the policemen, the Applicant filed an action against the Police claiming an infringement of her right to freedom of expression.

DECISION OF THE COURT

In resolving the dispute submitted to it for determination, the court acknowledged that the primary claim before it was for a declaratory order, and held, in line with the established jurisprudence of the Supreme Court, that it must be established on the strength of the Applicant’s case and not on the weakness of the Respondent’s case. The Court further observed that this suit was properly commenced via originating summons – which is best suited for cases where there is no likelihood of controversial facts. The Court however found that the Applicant failed to furnish ample evidence to establish her claim to the

declaratory relief sought in the first prayer. On the need to lead abundant and credible evidence in support of a claim for the enforcement of the constitutionally guaranteed fundamental right to freedom of expression: “For the abundance of caution, it is always good to place enough evidence for the court to evaluate even when it amounts to surplusage of proof...” On the need to link the evidence before the Court to the pleadings of parties: “Moving on, it would seem that the same challenges are shared with the images of the bruises. The applicant pleaded the picture to show the bruises and injury she allegedly sustained following assault by the Respondent’s officers. However, by itself, the image does nothing to prove what it was supposed to. There is no indication as to when that image was taken.” In the final analysis, the Court held that “the applicant must satisfy the court by cogent, credible and convincing evidence that she is entitled to the declaratory relief as sought. So, as the applicant by her own evidence has failed to prove her claim for declaration, her claim must fail.” (page 11). The Court consequently struck out the case.

OBSERVATION

This case was a golden opportunity for the court to recognize the importance of mobile phones and social media as a mode of exercising the fundamental right to freedom of expression. The Applicant’s mobile phone is her medium of expression, and depriving her access to her mobile phone is effectively depriving her access to the enjoyment of her constitutionally guaranteed rights to express herself and communicate freely with other persons. Sadly, the court chose to view this case restrictively from the lenses of a standard complaint against police harassment and intimidation. The court dismissed the claims on the grounds of insufficiency of evidence to link the Respondents to the Applicant’s claims in spite of the Respondent’s refusal to contradict the affidavit evidence before the court. The court, sadly, did not get around considering the constitutional implications of the case.

Incorporated Trustees of Digital Right Lawyers Initiative (DRLI) v. Commissioner of Police, Delta State

SUMMARY OF FACTS

DRLI filed this fundamental rights enforcement suit on behalf of one Prince Nicholas Makolomi—a journalist who was arrested by officers of the Special Anti–Robbery Squad Operatives (SARS) of the Nigerian Police Force and transported from Ughelli to State CID Asaba for allegedly making a video recording of the SARS operatives leaving an injured citizen on the ground and fleeing with his car. It is of note that, it was this video footage that sparked the nationwide EndSARS protest of 2020. When Prince Makolomi was arrested and detained indefinitely by SARS operatives for exercising his freedom of expression by posting the video footage online, DRLI filed an action to enforce his right

to personal liberty since the Respondent refused to release him or charge him before a competent court.

DECISION OF THE COURT

On the illegality of the arrest and detention of Prince Makolomi:

The court considered the affidavit in support of the originating motion filed by the Applicant and the counter-affidavit filed by the Police and found that:

“... I am of the view that the subject of the application, Prince Nicholas Makolomi, was indeed arrested and detained for a period of at least 3 days before he was charged to court. I do not believe in the reliability of the counter affidavit of the Respondent. Looking at the tenor of the counter affidavit of the Respondent, it did not deny the fact that Prince Makolomi was arrested on the 5th day of October 2020. It merely stated that he was transferred to the State CID Asaba for discreet investigation on the 8th of October 2020 without stating the date when he was initially arrested, or refuting the claim in the supporting affidavit that the arrest occurred on the 5th of October, 2020... Even if I agree with the Respondent that the Applicant was arrested and transferred to Asaba on the 8th day of October and that he was charged to court on the same day that is still a period of 3 days meaning that the detention exceeded the period allowed by law.” (pages 9 & 10).

On the violation of Prince Makolomi’s right to personal liberty:

“All the materials before me considered, I believe that the subject, Prince Nicholas Makolomi’s right to personal liberty was indeed violated by the Respondent having not charged the subject to court within a period of 1 day as provided by section 35 of the Constitution since there is no contest that a court of competent jurisdiction exists within Ughelli from where the subject was initially apprehended, nor was he released in the context of an administrative bail when it was clear the Respondent was not going to be able to charge the subject to court.” (pages 10 & 11). On the law enforcement powers of the Police: “I agree that the Respondent in the exercise of their law enforcement powers can arrest and detain a suspect, but the suspect must be brought before a court of competent jurisdiction within one day where there is such a court within a radius of forty kilometres, and in any other case, within a period of two days or such longer period as in the circumstances may be considered by the court to be reasonable. As I held in Suit No FHC/ABJ/CS/1051/2015, MR. SUNDAY OGABA OBANDE & ANOR V. MR. FATAI & 3 ORS, delivered on 26/01/2016, the requirement to release arrested suspects or charge them before a competent court promptly as required under section 35(4) & (5) of the Constitution, in my view, is only a logical expression of the presumption of innocence which [ensures] to their benefit and guaranteed by section 36(5) of the Constitution.” (page 11).

On reason for constitutional requirement to charge a suspect to court within a limited time:

“Additionally, the courts are the umpires and are far removed from the facts of a case. It will be unfair to expect the law enforcement agencies which apprehended a suspect and are quite biased regarding the circumstances of the apprehension, to be the very ones who will determine the entitlement or otherwise of the Applicant to his liberty. And that is why the Constitution requires that the person must not be detained for more than a day without being charged to court where a court exists within 40 kilometres radius or a period of not more than 48 hours where none exists within a radius of 40 kilometres.” (page 12).

On the whole, the court resolved the lone issue in favour of the Applicant, declared the arrest and detention of Prince Makolomi an interference with his fundamental right to personal liberty, and awarded N200,000 as general damages against the Respondent.

OBSERVATION

This decision joins a long line of decisions for progressive protection of the fundamental rights of Nigerian citizens especially the freedom of expression online which right Prince Makolomi exercised when he posted the video footage on the Internet. Notably, the action was commenced by a right group on behalf of Prince Makolomi. This is possible and allowed in line with the innovation introduced by the Fundamental Rights (Enforcement Procedure) Rules, 2009 (“FREP Rules 2009”) which allows for human right activists, advocates, or groups as well as any non-governmental organization to institute human rights action on behalf of any potential applicant. This would not have been possible under the Fundamental Rights (Enforcement Procedure) Rules, 1979 which the 2009 Rules replaced. The journalist was harassed by the security operatives for his dissemination of information to the citizens via social media and the Internet, hence, the judgment is a welcomed addition to the growing list of authorities on the enforcement of digital rights in Nigeria.

Incorporated Trustees of Media Rights Agenda v. National Broadcasting Commission

SUMMARY OF FACTS

During the EndSARS Protest in 2020, some television stations reported the events as they unfolded nationwide. When the Federal Government, through the National Broadcasting Commission fined the stations under the Nigeria Broadcasting Code for airing the protests, Media Rights Agenda—a civil society devoted to press freedom and sundry matters—approached the Federal High Court challenging the fine as arbitrary and an interference with freedom of expression and the press guaranteed by section 39 of the Constitution of the Federal Republic of Nigeria 1999 (as amended) (“CFRN”) and Article 9 of the African Charter on Human and Peoples Rights (Ratification and Enforcement) Act (“ACHPRA”) etc.

DECISION OF THE COURT

On locus standi in an action for enforcement of fundamental rights:

“Locus standi as it borders on actions commenced under Fundamental Rights (Enforcement Procedure) Rules 2009, is no longer an issue sufficient to bar the institution of fundamental rights cases. This principle was broadened by the Supreme Court in *Fawehinmi v. Akilu* (1987) 4 NWLR (Pt. 67) 797, wherein the Court held that: “It is the universal concept that all human beings are brother assets to one another”. Per Eso, J.S.C. (as he then was) (page 10).

The Court referenced paragraph 3(e) of the preamble to the Fundamental Rights (Enforcement Procedure) Rules 2009 which enjoins courts to encourage public interest litigation, and not to strike out any human right case for lack of locus standi. The section also provides for categories of people that can bring an action on behalf of an applicant to enforce his fundamental rights, including any person acting in the public interest.

Finally on locus standi, the court held that:

“Without dissipating much energy, I hold that the Applicant/Respondent have the locus standi to institute this suit against the Respondent/Applicant. Therefore, this Court have the necessary jurisdiction to determine this suit”.

On fulfilling condition precedent: filing of verifying affidavit in fundamental rights cases: “This observation was also held by the Court in the case of *Groner & Anor v. EFCC* (2014) LPELR–24466(CA), as follows: “In my view, what is important in the Rules is that the affidavit in support of the application be made by the applicant except he is in custody or unable to. The issue here is why the 2nd Applicant (appellant) failed to personally swear to the affidavit. It is immaterial whether it is an affidavit simplicita or a verifying affidavit.” I therefore discountenance learned counsel Respondent/ Applicant’s contention in this regard because, the records show that the Applicant/Respondent filed an eighteen paragraphs affidavit in support of his Originating process. That suffices in law.” (page 14).

On the competence of the suit

“After due consideration of the Originating process and its affidavit in support, I find the facts on which the reliefs are sought are speculative and do not yield for sound reasoning, how the fundamental rights of the Applicant have been encroached upon. The pith of the Appellant’s alleged breach of their fundamental rights is predicated on speculation. For emphasis paragraph 15 of the affidavit reads again– *Morisola* told me on phone on 29th October 2020 and I verily believe her that it must have been the sanction and fine imposed on Channels TV by the respondent alongside *ARISE TV* and *AIT* that made Channels TV not to broadcast the video she sent for *EYE WITNESS REPORT*. Conclusively, I adjudge that the case of the Applicant is purely academic, devoid of any reasonable cause of action, incompetent and if allowed to proceed to hearing, it will amount to an abuse and waste of court’s process.” (pages 16).

OBSERVATION

The decisions of the court on the issue of locus standi in fundamental rights enforcement actions and filing of verifying affidavit are commendable. They tow the progressive line, and in alignment with the provisions of the Fundamental Right (Enforcement Procedure) Rules 2009 and judicial authorities. However, the Court concluded that the action was purely academic, devoid of any reasonable cause of action and incompetent, or at least. This is so because the Court came to this conclusion without due consideration of the third limb of the basis for application for enforcement of fundamental rights. Section 46(1) of the CFRN provides three criteria for an applicant to enforce a fundamental right; (i) where a person alleges that any of the provisions of Chapter IV on fundamental rights has been contravened; (ii) where a person alleges that any of the provisions of Chapter IV is being contravened; and (iii) where a person alleges that any of the provisions of Chapter IV is likely to be contravened. The said section 46(1) of the CFRN provides that:

“Any person who alleges that any of the provisions of this Chapter has been, is being or likely to be contravened in any state in relation to him may apply to a High Court in that State for redress.” The decision of the Court of Appeal in *Mirchandi v. IGP & Ors*⁷ explains the three limbs of Section 46(1) of the Constitution. In our own case, paragraph 12 of the Applicant’s affidavit complies with the third limb of section 46 of the constitution which allows an applicant to institute a fundamental rights suit where there is a likelihood of infringement while paragraphs 13–15 are based on the first limb of the right haven been infringed. We are however Sceptical that the Court would have held differently even if the Court had considered the third limb of the basis. This is so because in *Mirchandi v. IGP & Ors* (supra), the Court adopted the reasoning in *Uzoukwu v. Ezeonu* (1991) 6 NWLR (Pt. 200) 708 at 784 where it was held that “Before a plaintiff or applicant invokes the third limb, he must be sure that there are enough acts on the part of the respondent aimed essentially and unequivocally towards the contravention of his rights. A mere speculative conduct on the part of the respondent without more, cannot ground an action under the third limb.” However, the Court should still have considered the claim of the Applicant based on the third limb, for whatever it was worth. That would have provided guidance for the citizens on the quantum of likelihood of injury that will sustain an application brought based on the third limb.

The Registered Trustees of the Socio–Economic Rights and Accountability Project (SERAP) v. Federal Republic of Nigeria

SUMMARY OF FACTS

On the 4th day of June 2021, the Federal Government of Nigeria announced the indefinite suspension of Twitter in Nigeria. Consequently, SERAP, a Non-Governmental Organization registered in the Federal Republic of Nigeria, filed a suit before the Community Court of Justice (ECOWAS Court) challenging the suspension as an infringement of Nigerian citizens' digital rights especially freedom of expression online. The Applicant also filed along with the substantive suit, an application for interim provisional measures seeking to restrain the federal government of Nigeria from intimidating or harassing citizens using the Twitter app in spite of the suspension of its activities in Nigeria.

DECISION OF THE COURT

On the effect of denial of access to Internet on the right to freedom of expression The Court agreed with the Applicant's Counsel that the cause of action of this matter borders on freedom of expression which is recognized by the African Charter on Human and People's Rights to which the Respondent/Applicant is a party when the court ruled that: "Access to the internet though not a right, in the strict sense, serves as a platform in which the rights to freedom of expression and freedom to receive information can be exercised, "therefore a denial of access to the internet or to services provided via the internet, as a derivate right, operates as denial of the right to freedom of expression and to receive information. This was adequately captured by the Court in its previous decision as follows:

"Twitter provides a platform for the exercise of the right to freedom of expression and freedom to receive information, which is fundamental human right and any interference with the access, will be viewed as an interference with the right to freedom of expression and information. By extension such interference will amount to a violation of a fundamental human right which falls within the competence of this Court pursuant to Article 9 (4) of the Supplementary Protocol (A/SP.I/ OI /05) amending the Protocol (A/PI/7/91) relating to the Community Court of Justice. Evidently, this situates the claim before the Court as one bordering on the Violation Of human rights which has occurred in a Member State. "Noting that the Respondent has also argued that its' action is against a particular entity, Twitter and not the Applicant, and that the subject matter of the suit is therefore not for the enforcement of human rights, the Court is inclined to reiterate its competence. Article 9(4) of the Supplementary Protocol (A/SP. 1/01 /05) Amending the Protocol (A.'P I,'7/91) relating to the Community Court of Justice provides "The Court has jurisdiction to determine cases of violation Of human rights that occur in any Member State. It is trite that a mere allegation of a violation of human rights in the territory Of a Member State is sufficient, prima facie, to justify the Court's jurisdiction" (p.11)

OBSERVATION

This decision is a landmark development to the human right jurisprudence in Africa. Most especially the decision of the court recognizing that denial of access to the Internet or to services provided via the internet, as a derivative right, operates as denial of the right to freedom of expression and to receive information. This decision is instructive to the extent that, since Twitter as a platform is used by the citizens to exercise their right to freedom of expression including freedom to receive information, which is a fundamental human right, any interference with such access constitutes an interference with the right to freedom of expression guaranteed by the Nigerian constitution.

Rachel Ochanya Uloko v. Inspector General of Police

SUMMARY OF FACTS

On the 11th October, 2020, the Applicant joined thousands of other Nigerian youths to exercise their fundamental rights to freedom of expression and association by participating in the “End SARS” Protest in Abuja, as a mode peacefully airing their grievances against the numerous atrocities committed by the Nigerian Police Force against young Nigerians over the country. During the protest, the Applicant made use of her Samsung Phone to take photographs and record the peaceful protest. Whilst this was on-going, some officers of the Nigerian Police Force (Respondent) disrupted the protest and ambushed the protesters. The Applicant was apprehended, harassed and assaulted by the Police. Aggrieved by the actions of the Policemen, the Applicant instituted this action against the Police vide an Originating Summons for the enforcement of her fundamental rights to freedom of expression and the press and claiming the sum of N10,000,000.00 (Ten Million Naira) in damages. The Applicant submitted two questions for determination by the Court viz:

a. Whether or not by the interpretation and construction of Section 39 and 46 of the Constitution of the Federal Republic of Nigeria 1999 (as amended) and Order 2 Rule 1 of the Fundamental Rights (Enforcement Procedure) Rules 2009, the Respondent’s officers harassment, intimidation, threatening and assault of the Applicant and further damage of the Applicant’s mobile phone during the End SARS Protest in Abuja interfered with the Applicant’s right to freedom of expression?

b. Whether or not the Applicant is entitled to damages sought?

The Respondent did not appear in Court or file any process despite service of numerous hearing notices on him.

DECISION OF THE COURT

In resolving the issue placed before it for determination, the court admitted that the primary claim before it was for a declaratory order, and held, in line with the established jurisprudence of the Supreme Court, that it must be established on the strength of the

Applicant's case and not the weakness of the Respondent's case. The Court further observed that this suit was properly commenced via originating summons—which is best suited for cases where there is no likelihood for dispute of facts. The Court however found that the Applicant failed to furnish ample evidence to establish her claim to the declaratory relief sought in the first prayer.

On the need to lead abundant and credible evidence in support of a claim for the enforcement of the constitutionally guaranteed fundamental right to freedom of expression:

“For the abundance of caution, it is always good to place enough evidence for the court to evaluate even when it amounts to surplusage of proof...”

On the need to link the evidence before the Court to the pleadings of parties:

“Moving on, it would seem that the same challenges are shared with the images of the bruises. The applicant pleaded the picture to show the bruises and injury she allegedly sustained following assault by the Respondent's officers. However, by itself, the image does nothing to prove what it was supposed to. There is no indication as to when that image was taken.”

In the final analysis, the Court held that “the applicant must satisfy the court by cogent, credible and convincing evidence that she is entitled to the declaratory relief as sought. So, as the applicant by her own evidence has failed to prove her claim for declaration, her claim must fail.” The Court consequently struck out the case.

OBSERVATION

This case was a golden opportunity for the courts to recognize the importance of mobile phones as a mode of exercising the fundamental right to freedom of expression. The Applicant's mobile phone was her medium of expression, and depriving her access to her mobile phone is effectively depriving her access to the enjoyment of her constitutionally guaranteed rights to express herself and communicate freely with other persons. Sadly, the court chose to view this case restrictively from the lenses of a standard complaint against police harassment and intimidation. The court dismissed the claims on the grounds of insufficiency of evidence to link the Respondent's to the Applicant's claims. It did not get around considering the constitutional implications of the case. One can only hope that a more meticulous applicant seeking to enforce similar rights would overcome the evidentiary hurdles highlighted by the court in this case.

Sun Publishing Ltd. V. Aladinma Medicare Ltd [2016]9NWLR557 CA/OW/218/2012

SUMMARY OF FACTS

In the issue of the “Daily Sun” of Friday, 1st June 2007 at page 10, a news item captioned “Corpse disappears from Owerri, reappears in Abia,” was published by the appellants, the publishing company and the author of the news story respectively. In the publication, the appellants wrote of and concerning the respondent’s hospital mortuary services. The appellants reported that a corpse meant for collection by its owners on a particular day got missing in the mortuary owned by the respondent and they made reference to the mortuary as being an establishment of “*Otokoto men*”.

As a result of the publication, the respondent instituted an action against the appellants claiming the sum of two hundred million Naira (N200,000,000.00) as exemplary or aggravated damages, injunction, unqualified apology and retraction of the publication which the respondent claimed to be libelous of it. The respondent pleaded that by the words used in the publication in their natural and ordinary meaning, the appellants meant and were understood to mean that the respondent ran a racket where corpses were sold for money-making rituals; that corpses deposited at the respondent’s mortuary were sold to ritualists for money-making rituals; and that the respondent’s mortuary was not a safe place to deposit corpses and should not be patronized by the public.

The appellants pleaded qualified privilege and further gave copious particulars in connection therewith. The respondent did not file a reply in answer to the appellants’ statement of defence and particularly to the appellants’ plea of qualified privilege and the particulars given therein.

At the trial, the respondent called three witnesses and tendered an exhibit. The appellants, on the other hand, called two witnesses. The respondent’s witness, CW3, gave evidence of how he read the publication and as a result decided to no longer patronize the establishment. He told the trial court of his fright for the “*Otokoto*”appellation by which the respondent had been described in the publication.

At the conclusion of trial, the trial court in its judgment found the appellants liable and ordered them to pay the respondent the sum of two hundred million Naira (N200,000,000.00) as exemplary or aggravated damages.

DECISION OF THE COURT

The appellants were dissatisfied with the judgment, and they appealed to the Court of Appeal. In determining the appeal, the Court of Appeal considered the provisions of section 39(1) and of the Constitution of the Federal Republic of Nigeria, 1999 (as amended) which state thus:

“39(1) Every person shall be entitled to freedom of expression, including freedom to hold opinions and to receive and impart ideas and information without interference.

Without prejudice to the generality of sub section of this section, every person shall be entitled to own, establish and operate any medium for the dissemination of information, ideas and opinions.”

On the Meaning of defamation, the court held that:

“Defamation involves a false statement that defames or harms another person’s reputation. Defamatory statements are categorised as “libel” or “slander”. Libel is written or visual defamation and slander is spoken or oral defamation. What was presented in the instant case was libel.

On the elements of tort of defamation, the court held that:

“The tort of defamation generally consists of the following elements:

- (a) a false statement of fact; the statement must be capable of a defamatory
- (b) meaning or by reason of an innuendo; the statement must be of and must concern
- (c) another living person;
- (d) publication to a third party; some degree of fault on the part of the person(e)making the statement; and
- (f) harm to the reputation of the person defamed.

In the application of the elements, where a statement is in fact true, no defamation action may be advanced, no matter how defamatory the statement is except where it carries a false implication. The disputed statement must also express or imply an assertion of fact rather than an opinion. The disputed statement also must have a defamatory meaning, that is, it must be capable of harming a person’s reputation in the eyes of a reasonable person. A statement can be defamatory on its face, or it can imply a defamatory meaning. A statement that is, on its face, not defamatory is none the less actionable if the defamatory implication or innuendo becomes reasonably apparent with the addition of other facts, whether contained in the publication itself or otherwise known to the reader. Context is critically important in determining whether a statement is defamatory. A statement standing alone may be rendered non-defamatory when considered in the larger context; conversely, an otherwise innocuous statement may be construed to be defamatory in the light of the surrounding statements. Words are to be given their ordinary, everyday meaning as understood by a reasonable person of ordinary intelligence. In addition, the disputed statement must be capable of harming the reputation of another as to lower him in the estimation of the community or deter third persons from associating or dealing with him. Statements that are merely embarrassing, unflattering or annoying are not defamatory. Rather, the statement must expose one to public hatred, contempt or ridicule, cause him or her to be shunned, and/or tend to injure one in his or her profession or trade.

In the instant case, the respondent did not deny that a corpse meant for collection by its owners on a particular day got missing, but what they rather took exception to be the reference made to the respondent's mortuary as being an establishment of "*Otokoto men*". At the trial, CW3 gave evidence of how he read the publication and as a result since decided to no longer patronize the establishment where he had previously taken all his treatments. He particularly told the court of his fright for the "Otokoto" application by which the respondent had been described in the news story.

On Proper test for person defamed in action for defamation:

"The proper test in a defamation matter is not really about the identity of the defamed, but who the audience may reasonably think is defamed. In the instant case, there was no doubt about the fact that the respondent clearly succeeded in establishing that it was the person defamed in the disputed publication being the legal person that owns the mortuary which the appellants wrote about".

On Defence of fair comment in libel case:

"Fair comment is an impartial observation, opinion or criticism on a matter of public interest, currency, or discourse. It is a dispassionate expression of opinion on fact correctly stated. Therefore, it is a defence to an action for libel that the statement complained of was fair comment on a matter of public interest. The defence of fair comment is very important for the press who daily examine and comment on multifarious topics and people. The plea is based on the important need to preserve the fundamental right to freedom of expression for a person to comment on any matter of public interest". Per OHO, J.C.A. held that:

"Here lies a situation where the DW1 and author of the disputed publication was not oblivious of the infamous 'Otokoto' saga of 1996 and the opprobrium it attracted for the decent minded residents of Owerri Community when a certain Mr. 'Otokoto' was caught with the remains of a little boy who got missing a few days before then. Mr. 'Otokoto' was in the process of using the boy's remains for rituals and this generated such a stigma for the Owerri Community, that no one since then has been willing to be publicly associated with the name; 'Otokoto', which had remained synonymous with using human beings for the performance of money rituals. Although, the saga of the missing corpse in this case was the truth, even as it was admitted by the respondent's witnesses who gave a perfectly logical explanation for the mix-up, such that the appellants cannot in all honesty say that the author's comments made of the Aladinma Hospital Mortuary and its staff, which described them as '*Otokoto men*' was indeed an honest and fair comment made with the best of intentions.

In the instant case, the appellants' newspaper enjoys very wide circulation in addition to the publication made in its website which implies that the news story was circulated world-wide. The trial court took all of these into consideration before making its award of N200,000,000.00 in the case.

On Constitutional guarantee of right to freedom of expression:

“By virtue of section 39(1) and of the Constitution of the Federal Republic of Nigeria, 1999 (as amended), every person shall be entitled to freedom of expression, including freedom to hold opinions and to receive and impart ideas and information without interference. Without prejudice to the generality of section 39(1), every person shall be entitled to own, establish and operate any medium for the dissemination of information, ideas and opinions. The section includes among the fundamental right of the citizens, the right to know and be heard by all. It also stipulates the duties of both the press and the citizens.

On whether freedom of press absolute:

“However, the fact that this provision defines their duties (press and citizen), does not in any way guarantee their going beyond the Constitution to seek information and disseminate same. Freedom of the press though fundamental is not absolute. The journalist in the practice of his or her profession is often subjected to the ordinary laws of the land. These laws usually come into play while the reporter is gathering news or during the story's publication.

Ideally, freedom of the press should include the freedom to gather news, write it, publish it and circulate it. But in most cases, journalism is vulnerable by the nature of its ownership, audience and political machinations. The reporters themselves and other professionals associated with the gathering, processing and dissemination of news, due largely to the failing and weaknesses inherent in the very nature of the human person do not seem to have helped matters. Press freedom guaranteed by the Constitution does not say that reporters should publish destructive stories about peoples' businesses without first having to conduct some investigation before hurrying to the press. Press freedom commands a corresponding measure of responsibility on the part of the reporter who must employ the highest level of professionalism in ensuring that a balanced and fair reportage of events are published as they have occurred. In the matter of the dissemination of news the press must ensure the accuracy of its information before it passes it to others as gospel truth. To know the truth and to disseminate untruth to the ignorant, or to disseminate news carelessly and recklessly as to whether it is true or false is the most heinous of all sins under section 39 of the Constitution of Nigeria. What if the people are misled and adverse consequences are recorded? The first attribute of the press in the service of society is truthfulness, or in journalistic parlance, accuracy of reporting.

This court and as well as the lower court having found that the appellants were on the wrong side of these professional virtues, there is no way this court will not resolve this issue against the appellants.”

Going by the above dicta, the statements published by the appellants were neither the truth nor fair comment but apparently lowered the reputation of the respondent in the estimation of right thinking members of society generally and indeed not only tended to cause the respondent to be shunned by members of the public but actually caused one of its esteemed customers to shun and avoid it as a hospital run by ‘*Otokoto*’ ritualists.

IFEANYI UKEGBU (For himself and on behalf of Media Rights Advocates, a Non-Governmental Organization) V. 1. NATIONAL BROADCASTING COMMISSION

2.DAAR COMMUNICATIONS LTD.

3.MULTI CHOICE (NIG.) LTD.

4.NIGERIAN TELEVISION AUTHORITY

[2007] 14 NWLR page 551 CA/A/146/05

SUMMARY OF FACTS

On 30th March, 2004, the Director-General of the 1st respondent did a press briefing on the re-transmission of foreign signals by Nigeria terrestrial broadcast stations and announced that in keeping with the mandate of monitoring and regulating the Nigerian airwaves, the 1st respondent has directed all terrestrial broadcast stations in Nigeria who re-transmit live foreign news and news programmes to put an end to the practice forthwith, in accordance with section 2(1)(k) of the National Broadcasting Commission Act. The order was to take effect from 1st April 2004. According to the 1st respondent, the directive become necessary because of the perspectives the news and news magazines convey and the danger the broadcasts post to Nigerians' national interest. In the press briefing, the 1st respondent also noted the persistent issue of unverified claims of miraculous healings on radio and television stations. The 1st respondent insisted that all stations should ensure that their religious programmes conform with the requirements of the Broadcasting Code and ordered that an advert promoting religion in any form must present its claim especially those relating to miracles in such a manner that it is provable and believable. The appellant was very uncomfortable with the stance of the 1st respondent in the press briefing. Consequently, he filed a motion on notice at the Federal High Court under the Fundamental Rights (Enforcement Procedure) Rules seeking *inter alia* a declaration that the code and/or regulation and/or directive issued by the 1st respondent stopping the relay of news and news magazine broadcasts from foreign stations by Nigerian terrestrial stations effective from 1st April, 2004 is illegal, unconstitutional and a breach of the appellant's right to receive information as guaranteed by section 39(1) of the 1999 Constitution and/or Article 9(1) of the African Charter on

Human and Peoples Rights (Ratification and Enforcement) Act; a declaration that the compliance by the 2nd respondent with the code and/or regulation and/or directive of the 1st respondent is illegal, unlawful, unconstitutional, a breach and a denial of the appellant's right to receive information. The appellant also sought a declaration that the code/or regulation and/or directive issued by the 1st respondent stopping the broadcast of religious programmes featuring miracles on Nigerian broadcast stations is illegal, unconstitutional and a breach of the appellant's right to religion and to receive information; an order restraining the 1st respondent from directing the 2nd - 4th respondents to desist from relaying news and news magazines of foreign stations to the appellant; and an order restraining the 1st respondent from directing the 2nd - 4th respondents to desist from broadcasting religious programmes featuring miracles. The respondents filed a preliminary objection on the grounds that the appellant lacked the requisite *locus standi* to maintain the action; that the subject matter of the suit as constituted was not justiciable and therefore the court lacked the jurisdiction to entertain the matter; and that the reliefs sought against the 2nd and 3rd respondents were not within the jurisdiction of the court. After hearing arguments on the objection, the trial court overruled the objection and proceeded to hear the motion on notice. In overruling the objection, the trial court held that the appellant had *locus standi* to maintain the action and that his *locus standi* was in the fact that he was alleging that his right under section 38 of the 1999 Constitution had been violated by the respondents.

After hearing arguments on the motion on notice, the trial court dismissed the application on the ground that it lacked merit. The trial court held that the banning of direct relay of foreign news in the Nigerian Broadcasting Code was justifiable and in accordance with the provisions of section 39 of the 1999 Constitution.

Dissatisfied, the appellant appealed to the Court of Appeal.

DECISION OF THE COURT

In determining the appeal, the Court of Appeal considered the provisions of sections 38(1), 39(1) and 46(1) of the 1999 Constitution which respectively state thus:

- "38(1) Every person shall be entitled to freedom of thought, conscience and religion, including freedom to change his religion or belief, and freedom (either alone or in community with others, and in public or in private) to manifest and propagate his religion or belief in worship, teaching, practice and observance.
- 39(1) Every person shall be entitled to freedom of expression, including freedom to hold opinions and to receive and impart ideas and information without interference.

- 46(1) Any person who alleges that any of the provisions of this Chapter has been, is being or likely to be contravened in any State in relation to him may apply to a High Court in that State for redress."

On Meaning of locus standi:

"*Locus standi* or standing to sue is the legal right of a party to an action to be heard in litigation before a court of law or tribunal. The term entails the legal capacity of instituting, initiating or commencing an action in a competent court of law or tribunal without any inhibition, obstruction or hindrance from any person or body whatsoever. In other words, *locus standi* is the right of appearance in a court of justice or before a legislative body on a given question.

On Need for plaintiff to have sufficient legal interest in seeking redress in court:

"A plaintiff must have sufficient legal interest in seeking redress in court. Without sufficient legal interest, a party cannot completely seek redress in a court of law. And the term "sufficient interest" can be determined in the light of the facts and circumstances of each case".

On Locus standi of party who complains of breach of fundamental right:

"By virtue of section 46(1) of the 1999 Constitution, a party who complains or is able to show that his civil rights and obligations have been or are in danger of being infringed has the *locus standi* to ventilate his grievance in a court of law. The fact that the party may not succeed in the action does not have anything to do with whether or not he has *locus standi* to sue. The party has an added responsibility to satisfy the court that he has an interest over and above that of the general public. In the instant case, the appellant failed to show a personal interest that was above that of the public which was affected by the press briefing of the Director General of the respondent on 30/3/4. The appellant did not establish his interest in the religious broadcast of miracles, or that he owned a broadcast station or was a sponsor of any of the programmes, other than that he listened to such programmes".

On Constitutional guarantee of right to freedom of thought, conscience and religion and to freedom of expression:

"By virtue of section 38(1) of the Constitution, every person shall be entitled to freedom of thought, conscience and religion, including freedom to change his religion or belief, and freedom (either alone or in community with others, and in public or in private) to manifest and propagate his religion or belief in worship, teaching, practice and observance".

On Constitutional guarantee of right to freedom of expression:

“Also, by virtue of section 39(1) of the Constitution, every person shall be entitled to freedom of expression, including freedom to hold opinions and to receive and impart ideas and information without interference”.

On whether rights in section 39 of the 1999 Constitution absolute:

“The rights in section 39 of the 1999 Constitution are not absolute, rights. The rights can be regulated when it comes to wireless, broadcasting, television or films”.

On Need on party who complains of breach of rights under sections 38 and 39 of the 1999 Constitution to depose personally to affidavit in support:

“It is necessary for a party who complains that his rights under sections 38 and 39 of the Constitution have been or are being infringed to depose to an affidavit in support of his case or for the deponent to the affidavit to depose to the party's inability to so depose, the party's whereabouts and that the affidavit is filed on behalf of the party. Where any of these is not done, the party will be held unserious in his application”.

On Whether Nigerian Broadcasting Corporation Code contravenes sections 38 and 39 of 1999 Constitution:

“The Nigerian Broadcasting Corporation Code is not contrary to the Constitution. It is a valid subsidiary legislation to give full effect to the National Broadcasting Act No. 38 of 1992, as amended. The Code does not contravene sections 38 and 39 or any section of the Constitution”.

President, F.R.N.v.Isa [2017]3NWLR347

SUMMARY OF FACTS

The respondent by originating summons at the Federal High Court, Lagos, challenged the powers of the National Assembly to promulgate the Nigerian Press Council Decree No. 85 of 1992 and the Nigerian Press Council (Amendment) Decree No. 60 of 1999. The two decrees legislated on matters relating to or concerning the press by *inter alia* establishing a body to be known as Nigerian Press Council. The respondents are members of the Newspaper Proprietors Association of Nigeria, and they sued on behalf of themselves and on behalf of the Association. The reliefs they claimed before the trial court include declarations that the press is not one of the matters with respect to which the National Assembly of the Federal Republic of Nigeria is empowered to make laws as contained in section 4(2)(a) and of the Constitution of the Federal Republic of Nigeria, 1999; perpetual

injunction from treating the Decrees as existing laws and implementing or giving effect to them; or in the alternative a declaration that the Decrees are inconsistent with section 39(1)(e) of 1999 Constitution.

The trial court granted the reliefs in part. The appellants being dissatisfied with the decision of the trial court appealed to the Court of Appeal. In resolving the appeal, the Court of Appeal considered the relevant provisions of the 1999 Constitution and the Nigerian Press Council Act.

Section 39 (1), and of 1999 Constitution which provides as follows:

Every person shall be entitled to freedom of expression, including freedom to hold opinions and to receive and impart ideas and information without interference.

Without prejudice to the generality of sub section of this section every person shall be entitled to own, establish and operate any medium for dissemination of

(2) information, ideas and opinions:

Provided that no person, other than the Government of the Federation or of a State or any other person or body authorized by the president on the fulfilment of conditions laid down by an Act of the National Assembly shall own, establish or operate a television or wireless broadcasting station for any purpose whatsoever.

Nothing in this section shall invalidate any law that is:

(3) reasonably justifiable in a democratic society -

For the purpose of preventing the disclosure of information received in confidence, maintaining the authority and independence of courts or regulating telephone, wireless broadcasting, television or the exhibition of

(a) cinematograph films: or

Impose restrictions upon persons holding office under the Government of the Federation or of a state, members of armed forces of the Federation or members of the Nigeria Police Force or other Government security services or

(b) agencies established by law.

Sections 1 and 3 of the Nigerian Press Council Act, which state:

There is hereby established a body to be known as the Nigerian Press Council (in this Act referred to as ‘the Council’) which shall be a body corporate with perpetual succession and a common seal and may sue and be sued in its corporate name.

Section 3 provides:

The council shall be charged with the duty of: -

Enquiring into complaints about the conduct of the press and the organization towards the press and exercising in respect of the complaints the power

(a) conferred upon it under this Act.

Monitoring the activities of the press with a view to ensuring compliance with the code of professional and

(b) Ethical conduct of the Nigeria Union of Journalist.

Receiving application from and documenting the print media and monitoring their performance to ensure that owners and publishers comply with the terms of their mission and objectives in liaison with the Newspaper.

(c) proprietors Association of Nigeria.

Researching into contemporary press development

(d) and engaging in updating press documentation.

Fostering the achievement and maintenance of high

(e) professional standards by the press;

Reviewing development likely to restrict the supply through the press, of information of public interest and importance or which are liable to prevent free access of the press to information and advising on measures.

(f) necessary to prevent or remedy such development.

Ensuring the protection of the rights and privileges of journalists in the lawful performance of them

(g) professional duties.

DECISION OF THE COURT

On Right to freedom of expression and to own medium for dissemination of information:

“By virtue of section 39(1) and of the 1999 Constitution, every person shall be entitled to freedom of expression, including freedom to hold opinions and to receive and impart ideas and information without interference. Without prejudice to the generality of subsection of the section, every person shall be entitled to own, establish and operate any medium for dissemination of information, ideas and opinions provided that no person, other than the Government of the Federation or of a State or any other person or body authorized by the president on the fulfilment of conditions laid down by an Act of the National Assembly, shall own, establish or operate a television or wireless broadcasting station for any purpose whatsoever”.

On Extent of right to freedom of expression:

“Nothing in section 39 and of 1999 Constitution shall invalidate any law that is reasonably justifiable in a democratic society for the purpose of preventing the disclosure of information received in confidence, maintaining the authority and independence of courts or regulating telephone, wireless broadcasting, television or the exhibition of cinematograph films; or impose restrictions upon persons holding

office under the Government of the Federation or of a state, members of armed forces of the federation or members of the Nigeria Police Force or other Government security services or agencies established by law”.

On Establishment and duties of Nigerian Press Council:

“Sections 1 and 3 of the Nigerian Press Council Act provide for the establishment of the Nigerian Press Council, in the Act referred to as the Council, which shall be a body corporate with perpetual succession and a common seal and may sue and be sued in its corporate name”.

On Functions of Nigerian Press Council -

The Council shall be charged with the duty of:

Enquiring into complaints about the conduct of the press and the organization towards the press and exercising in respect of the complaints the power conferred upon

(a) it under the Act; Monitoring the activities of the press with a view to ensuring compliance with the code of professional and ethical conduct of the

(b) Nigeria Union of Journalist;

Receiving application from and documenting

(c) The print media and monitoring their performance to ensure that owners and publishers comply with the terms of their mission and objectives in liaison with the Newspaper Proprietors Association of Nigeria; Researching into contemporary press development and engaging in updating

(d) press documentation; Fostering the achievement and maintenance

(e) of high professional standards by the press; Reviewing development likely to restrict the supply through the press, of information of public interest and importance or which are liable to prevent free access of the press to information and advising on measures necessary to prevent or remedy such

(f) development; and

Ensuring the protection of the rights and privileges of journalists in the lawful

(h) performance of their professional duties.

On Constitutional right of every citizen of Nigeria to hold and disseminate information -

“Section 39 of the 1999 Constitution of the Federal Republic of Nigeria makes provision for the right of every citizen in Nigeria to freely hold and disseminate information without interference. Further, section 22 of the same Constitution amplifies the constitutional right by enjoining the press, radio, television and other agencies of the mass media to uphold the fundamental objectives contained in Chapter 2 of the Constitution”.

On Constitutional guarantee of right to freedom of association:

“Our Constitution recognizes the establishment and membership of professional bodies in Item 49 of the Second Schedule, Part 1 of the Constitution; and the right to freedom of association is guaranteed in section 40 of the 1999 Constitution of the Federal Republic of Nigeria”.

On Extent of right of freedom of expression:

Our laws empower professional bodies to make codes and/or regulations for themselves so long as such codes and/or regulations are not inconsistent with the provisions of the Constitution. Professional bodies with provisions similar to the Nigerian Press Council Act are many. Thus, sanctions provided for members in a professional body are meant to maintain professional standards and do not foreclose the right to seek redress in the regular court. Indeed, every professional body has similar provisions. Freedom of professional occupation is guaranteed by the Constitution. To that effect, the Press Council, in this case, is empowered to receive applications, document the print media and also monitor their performance to ensure that owners and publishers comply with the terms of their mission and objectives in conjunction with the Newspaper proprietors Association of Nigeria. This does not portend any danger to the exercise of the right to freedom of the press as it addresses application relating to printing of media materials and making sure that such is documented and that the publishers comply with their set down objectives.

On whether power of Nigerian Press Council to make laws on publication constitute infraction of constitutional right to freedom of press:

“Section 17 of the Nigerian Press Council Act empowers the Council to direct publication of apology or correction and to reprimand. This is in line with the law of defamation. Publications are expected to be accurate and un-prejudicial. Empowering the Council to direct written apology or correction and reprimand a professional does not amount to an infraction of section 39 to the extent that the Council constituting itself a court; it only straightens an erring professional who might hide under the cloak of freedom of the press to make scandalous publications”.

On whether right to freedom of expression is absolute -

“By virtue of section 45(1)(a) of the Constitution, nothing in sections 37, 38, 39, 40 and 41 of the Constitution shall invalidate any law that is reasonably justifiable in a democratic society: in the interest of defence, public safety, public order, public morality or public.

- (a) health; or for the purpose of protecting the right and
- (b) freedom of another person.

The consequence of the above provision is that though the right to freedom of expression, including freedom to hold opinions and to receive and impart ideas and information without interference, is guaranteed in section 39 of the Constitution that right however is not absolute”.

On whether right to freedom of expression is absolute -

“In a democratic set up, the right to freedom of expression can never be absolute. There must be boundaries for the protection of society and to avoid anarchy. The right to disseminate information carries with it the responsibility to investigate the accuracy of the information. It can never be absolute. The fact that there are other laws protecting the rights of others cannot preclude the National Assembly from enacting laws for further protection of others and for public order within the contemplation of the Constitution. It is thus necessary that professional standards be provided by professional bodies in specific terms to give effect to the constitutional functions of the press, hence the establishment of the Nigerian Press Council”.

On Conditions for law to derogate from freedom of expression:

“By the express provision of section 45(1) of the Constitution, the law must be reasonably justifiable in a democratic society and it must be in the interest of defence, public safety, public order, public morality or public health, it could also be for the purpose of protecting the right and freedom of other persons. In the instant case the Nigerian Press Council Act satisfies the conditions laid down in section 45(1) of the Constitution. The law is absolutely necessary and reasonably justifiable in a democratic society in the interest of public order and for the purpose of protecting the right and freedom of other persons “.

On whether constitutional right to freedom of association is absolute:

“The right of association guaranteed in section 37 of the Constitution, like the other rights in Chapter IV of the Constitution, is not an absolute right, but a qualified right; which can be derogated from in accordance with the provisions of the 1979 Constitution”.

On whether constitutional right to freedom of expression is absolute:

“Section 39 of the 1999 Constitution, which provides that every person shall be entitled to freedom of expression etc, can never; be absolute in a democratic set up. Otherwise, it will lead to a chaotic society. The practice of various professions must be regulated to ensure order in the society. The general intendment of the Act

(repealing the Nigeria Media Council Act, 1988) is to establish standards for the Nigerian press and to deal with complaints emanating from members of the public about the conduct of journalists in their professional capacity and/or complaints emanating from the press about the conduct of persons or organization towards the press. This is an innocuous intention, which does not negate the Constitution nor gag the right to freedom of the press”.

CASES ON FREEDOM OF ASSEMBLY AND ASSOCIATION **Duruakuv.Nwoke [2015] 15 NWLR PG 417 CA/OW/254/2013**

SUMMARY OF FACTS

The 1st - 3rd respondents and the 1st and 2nd appellants belonged to an association known and called Independent Petroleum Marketers Association of Nigeria, popularly known as and called “IPMAN”, Aba Depot unit. The 1st - 3rd respondents wrote a petition to the 5th respondent against the appellants in which they alleged that the 1st appellant and his cohorts were holding illegal meetings at a hotel in Owerri to incite members of the Association to hoard fuel in order to cause scarcity during the festive period. The appellants alleged that pursuant to the petition, they were arrested, detained at the State Criminal Investigation Department and released on bail. The appellants also alleged that the 1st respondent was using the 4th and 5th respondents to coerce them and other members of the Association to withdraw or amend the resolution of its members to recall the 1st respondent.

Aggrieved by their alleged arrest, detention and humiliation by the police, the appellants filed an application at the High Court of Imo State, Owerri to enforce their fundamental human rights. The appellants sought *inter alia* a declaration that their arrest, harassment, humiliation, torture and detention by the 5th respondent’s agents at the instigation of the 1st - 3rd respondents without any lawful and justifiable cause was unconstitutional, wrongful, unlawful, null and void and an infringement of the appellants’ rights as enshrined in the 1999 Constitution (as amended); and an order compelling the respondents jointly and severally, particularly the 1st - 3rd respondents, to pay to the appellants the sum of N200,000,000.00 (two hundred million naira) as general and exemplary damages and/or compensation for the violation of the appellants’ constitutional rights.

Upon being served with the appellants’ originating processes, the 1st - 3rd respondents filed a counter-affidavit of thirty-four paragraphs denying all the averments in the appellants’ affidavit. The 1st - 3rd respondents averred that the appellants and other marketers were strategizing on how to hoard fuel and cause artificial scarcity of petroleum products so as to achieve price increase consequent

upon which the Association as a body lodged a written complaint with the police, which the 1st - 3rd respondents signed as Chairman, Secretary and Legal Adviser respectively. They also averred that apart from lodging the complaint, the Association did not take any other step to influence the police in the discharge of their duties; that the 5th respondent invited the 1st - 3rd respondents and the appellants to a meeting whereat the issue raised in the petition were discussed after which they all left; and that the appellants were merely invited by the police and were not arrested, detained or tortured.

The 4th and 5th respondents through the 4th respondent deposed to a twenty-two-paragraph counter-affidavit to the effect that they were investigating police officers who investigated a case of conduct likely to cause a breach of the peace reported against the appellants. They admitted that the 1st appellant was arrested but stated that he was not harassed, humiliated or tortured; and that he was released on police bail on self-recognition. They stated that following the petition, the 1st - 3rd respondents were invited to make their statements but only the 3rd respondent volunteered his statement; that they made efforts to bring the 1st and 2nd respondents to make their statements to no avail; that all the interviews that were scheduled between the parties failed as the respondents did not attend; and that had the 1st - 3rd respondents attended the interviews, it would have allowed the 4th and 5th respondents the opportunity to determine the veracity or otherwise of the 1st - 3rd respondents' petition.

The 1st - 3rd respondents filed a notice of preliminary objection on the ground that the appellants failed to comply with the provisions of the Sheriffs and Civil Process Act.

At the conclusion of hearing, the trial court in its judgment dismissed the preliminary objection. The court also held that the appellants' application lacked merit and it was dismissed. The trial court reasoned that the police was justified to react to the complaint that some industrial union members, who procure and distribute petroleum products, were planning to create artificial scarcity and increase price beyond the official price regime; that such complaint had the façade of economic crime and sabotage and the police would be rising to a national security duty to arise and nip such plan, whether real or imagined, in the bud.

The appellants were aggrieved, and they appealed to the Court of Appeal.

DECISION OF THE COURT

In reaching its decision, the court some issues and attempted to proffer answers.

On Constitutional guarantee of right to peaceful assembly and right to freedom of movement:

“Section 40 of the 1999 Constitution (as amended) entrenches the right to peaceful assembly and association while section 41 of the Constitution guarantees a citizen’s right to freedom of movement”.

On whether acts of officers of Association bind Association:

“The acts of the officers of an Association will bind the Association under the Companies and Allied Matters Act since the Association is an artificial person who can only act through its officers who are its alter ego”.

The court further held that:

“Going by the above authorities, it is clear that the 1st - 3rd respondents who set the machinery of the arrest and detention of the appellants by the 4th and 5th respondents are liable for the breach of the appellants’ fundamental rights. It is immaterial whether they were acting on the instructions of IPMAN Aba Depot Unit, for as the learned counsel for the appellants had rightly submitted, under the Companies and Allied Matters Act, the acts of the 1st - 3rd respondents bind the Association since the Association is an artificial person who can only act through the 1st - 3rd respondents who are their alter ego. In any case, there is no evidence from the Association by way of any resolution that they mandated the 1st -3rd respondents to write that petition on their behalf. The conclusion that I have arrived at is that either the respondents would be liable in their personal capacities or vicariously on behalf of the Association they purported authorized them to originate the false, frivolous and malicious petition.”

AGBAI V. OKOGBUE [1991] 7 NWLR PG 391 SC. 104/1989

SUMMARY OF FACTS

The respondent as the plaintiff commenced the suit in the Chief Magistrate Court Aba on 10th August 1978 claiming against the appellants as the defendants the sum of N2,000.00 made up of:

- "(a)i. Return of the Butterfly sewing machine or its value namely N115.00
- ii. Loss of use at the rate of N15.00 per day for 74 days from 22/4/78 to 17/7/78 working days.
- (b) General damages: N775.00"

It was the case for the plaintiff/respondent that he was a tailor by profession and carried on business at Aba. The defendants were members of Aba branch of

Umunkalu Age Group of Alayi. On the 22nd day of April 1978, the defendants/appellant broke and entered the plaintiff's shop and seized and carried away his Butterfly sewing machine. Their refusal to return the sewing machine led to instituting the action against them.

It was the contention of the defendants before the Chief Magistrate that the plaintiff, being a native of Amankalu Alayi, was, by custom, obliged to join an age group and that he could not opt out. He was also obliged by custom to pay all development levies imposed on members by the age group. The plaintiff's sewing machine was seized because he failed to pay the development levy for the purposes of building a health centre in their village. The plaintiff contended that he was not a member of the age grade association in that his religion forbids him to join and that his sewing machine was seized because he refused to pay the contribution levied by the defendants for the construction of a health centre.

The Chief Magistrate court found for the plaintiff and ordered that the sewing machine or its value of N115.00 be returned to the plaintiff. He also awarded N740.00 as special damages for the loss of use of the sewing machine. The defendants appealed to the High Court.

The High Court sitting on appeal, in allowing the appeal and dismissing the plaintiff's claim, held that the custom of plaintiff's people is to seize and keep any goods of a person who fails to pay his own share for the communal project until the person pays, and that the custom is not repugnant to natural justice equity and good conscience nor does it offend any section of the Constitution. The plaintiff who was dissatisfied with the judgment of the High Court appealed to the Court of Appeal.

DECISION OF THE COURT

The Court of Appeal in reversing the decision of the High Court held that the custom of the Amankalu Alayi people enabling seizure of properties of members of age-grade who default in their obligations to their association is unconstitutional.

The defendants being dissatisfied with the decision appealed to the Supreme Court contending, inter-alia, that the court erred in holding that the Alayi custom is invalid, and that the plaintiff/appellant is not a member of the Umunkalu Age-grade Association. Issues raised included:

On Right to freedom of association:

“It is the law that nobody can be compelled to associate with other persons against his will. The constitution of the Federal Republic of Nigeria guarantees every citizen that freedom of choice. Accordingly, any purported drafting of any person into an association against his will even if by operation of customary law is in conflict with the provision of section 26(1) of the 1963 Constitution and is void”.

On Freedom of individual to contract:

“Where a person is a member of an association which has agreed on the mode of enforcing the payment of their levies, it would be a case of *volenti non fit injuria* if the agreed mode is resorted to on failure of a member to pay levies. In the instant case all voluntary members of the Umunkalu age grade association are taken to have agreed that they will be liable to certain penalties if they failed to discharge their civil obligation to the age grade Association. They also agreed by implication that the customary law of Amankalu-Alayi with respect to the seizure of their property in the circumstances should apply. Therefore, the said custom is not repugnant to natural justice, equity and good conscience.

**Anambra State Govt.v. Igbonwa [2021]13NWLR475
NigerianWeeklyLawReports27September2021 CA/AW/80/2020**

SUMMARY OF FACTS

The 1st and 2nd respondents were the President-General and Legal Adviser of a town union known as Alor Peoples’ Convention (APC). The union is governed by a constitution and bye-laws. Consequent upon the said constitution, an election was scheduled to take place about the 17th of March 2012. The 1st and 2nd respondents were to stand for re-election for their respective posts.

About the month of January 2012, an indigene of Alor community, Val Elosiuba (now deceased), wrote a petition to the Governor of Anambra State as well as to the Commissioner for Local Government and Chieftaincy Matters alleging that the 1st respondent was staying in office beyond his tenure as President-General of Alor Peoples’ Convention. The Petitioner therefore prayed the Governor to do all that was necessary and convenient in the circumstances for Alor town to remain as one. A similar petition had been written in 2009 by one Chief Okey Ojibe.

Consequent upon the said letters, the Commissioner for Local Government by a letter dated 1st January 2012 dissolved the Alor People’s Convention and set up a Caretaker Committee of 16 persons to run the affairs of the said town union government for three months with effect from 1st February 2012. The Caretaker

Committee was given the task to conduct election of Alor Peoples Convention at least two weeks before the expiration of their tenure.

The cabinet of Alor community (the Igwe in Council) in reaction to the dissolution (Exhibit 0) responded through their letter dated 11/2/2012 Exhibit E) condemning the dissolution of the town union for no justification. Sequel to exhibit E, the Government appointed a Caretaker Committee by a letter dated 27th March 2012 (Exhibit F) addressed to the Commissioner for Local Government and Chieftaincy Matters who made a finding that there was no crisis in Alor community. The said Committee therefore scheduled an election for Saturday the 14th of April 2012 at Alor Town Hall.

In the early hours of Saturday 14th April 2012, the date fixed for the election, the Anambra State Government cordoned off the area, using Mobile Policemen on the orders of the 5th - 6th respondents. Nobody was allowed into the venue of the election. Consequently, the 1st - 2nd respondents filed a suit at the Federal High Court which was later transferred to the High Court of Anambra State.

Thereafter, the 1st and 2nd respondents filed the present suit with a further amended originating summons dated 5th July 2017 wherein they sought the resolution of seven questions. The 1st and 2nd respondents consequently sought twelve reliefs against the appellants and the 3rd - 7th respondents jointly and severally.

It is on record that the 5th and 6th respondents did not appear at the trial court to defend the suit despite being served with the relevant court processes. It is also on record that the appellants filed counter affidavits in opposition to the suit, but same was struck out for want of diligent prosecution.

Judgment was subsequently delivered on the 5th of January 2019 upholding the claims of the 1st & 2nd respondents. Sequel to the said judgment, election was scheduled for the election of officers of Alor Peoples Convention on the 18th of February 2019 wherein the 1st and 2nd respondents were re-elected as the President-General and Legal Adviser respectively.

Aggrieved by the judgment of the trial court, the appellants appealed to the Court of Appeal.

DECISION OF THE COURT

In arriving at its decision, the court considered some issues for determination, including:

On Constitutional guarantee of right to freedom of association:

“By the provision of section 40 of the 1999 Constitution, every person shall be entitled to assemble freely and associate with other persons. He may form or belong to any political party, trade union, or other association for the protection of his interest. In the instant case, section 26 of Fund for Rural Development Law is in conflict with section 40 of the 1999 Constitution”.

On Constitutional guarantee of right to freedom of association:

“The right to freedom of assembly and freedom of expression are key in any proper democratic system of Government. A law that gives a mortal the powers to unilaterally decide to dissolve an association or town union depending on his mood or which side of his bed he woke up from is not only dictatorial but repressive, unjust, and uncivilized. It runs contrary to all known dictates of modern-day civilization. It is clear that the provisions of section 26 of Fund for Rural Development Law, Cap. 54, Laws of Anambra State 1991, is an affront to Sections 36 and 40 of the 1999 Constitution of the Federal Republic of Nigeria (as amended). The court is not unmindful of the fact that the said Law was made for the peace, order and good governance and that the House of Assembly has the power to make laws, such laws must not be an affront to the Constitution. Any law that is inconsistent with the 1999 Constitution of the Federal Republic of Nigeria (as amended) is void to the extent of its inconsistency.

I.G.P. v. A.N.P.P. [2007] 18 NWLR PG 457 CA/A/193/M/05

SUMMARY OF FACTS

The respondents, being registered political parties in Nigeria requested the appellant, by a letter dated 21st May 2004 to issue police permits to their members to hold unity rallies throughout the country to protest the rigging of the 2003 elections. The request was refused. There was a violent disruption of the rally organized in Kano on the 22nd of September 2003 on the ground that no permit was obtained. The respondents, in turn, instituted an action at the Federal High Court, by way of originating summons, against the appellant where they submitted the following issues for determination of the court:

(1) Whether the police permit or any authority is required for holding a rally or procession in any part of the Federal Republic of Nigeria.

(2) Whether the provisions of the Public Order Act, Cap. 382, Laws of the Federation of Nigeria, 1990, which prohibit the holding of rallies or processions without a police permit are not illegal and unconstitutional having regard to section 40 of the 1999 Constitution and Article 11 of the African Charter on Human and People's Rights (Ratification and Enforcement) Act, Cap. 10, Laws of the Federation of Nigeria, 1990."

The respondents then claimed as follows:

(I) A declaration that the requirement of police permit or other authority for the holding of rallies or processions in Nigeria is illegal and unconstitutional as it violates section 40 of the 1999 Constitution and Article 11 of the African Charter on Human and People's Rights (Ratification and Enforcement) Act, Cap. 10, Laws of the Federation of Nigeria (1990).

(II) A declaration that the provisions of the Public Order Act, Cap. 382, Laws of the Federation of Nigeria 1990 which require police permit or any other authority for the holding of rallies or processions in any part of Nigeria is illegal and unconstitutional as they contravene section 40 of the 1999 Constitution and Article 7 of the African Charter on Human and People's Rights (Ratification and Enforcement) Act, Cap. 10, Laws of the Federation of Nigeria, 1990.

(III) A declaration that the defendant is not competent under the Public Order Act, Cap. 382, Laws of the Federation of Nigeria, 1990 or under any law whatsoever to issue or grant permit for the holding of rallies or processions in any part of Nigeria.

(IV) An order of perpetual injunction restraining the defendant whether by himself his agents, privies and servants from further preventing the plaintiffs and other aggrieved citizens of Nigeria from organizing or convening peaceful assemblies, meetings and rallies against unpopular government measures and policies."

At the trial court, both parties contended as to whether the provisions of the Public Order Act, Cap. 382, Laws of the Federation of Nigeria, 1990, particularly its section 1(2), (3), (4), (5) and (6) and sections 2, 3 and 4 are inconsistent with the fundamental rights to peaceful assembly and association as guaranteed in sections 39 and 40 of the 1999 Constitution and Article 11 of the African Charter on Human and People's Rights, Cap. 10, Laws of the Federation of Nigeria, 1990. They also contended as to whether there is any provision of the Public Order Act which authorizes the Inspector General of Police to grant permit before holding rallies or to disrupt rallies and as to when sections 39 and 40 of the 1990 Constitution and the African Charter can be violated pursuant to section 45 of the 1999 Constitution.

In its considered ruling, the trial Court granted the reliefs of the respondents. Aggrieved by the judgment, the appellant appealed to the Court of Appeal. In determining the appeal, the Court of Appeal considered the provisions of Order 3 rule 15(1) & (3) Court of Appeal Rules, 2002, section 1(2), (3), (4), (5) & (6) and

sections 2, 3 & 4. Public Order Act Cap. 382, Laws of the Federation of Nigeria, 1990 and sections 40 and 45(1), 1999 Constitution. They provide as follows:

Sections 40 and 45(1), 1999 Constitution -

"Every person shall be entitled to assemble freely and associate with other persons, and in particular he may form or belong to any political party, trade union or any other association for the protection of his interests: Provided that the provisions of this section shall not derogate from the powers conferred by the Constitution on the Independent National Electoral Commission with respect to political parties to which that commission does not accord recognition."

45(1) Nothing in sections 37, 38, 39, 40 and 41 of this Constitution shall invalidate any law that is reasonably justifiable in a democratic society:

(a) In the interest of defence, public safety, public order, public morality or public health; or

(b) for the purpose of protecting the rights and freedom of other persons.

(2) An Act of the National Assembly shall not be invalidated by reason only that it provides for the taking, during periods of emergency, of measures that derogate from the provisions of section 33 or 35 of this Constitution; but no such measures shall be taken in pursuance of any such Act during any period of emergency save to the extent that those measures are reasonably justifiable for the purpose of dealing with the situation that exists during that period of emergency:

Provided that nothing in this section shall authorise any derogation from the provisions of section 33 of this Constitution except in respect of death resulting from acts of war or authorise any derogation from the provisions of section 36(8) of this Constitution."

Sections 1(2), (3), (4), (5) & (6), 2. 3 and 4, Public Order Act, Cap. 382, Laws of the Federation of Nigeria, 1990:

1(2) Any person who is desirous of convening or collecting any assembly or meeting or of forming any procession in any public road or place of public resort shall, unless such assembly, meeting or procession is permitted by a general license granted under subsection (3) of this section, first make application for a license to the Governor not less than 48 hours thereto, and if such Governor is satisfied that the assembly, meeting or procession is not likely to cause a breach of the peace, he shall direct any superior police officer to issue a license, not less than 24 hours thereto, specifying the name of the licensee and defining the conditions on which the assembly, meeting or procession is permitted to take place; and if he is not so satisfied, he shall convey his refusal in like manner to the applicant within the time herein before stipulated.

DECISION OF THE COURT

In arriving at its decision, these are some of the issues that was raise by the court:

On Right of the Nigerian citizens to peaceful assembly and association:

“By virtue of section 40 of the 1999 Constitution, every person shall be entitled to assemble freely and associate with other persons and in particular he may form or belong to any political party, trade union or any other association for the protection of his interests. Provided that the provisions of section 40, 1999 Constitution shall not derogate from the powers conferred by this Constitution on the Independent National Electoral Commission with respect to Political Parties to which that commission does not accord recognition”.

On Importance of rights to freedom of assembly and expression:

“The rights to freedom of assembly and freedom of expression are the bone of any democratic form of government. Besides their embodiment in the supreme law of the land, the 1999 Constitution, and the African Charter on Human and People's Rights adopted as Ratification and Enforcement Act Cap. 10, Law s of the Federation of Nigeria, 1990, a plethora of decisions of Nigerian courts have endorsed same”.

On Supremacy of the Constitution:

“The Constitution of any country is the embodiment of what the people desire to be their guiding light in governance, their supreme law, the grundnorm of all their laws. All actions of the government in Nigeria are governed by the Constitution and it is the Constitution as the organic law of a country that declares in a formal, emphatic and binding principles the rights, liberties, powers and responsibilities of the people both the governed and the government”.

On Duty on courts in interpreting Law or Constitution:

"The duty of the courts is to simply interpret the law or Constitution as made by the legislators or framers of the Constitution. It is not the constitutional responsibility of the judiciary to make laws already made by the legislature. Courts cannot through its interpretation amend the Constitution, neither can they change the words used. Where saddled with the obligation of interpreting the Constitution the primary concern is the ascertainment of the intention of the legislature or law makers. The Constitution cannot be strictly interpreted like an act of the National Assembly, and it must be construed without ambiguity as it is not supposed to be ambiguous. All its provisions must be given meaning and interpretation even with the imperfection of the legal draftsman. All cannons of Constitution must be employed with great caution. A liberal approach must be adopted. Where the provisions of a statute are clear and unambiguous effects should be given to them

as such unless it would be absurd to do so having regard to the nature and circumstance of the case. The court of law is without power to import into the meaning of a word, clause or section of the Constitution or Statute what it does not say. Indeed, it is a corollary to the general rule of construction that nothing is added to a statute, and nothing is taken from it unless there are grounds to justify the inference that the legislature intended something which it omitted to express. The court must not or is not concerned with the result of its interpretation that is it is not the courts province to pronounce on the wisdom or otherwise of the statute but to determine its meaning. The court must not amend any legislation to achieve a particular object or result”.

On Right of Nigerian citizens to hold rallies:

"I am persuaded by the incident cited by the learned counsel for the respondents that Nigerian Society is ripe and ready to be liberated from our oppressive past. The incident captured by the Guardian Newspaper edition of October 1st, 2005, where the Federal Government had in the broadcast made by the immediate past president of Nigeria General Olusegun Obasanjo publicly conceded the right of Nigerians to hold public meetings or protest peacefully against the government against the increase in the price of petroleum products. The Honourable President realized that democracy admits of dissent, protest, marches, rallies and demonstrations. True democracy ensures that these are done responsibly and peacefully without violence, destruction or even unduly disturbing any citizen and with the guidance and control of law enforcement agencies. Peaceful rallies are replacing strikes and violence demonstrations of the past.....

The Police Order Act - relating to the issuance of police permit cannot be used as a camouflage to stifle the citizens' fundamental rights in the course of maintaining law and orderThe right to demonstrate and the right to protest on matters of public concern are rights which are in the public interest and that which individuals must possess, and which they should exercise without impediment as long as no wrongful act is done.....Finally, freedom of speech and freedom of assembly are part of democratic rights of every citizen of the Republic; our legislature must guard these rights jealously as they are part of the foundation upon which the government itself rests....Public Order Act should be promulgated to compliment sections 39 and 40 of the Constitution in context and not to stifle or cripple it. A rally or placard carrying demonstration has become a form of expression of views on current issues affecting government and the governed in a sovereign state. It is a trend recognized and deeply entrenched in the system of governance in civilized countries - it will not only be primitive but also retrogressive if Nigeria continues to require a pass to hold a rally. We must borrow

a leaf from those who have trekked the rugged path of democracy and are now reaping the dividend of their experience."

On Whether the Public Order Act is constitutional:

"The Public Order Act violates the provision of the Constitution and as such it is null and void. The Constitution should be interpreted in such a manner as to satisfy the yearnings of the Nigerian society. The 1999 Constitution is superior to other legislations in the country and any legislation which is inconsistent with the Constitution would be rendered inoperative to the extent of such inconsistency. Section 1 subsections (2), (3), (4), (5), (6), and sections 2, 3.4 of the Public Order Act are inconsistent with the Constitution - they are null and void to the extent of their inconsistency".

Chukwuma v. C.O.P. Nigeria Weekly Law Report 30 May 2005 pg. 278
CA/IL/35/2004

SUMMARY FACTS

The appellants who were the plaintiffs belonged to a social cultural association known as Igbo Community Association, which was meant to promote the welfare of its members resident in Kwara State. The association was to host a meeting of Igbo delegates' assembly which comprised of all the Igbo Community associations in the Northern States of Nigeria in Ilorin at a private hotel, called Yebumot Hotel. On the scheduled day of the meeting, the officers, men and agents of the respondent in this case came to the venue of the meeting and forcefully dispersed the appellants and their members from the venue of the meeting and sealed-off the venue.

The appellants aggrieved by the action of the respondent instituted an action at the Federal High Court, Ilorin seeking a declaration that the action of the respondent was a violation of their constitutional right of association, freedom of movement and assembly; a claim for damages and an injunction restraining the respondent from stopping, intimidating or harassing the appellants from holding their meeting in Kwara State.

The trial court dismissed the action on the ground that the action of the police was justified as they had powers to do so. The appellants dissatisfied with the said judgment appealed to the Court of Appeal which in determining the appeal considered the provisions of section 45 of the Constitution of the Federal Republic of Nigeria, 1999 which provides as follows:

"45(1) Nothing in sections 37, 38, 39, 40 and 41 of this Constitution shall invalidate any law that is reasonably justifiable in a democratic society –

- (a) in the interest of defence, public safety, public order, public morality or public health; or
- (b) for the purpose of protecting the rights and freedom of other persons."

DECISION OF THE COURT

The court in dismissing the appeal considered the issues below:

On Meaning of assembly under the Public Order Act:

"By virtue of section 12(1) of the Public Order Act, Cap. 382, Laws of the Federation, 1990, assembly means meeting of five or more persons".

On Freedom of association:

"By virtue of section 40 of the 1999 Constitution, every person shall be entitled to assemble freely and associate with other persons and may form or belong to any political, trade union or any other association for the protection of his interests".

On Power of governor to direct the conduct of all assemblies, meetings and processions -

"By virtue of section 1(1) of the Public Order Act, Cap. 382, Laws of the Federation, 1990. The Governor of each state is for the purposes of the proper and peaceful conduct of public assemblies, meetings and processions and subject to section 11 of the Public Order Act, empowered to direct the conduct of all assemblies, meetings and processions on the public roads or places of public resort in the state and prescribe the route by which and the times at which any procession may pass".

On Power of police to stop assembly for which no licence has been obtained -

"By virtue of section 2 of the Public Order Act, any police officer of the rank of Inspector or above may stop any assembly, meeting or procession for which no licence has been issued or which violates any conditions of the licence issued under section 1 of this Act, and may order any such assembly, meeting or procession which has been prohibited or which violates any such conditions as aforesaid to disperse immediately. In the instant case, the appellants did not obtain any licence for the assembly, therefore the police were right to disperse them".

On Duties of the police:

"By virtue of section 4 of the Police Act, Cap. 359, Laws of the Federation, 1990, the duties of the police include amongst others the prevention and detection of crime, the apprehension of offenders, the preservation of law and order, the

protection of life and property and the due enforcement of all laws and regulations with which they are directly charged, and they shall perform such military duties within or without Nigeria as may be required of them by, or under the authority of, the Police Act or any other Act. In the instant case, the action of the police in frustrating the meeting of the association was to maintain law and order and their action was justifiable”.

On Whether a Nigerian citizen requires a police permit to hold a private meeting in a private place:

“A Nigerian citizen does not require a police permit to hold a private meeting in a private place”.

On Meaning of public meeting under the Public Order Act”

“By the provision of section 12(1) of the Public Order Act, Cap. 382, Laws of the Federation, 1990, a public meeting includes any assembly in a place of public resort and any assembly which the public or any section thereof is permitted to attend, whether on payment or otherwise, including any assembly in a place of public resort for the propagation of any religion or belief whatsoever of a religious or anti-religious nature. In the instant case, it was not in dispute that the meeting of the appellants was for all the Igbos residing in the entire Northern States of Nigeria. The contents of exhibit 1 leave no one in any doubt that though the meeting was to be held in a private place, for all intents and purposes, same was public meeting”.

Eronini v. Eronini **7October2013 page 32** CA/PH/304/2005

SUMMARY OF FACTS

The 1st to 4th appellants allegedly banned the women organization of the respondents, the Aladinma women organization and which ban the 5th and 6th respondents at the trial court had been giving effect to. The women organization had been involved in the construction of Town Hall in Awo Mbieri through self-help efforts. The appellants through various means tried to prevent the women organization from carrying on its meetings and other activities but that they could only do so by joining or registering with another association called Oganihu women meeting.

The appellants alleged that they proscribed the women organization because the respondents were allegedly using the organization for their selfish interest and had

been removed from office as they failed to organize election in accordance with section 9(c) of the Constitution of Aladinma women Association. They equally alleged that the women opposed the selection and recognition of the 1st respondent as the Eze of Awo Mbieri Autonomous Community. Based on the allegations, the appellants were using the 5th and 6th respondents to arrest, detain and disrupt the meetings of the respondents. They equally used thugs to stop their town hall project.

Consequently, the respondents filed an application against the appellants for the enforcement of their fundamental rights.

At the conclusion of hearing, the trial court granted the prayers of the respondents. Aggrieved, the appellants appealed to the Court of Appeal.

In determining the appeal, the Court of Appeal considered the provisions of sections 40 and 44(1), Constitution of the Federal Republic of Nigeria, 1999 which provide as follows:

“40. Every person shall be entitled to assemble freely and associate with other persons, and in particular he may form or belong to any political party, trade union or any other association for the prosecution of his interests.

Provided that the provisions of this section shall not derogate from the powers conferred by this Constitution on the Independent National Electoral Commission with respect to political parties to which that Commission does not accord recognition.

44(1) No moveable property or any interest in an immovable property shall be taken possession of compulsorily and no right over or interest in any such property shall be acquired compulsorily in any part of Nigeria except in the manner and for the purposes prescribed by a law that, among other things: requires the prompt payment of compensation

(a) therefore; and gives to any person claiming such compensation a right of access for the determination of his interest in the property and the amount of compensation to a court of law or tribunal or

(b) body having jurisdiction in that part of Nigeria.

DECISION OF THE COURT

In dismissing the appeal the court considered the following issues below:

On Right to peaceful assembly and association:

“By virtue of section 40 of the Constitution of the Federal Republic of Nigeria, 1999, every person shall be entitled to assemble freely and associate with other persons, and in particular he may form or belong to any political party, trade union

or any other association for, the protection of his interest provided that the provisions of this section shall not derogate from the powers conferred by the Constitution on the Independent National Electoral Commission with respect to political parties.....”

On Right to freedom of association:

“Nigeria is governed by a living law, the Constitution fashioned after the Constitution of older democracies and had moved away from the law governing the native community which was force of custom whether good or bad and whether repugnant or not. No one can force or coerce any to join a club, society or group that he does not intend or wish to be a member. It is an affront and infraction of the constitutional right to use old age custom that has now been relegated to moribundity to make one acquiesce or become a member to a body that he or she despises”.

PANYA ANIGBORO V. SEA TRUCKS NIGERIA LIMITED [1995] 6
NWLR pg. 35 CA/B/186/93

SUMMARY OF FACTS

The facts of the case are as follows: Sometime in November, 1985, certain workers in Sea Trucks Nigeria Ltd., the respondent in this case, decided to join a Trade Union known as "National Union of Petroleum and Natural Gas Workers (NUPENG) instead of the Nigerian Union of Seamen and Water Transport Workers, which their employer (the respondent) considered to be more appropriate. It appears that efforts were made to resolve the matter amicably but when such moves failed, and the workers were adamant and became militant, the employers were compelled to lock out the belligerent workers from their premises, and to put up a Notice at their gate announcing that all the workers had been summarily dismissed en masse.

According to the employers, there was a subsequent notice/radio announcement that all workers who returned to work on or before a certain date would be reengaged on new terms, but on their former salaries. Some workers returned to work as requested, but the appellant and at least three of his other colleagues did not return. The appellant subsequently filed an application at the High Court under the Fundamental Rights (Enforcement Procedure) Rules, 1979, against the respondent claiming that he was wrongly dismissed summarily on the 28th day of February 1986.

He Claimed as follows:

(a) that his purported summary dismissal from the said employment of Sea Truck Nigeria Limited (the defendant) on the 28th of February, 1986 is a breach of his fundamental rights under the Constitution of the Federal Republic of Nigeria 1979 when the defendant locked the plaintiff out of the premises of the defendant and thereby preventing the plaintiff from entering the premises and carrying out the duties of his employment for the defendant and when the defendant pasted the notice of the summary dismissal of the plaintiff written on the notice board at the gate of the premises of the defendant within the jurisdiction of this Honourable Court on the ground that the plaintiff declared along with the other workers of the defendant for NUPENG

(b) order of this Honourable Court to reinstate the plaintiff to his said employment and benefits and entitlements as from the 28th of February 1986; and/or in the alternative N20,000.00 compensation for the said breach of the Fundamental rights of the plaintiff under the Constitution of the Federal Republic of Nigeria 1979.

Ground on which Reliefs are sought.

(a) The summary dismissal is a breach of the fundamental rights of the plaintiff to belong to an association of his own which is NUPENG - National Union of Petroleum and Natural Gas Workers as entrenched in section 37 of the Constitution of the Federal Republic of Nigeria.

(b) The summary dismissal is a further breach of the fundamental right of the plaintiff to a fair hearing (or to be heard) before any punitive action can be taken against him under section 33(1) of the constitution of the Federal Republic of Nigeria.

(c) the summary dismissal is contrary to the current Sea Truck (Nig.) Limited Conditions of service as of the 28th of February 1986 as applied to a confirmed employee of the defendant in Articles 13 and 14 thereof. Dated at Warri this 25th day of February 1987."

The learned trial Judge granted leave to the appellant. However, the learned trial Judge in his final judgment held that the action was statute barred and accordingly struck it out. He then proceeded and considered in extenso the merits of the application in the event he was wrong on the issue of limitation. He found the summary dismissal of the appellant unconstitutional, void, null and invalid. He concluded that but for his conclusion on the issue of limitation he would have ordered reinstatement with full pay and benefits as the remedy.

Both parties were partly dissatisfied with the judgment. While the appellant was dissatisfied with the first part of the judgment, the respondent was satisfied with

the first part of the judgment but dissatisfied with the alternative judgment. Therefore, the appellant appealed while the respondent also cross-appealed.

The Court of Appeal in resolving the appeal considered the provisions of Section 37 of the 1979 Constitution and Order 1 rule 3 (1) of the Fundamental Rights (Enforcement Procedure) Rules, 1979. They provide:

"37. Every person shall be entitled to assemble freely and associate with other persons, and in particular he may form or belong to any political party, trade union or any other association for the protection of his interests:"

Order 1 rule 3(1):

"3(1) Leave shall not be granted to apply for an order under these rules unless the application is made within twelve months from the date of the happening of the event, matter or act complained of or such other period as may be prescribed by any enactment or, where a period is so prescribed, the delay is accounted for to the satisfaction of the court or judge to whom the application for leave is made."

DECISION OF THE COURT

The court in allowing the appeal and dismissing the cross-appeal held as follows:

On Constitutional right to freedom of association -

"By virtue of Section 37 of the 1979 Constitution, the right to form or join any political party or trade union is exclusively that of the individual citizen and not that of his employer. His employer has no business forming a trade union let alone compelling his workers to join it. In the instant case, it was a violation or breach of Section 37 of 1979 Constitution for the defendant to insist that the appellant and his other co-workers should join the Nigerian Union of Seamen and Water Transport Workers instead of the National Union of Petroleum and Natural Gas Workers (NUPENG). And to go further and dismiss them summarily for refusing to carry out the order virtually amounted to aggravating a bad situation or adding insult to injury which must be redressed".

On Meaning of 'trade dispute' -

"Trade dispute" means any dispute between employers and workers or between workers and workers, which is connected with the employment or non-employment, or the terms of employment or conditions of work of any person".

The court decided that:

- (a) the "Summary dismissal by Sea Truck (Nig.) Ltd., on the 28th of February 1986 is unconstitutional and a breach of his Fundamental right to belong to a trade union of his choice.
- (b) Reinstatement and
- (c) N20,000.00 compensation for breach of his fundamental rights."

DRLI VS LTSM:

The facts of this suit occurred on the back of an alleged tweet by LTSM offering for sale, over 200 million Nigerian and international mailing lists. DRLI brought the suit under the FREP Rules and contended that LTSM does not have the right or legal basis to process Personal Data, which was ratified by Nigeria on 22 June 1983, and Domesticated by the African Charter on Human and Peoples' Rights (Ratification and Enforcement) Act, Cap. A9 Laws of the Federation of Nigeria, 2004 9 Suit No. AB/83/2020. The central issue was whether LTSM invaded or was likely to invade DRLI's rights to privacy provided under Section 37 of the Constitution and the NDPR. The court held that the right to privacy under Section 37 of the Constitution ought to be interpreted expansively to include protection of Personal Data under the NDPR and therefore, the suit was properly situated under the FREP Rules.

The approach adopted by the court in this case tends to suggest that a breach of a Data Subject's right under the NDPR may be remedied by an action brought under the FREP Rules simpliciter.

On the flip side, those opposed to this view, however, argue that a Data Subject's rights under the NDPR are neither constitutional rights nor fundamental human rights under the African Charter, and as such, cannot be enforced under the procedure provided in the FREP Rules.

This position received judicial approval in the recent judgment of the Federal High Court of Nigeria (the "FHCN") presided over by the Honourable Justice Ibrahim Watila delivered on 9 December 2020 in the case between the **Incorporated Trustees of Laws and Rights Awareness Initiative and The National Identity Management Commission (RAI vs NIMC)**: It was held in the case that a breach of Data Subject's right under the NDPR is not necessarily a breach of the right to privacy under the Constitution, so that a claim for interpretation of the provisions of the NDPR is not a fundamental rights action falling within the purview of the FREP Rules. This seems to be the latest judicial decision on the subject and which for clarity's sake, we have considered the facts in detail below.

The facts of RAI VS NIMC: The suit was filed in connection with the initiative of the Nigerian Government to establish a national identity database pursuant 10 Suit

No. FHC/AB/CS/79/2020 (Unreported) to the National Identity Management Commission (“NIMC”) Act enacted in 2007. NIMC is the public body established to, among others, maintain this database and issue National Identification Numbers to registered persons. RAI, a public interest litigant purportedly suing for and on behalf of one Daniel John, claimed that the processing of Personal Data by NIMC is likely to interfere with Daniel John’s right to privacy guaranteed under Section 1.1(a) of the NDPR and Section 37 of the Constitution. On the basis of this contention, RAI sought to injunct NIMC from further releasing digital identity cards pending an independent report of external cyber security experts on the safety and security of the Respondent’s applications. The suit was brought under the FREP Rules. One of the central issues that came up for consideration was whether the claim for breach, or rather, potential breach of the provisions of the NDPR was properly brought under the FREP Rules having been lumped together with a claim for breach, or potential breach of the right to privacy under Section 37 of the Constitution?

The FHCN, after a careful review of the arguments on both sides, held that the suit was wrongly brought as a fundamental right enforcement action under the FREP Rules for the following reasons:

- by virtue of Section 3.2.2 of the NDPR¹¹, a breach of the NDPR is construed as a breach of the provisions of the National Information Technology Development Agency Act, 2007 (the “NITDA Act”) and therefore, a Data Subject can only sue for breach of his rights under the NITDA Act; and before an action can be brought under the FREP Rules, the action must be premised on a breach of a fundamental right provided for under Chapter IV of the Constitution as the primary or principal claim. The court found that the principal Provides as follows, “Any breach of this Regulation [the NDPR] shall be construed as a breach of the provisions of the NITDA Act” claim in this suit was for breach of the provisions of the NDPR and the claim of breach, or potential breach, of the right to privacy under the Constitution was merely incidental or ancillary to the principal claim. On the balance, the reasoning of the FHCN in RAI vs NIMC referenced above, seems plausible and persuasive. We say so for the following sundry reasons:

First, while some rights of the Data Subject under the NDPR may be similar to the right to privacy under the Constitution, we believe that should not necessarily elevate the rights of a Data Subject under the NDPR to the status of rights

specifically cognizable under the Constitution, to justify their enforcement under the FREP Rules.

Second, the NDPR derives its legitimacy from the NITDA Act and not the Constitution. The FREP Rules was enacted to regulate the enforcement of to regulate the enforcement of fundamental rights provided for under Chapter IV of the Constitution as well as the African Charter. Therefore, the FREP Rules ought not be deployed in a proceeding where the principal claim is for enforcement of a Data Subject's rights under the NDPR.

Also, in our opinion, the NDPR does not have any constitutional flavour necessary to bring it under the purview of the Constitution for the sake of enforcement by way of an action under the FREP Rules.

And in any case, it must be noted that the FREP Rules were enacted for the very specific purpose of expeditiously hearing and determining proceedings for enforcement of fundamental rights under Chapter IV of the Constitution or under the African Charter. By implication therefore, unless the right to be enforced is one.

See the case of **Enemu & Another vs Ezeonyeka & Others (2016) LPELR-40171(CA)** where it was held that, "the Fundamental Rights (Enforcement Procedure) Rules 1979 were made specifically for a speedy determination of cases seeking the enforcement of the fundamental rights guaranteed by the Constitution of the Federal Republic of Nigeria." Specifically guaranteed and provided under Chapter IV or the African Charter, recourse to the procedure prescribed by the FREP Rules may not be validly had or deployed.

Furthermore, we believe that the approach adopted by the court in the **DRLI VS LTSM** case ignores the import of Section 3.2.2 of the NDPR which states that a breach of the provisions of the NDPR is to be construed as a breach of the NITDA Act, and thus and perhaps, more significantly, the rule that where the words or language used in a statute or law (such as the NDPR), is clear and unambiguous, it ought to be applied and given its ordinary grammatical meaning. More so, as provided in the law, a breach of the NITDA Act may only be remedied or sanctioned in accordance with its provisions, and Section 18 thereof provides that a breach of the NITDA Act by a body corporate or person would upon conviction, attract a fine of N200,000 or imprisonment for a term of one year, or both for first offence; and for a second offence and subsequent offence, the breach would attract a fine of N500,000 or imprisonment for a term of three years, or both a fine and a term of imprisonment. It is equally instructive to note that Section 2.10 of the

NDPR prescribes specialized penalties for breaches of the data privacy rights of any Data Subject. (3)

International Cases Laws on breach of Privacy:

Uber Technologies (4)

The scenario: In August 2018, the FTC announced an expanded settlement with Uber Technologies for its alleged failure to reasonably secure sensitive data in the cloud, resulting in a data breach of 600,000 names and driver's license numbers, 22 million names and phone numbers, and more than 25 million names and email addresses.

The settlement: The expanded settlement is a result of Uber's failure to disclose a significant data breach that occurred in 2016 while the FTC was conducting its investigation that led to the original settlement. The revised proposed order includes provisions requiring Uber to disclose any future consumer data breaches, submit all reports for third-party audits of Uber's privacy policy and retain reports on unauthorized access to consumer data.⁵

Emp Media Inc. (Myex.com)

The scenario: The FTC joined forces with the State of Nevada to address privacy issues arising from the "revenge" pornography website, Myex.com, run by Emp Media Inc. The website allowed individuals to submit intimate photos of the victims, including personal information such as name, address, phone number and social media accounts. If a victim wanted their photos and information removed from the website, the defendants reportedly charged fees of \$499 to \$2,800 to do so.

The settlement: On June 15, 2018, the enforcement action brought by the FTC led to a shutdown of the website and permanently prohibited the defendants from posting intimate photos and personal information of other individuals without their consent. The defendants were also ordered to pay more than \$2 million.⁶

Lenovo and Vizio

The scenario: In 2018, FTC enforcement actions led to large settlements with technology manufacturers Lenovo and Vizio. The Lenovo settlement related to allegations the company sold computers in the U.S. with pre-installed software that sent consumer information to third parties without the knowledge of the users. With the New Jersey Office of Attorney General, the FTC also brought an enforcement action against Vizio, a manufacturer of "smart" televisions. Vizio

entered into a settlement to resolve allegations it installed software on its televisions to collect consumer data without the knowledge or consent of consumers and sold the data to third parties.

The settlement: Lenovo entered into a consent agreement to resolve the allegations through a decision and order issued by the FTC. The company was ordered to obtain affirmative consent from consumers before running the software on their computers and implement a software security program on preloaded software for the next 20 years. Vizio agreed to pay \$2.2 million, delete the collected data, disclose all data collection and sharing practices, obtain express consent from consumers to collect or share their data, and implement a data security program. (7)

VTech

The scenario: The FTC's action against toy manufacturer VTech was the first time the FTC became involved in a children's privacy and security matter. The settlement: In January 2018, the company entered into a settlement to pay \$650,000 to resolve allegations it collected personal information from children without obtaining parental consent, in violation of COPPA. VTech was also required to implement a data security program that is subject to audits for the next 20 years. (8)

LabMD

The scenario: LabMD, a cancer-screening company, was accused by the FTC of failing to reasonably protect consumers' medical information and other personal data. Identity thieves allegedly obtained sensitive data on LabMD consumers due to the company's failure to properly safeguard it. The billing information of 9,000 consumers was also compromised. The settlement: After years of litigation, the case was heard before the U.S. Court of Appeals for the Eleventh Circuit. LabMD argued, in part, that data security falls outside of the FTC's mandate over unfair practices. The Eleventh Circuit issued a decision in June 2018 that, while not stripping the FTC of authority to police data security, did challenge the remedy imposed by the FTC.⁹

The court ruled that the cease-and-desist order issued by the FTC against LabMD was unenforceable because the order required the company to implement a data security program that needed to adhere to a standard of "reasonableness" that was too vague.

The ruling points to the need for the FTC to provide greater specificity in its cease-and-desist orders about what is required by companies that allegedly fail to safeguard consumer data. (10)

Big Brother Watch and Others v The United Kingdom (Applications nos. 58170/13, 62322/14 and 24960/15) (13 September 2018).

The European Court of Human Rights has found that the UK's bulk interception regime violates Article 8 of the European Convention on Human Rights (right to respect private and family life) because of insufficient safeguards governing the selection of intercepted communications and related communications data. Further, the Court held that the regime for obtaining data from communications providers violated Article 8 of the Convention because it was not in accordance with EU law that requires data interference to combat "serious crime" (not just "crime"), and for access to retained data to be subject to prior judicial or administrative review. Finally, the Court found that the bulk interception regime and the regime for obtaining communications data from communications service providers violated Article 10 (right to freedom of expression) because of insufficient safeguards for confidential journalistic material. (11)

Catt v The United Kingdom (Case No. 43514/15), European Court of Human Rights, 24 January 2019

The European Court of Human Rights (**ECHR**) has held that an "Extremism Database" maintained by UK police violated an activist's right to privacy under Article 8 of the European Convention for the Protection of Human Rights and Fundamental Freedoms (the **Convention**). (12)

R (on the application of Edward Bridges) v The Chief Constable of South Wales [2020] EWCA Civ 1058

The Court of Appeal of England and Wales has held that the use of automated facial recognition technology (**AFR**) by the South Wales Police Force (**SWP**) unlawfully interfered with Edward Bridges' right to respect for and non-interference by public authorities in his private and family life, which is protected by Article 8 of the *European Convention on Human Rights* (**ECHR**). The Court found that:

- the current legal framework for the use of AFR afforded police officers too broad a discretion;
- the SWP's Data Protection Impact Assessment (**DPIA**) was deficient; and
- the SWP had not taken reasonable steps to comply with the Public Sector Equality Duty (**PSED**) in regard to the characteristics of race and sex.

The decision will impact the development and testing of AFR and marks a step towards ensuring stronger legal frameworks for the use of AFR are instituted in the UK and beyond. (13)

***Minogue v Thompson* [2021] VSC 56 (16 February 2021)**

The Victorian Supreme Court has found that whilst being held in prison, a person's right to privacy and the right to be treated with dignity while deprived of liberty under the *Charter of Human Rights and Responsibilities Act 2006* (Vic) (the **Charter**) were violated when he was subjected to random drug and alcohol testing and a strip search before providing a urine sample for such testing. While Justice Richards found that Dr Minogue's Charter rights were breached, Her Honour is yet to make orders on relief. (14)

INTERNATIONAL CASE LAWS

A Lakshminarayanan v. Assistant General Manager HRM

Case Summary: The Madras High Court quashed the misconduct charges framed against an employee for posting a message in a private WhatsApp Group, as it was protected under the right to freedom of speech and expression. The case concerns an employee and active trade union member who formed a WhatsApp Group to discuss union activities and subsequently shared some messages against the Management. The Management suspended the employee and issued a Charge memo. The High Court analysing the bank's circular and regulations, emphasized the employee's right to freedom of speech and expression under Article 19(1)(a) of the Indian Constitution. The Court interpreted the circular in a manner consistent with legal boundaries, safeguarding the petitioner's right to criticize management within the limits of the law. Stressing the importance of privacy, the Court protected private discussions within encrypted platforms, cautioning against thought-policing. Referring to precedent cases, the Court upheld the petitioner's right to vent grievances and quashed the charge memo, asserting that the petitioner's actions did not constitute misconduct, reinforcing the significance of privacy and freedom of expression in the digital age. (16)

Serap v. Federal Republic of Nigeria

Case Summary: The Community Court of Justice of the Economic Community of West African States (ECOWAS) held that the Nigerian government violated the Applicant's right to freedom of expression, access to information and the media by suspending the operation of Twitter on June 4, 2021. The Nigerian authorities claimed the action was necessary to protect its sovereignty on the grounds that the platform was being used by a separatist leader to sow discord. The Applicants, however, claimed the suspension was in retaliation for a flagged Tweet by Nigerian President Muhammadu Buhari, for violating its rules. The Court found that access to Twitter is a "derivative right" that is "complementary to the enjoyment of the right to freedom of expression." The Court concluded that the law did not suspend the operations of Twitter, and the Nigerian government had

violated Article 9 of the African Charter on Human and People’s Rights (ACHPR) and Article 19 of the International Covenant on Civil and Political Rights (ICCPR). The Court subsequently ordered the Respondent to lift the suspension of Twitter and guarantee non-repetition of the unlawful ban of Twitter. (17)

Amnesty International Togo and Ors v. The Togolese Republic

Case Summary: The Community Court of Justice of the Economic Community of West African States (ECOWAS) held that the Togolese government violated the applicants’ right to freedom of expression by shutting down the internet during protests in September 2017. The Court found that access to the internet is a “derivative right” as it “enhances the exercise of freedom of expression.” As such, internet access is “a right that requires protection of the law” and any interference with it “must be provided for by the law specifying the grounds for such interference.” As there was no national law upon which the right to internet access could be derogated from, the Court concluded that the internet was not shut down in accordance with the law and the Togolese government had violated Article 9 of the African Charter on Human and Peoples’ Rights. The Court subsequently ordered the Respondent State of Togo to take measures to guarantee the “non-occurrence” of a future similar situation, implement laws to meet their obligations with the right to freedom of expression and compensate each applicant to the sum of 2,000,000 CFA (approx. 3,500 USD). (18)