...networking for development

ENHANCING THE DIGITAL RIGHTS OF **NONPROFITS IN NIGERIA**

INTRODUCTION

Citizens and citizen organisations work during a period when technology is driving the interdependence that characterises the quest for change. Computers, mobile connectivity, applications, internet are shaping the way civil society organisations address their vision and mission in ways that bring out solutions and opportunities for growth.

Internet and digital technologies are rapidly transforming the way organisations deliver change across Nigerian communities. Technologies such as artificial intelligence (AI), machine learning (ML) and big data will change the way civil society organisations carry out their business, given the volume of data generated by the sector.

If civil society organisations must play a critical role in decades to come, they need to understand their digital rights so they can interpret the pros and cons of AI, ML and big data within the civic space. The emergence of the COVID-19 pandemic in recent times has necessitated the need for nonprofits to be proactive, responsive, and inclusive in using the internet and digital technologies to do their work as we have never seen in times past.

With technologies evolving as well as bringing together (digital connectivity) and diving (digital divide) and having implications for civic space, we urgently need a foundation for the understanding of how existing laws on internet and digital technologies in Nigeria affect citizens and citizen organisations.

The main laws that relate to CSOs in Nigeria are found in federal legislation because the constitution guarantees freedom of association, there is no restriction on those who wish to join together for any kind of purpose, provided that the purpose for which the group is formed or the methods used are not illegal.

The range of CSOs is as wide and diverse as the country itself, including local 'elites' clubs, traditional age class associations, unions in villages and small towns, and national organisations with thousands of members. While not every group or association must register, those that wish to enjoy the benefits of legal personality or the limited tax advantages that may be available must be registered or incorporated under the Companies and Allied Matters Act (CAMA) 2020.

In Nigeria, the right to internet access is recognized as the most basic means through which citizens have been able to meaningfully participate in governance through the guarantee of human rights. Even though with Nigeria's chequered history on respect for human rights, the past twenty-one years of Nigeria's democratic rule have shown a fair degree of promise for respect for human rights in the Nigerian socio-political space.

This research report is our first attempt at understanding the legal landscape for digital technologies in Nigeria and its implications for the activities and operations of civil society organizations. While technologies are evolving and laws governing them are shaping, the Nigeria Network of NGOs will continue updating this report based on new learnings and findings relating to this topic.

We understand that we may not have captured all of the implications these laws and policies have for organisations within the civil society family, hence, we welcome your thoughts and submissions in making this document more better and suited for our audiences—YOU.

INFORMATION COMMUNICATIONS TECHNOLOGY (ICT) GOVERNANACE IN NIGERIA

Governance of information communications technology in Nigeria is domiciled with the National Information Technology Development Agency (NITDA), a public service institution established by NITDA Act 2007 as the ICT policy implementing arm of the Federal Ministry of Communication of the Federal Republic of Nigeria.

It has sole responsibility of developing programs that caters for the running of ICT related activities in the country. NITDA is also mandated with the implementation of policies guidelines for driving ICT in Nigeria. It plays advisory role in copyright law by verification and revision of applicable laws in tandem with the application of software and technology acquisition.

Nigeria has 2 major Information, Communication and Technology (ICT) laws/regulations:

1. The Nigeria Data Protection Regulation 2019.

2. The Nigerian Cybercrime (Prohibition, Prevention Etc.) Act 2015

Two pending bills at the National Assembly:
1. The Digital Rights and Freedom Bill 2019 (HB. 490)

2. The Social Media Bill 2019 (Protection from Internet Falsehoods and Manipulation and Other Related Matters Bill 2019)

Frameworks and guides which are the:
1. Risk-Based Cybersecurity Framework by the Central Bank of Nigeria to strengthen the cyber defenses of banks and payment service providers.

2. Internet Code of Practice being developed by the Nigerian Communications Commission as part of its internet governance function aimed at defining the rights of and obligations of Internet Access Service. Providers.

Others

1. Nigeria Broadcasting Code 6th Edition.

This report focuses its analysis on the 2 major information, communication and technology laws; however.,it will expand its reach to briefly discuss the digital rights and freedom bill including the social media bill contextualising both within the framework of the rights and operations of civil society organisations.

The internet code of practice which is still under consideration by the NCC is also highlighted along with the Nigeria Broadcasting Code (6th edition) which provides for the establishment of nonprofit and community radio and the controversial hate speech regulation in the code.

1. THE NIGERIA DATA PROTECTION REGULATION 2019 AND ITS IMPACT ON CIVIL SOCIETY ORGANIZATIONS IN NIGERIA

The Nigeria Data Protection Regulation (NDPR) is a regulation issued by the National Information Technology Development Agency (NITDA) specifically to proscribe the minimum data protection required for the collection, storage, processing, management, operation and technical control of personal data in Nigeria.

It is the most far reaching data law passed in Nigeria, imposing stringent conditions on companies and stiff penalties on defaulters. The objectives of the regulation is to safeguard the rights of natural persons to data privacy, foster safe conduct for transactions involving the exchange of personal data, prevent the manipulation of personal data and ensure that Nigerian businesses remain competitive in international trade through the safe-guards afforded by a sound data protection regulation.

The regulation applies to all storage and processing of personal data conducted in respect of Nigerian citizens and residents. The Nigerian Data Protection Regulation introduces new restrictions on collection and processing of personal data and requires such activities be in accordance with a lawful purpose consent by the data subject.

The NDPR regulation requires that data controllers and data processors engage a Data Protection Compliance Organisation (DPCO) to perform a data protection audit and file a report with NITDA within the stipulated timeline, designate a data the organisation, document and publish a protection officer who will be responsible for driving NDPR compliance initiatives within data protection policy in line with the requirements of the data protection regulation, ensure continuous capacity building/training for data protection officer and other personnel involved in processing personal data.

According to the regulation, data controller dealing with more than 10,000 beneficiaries and defaults to the provision of the regulation shall be liable to payment of the fine of 2% of its annual gross revenue of the preceding year or payment of 10 million naira, whichever is greater. Where the data controller deals with less than 10,000 beneficiaries, such controller is liable to a payment of the fine of 1% of its annual gross revenue of the preceding year or payment of the sum of 2 million naira.

Implication for civil society

Civil society organisations collect a lot of personal data such as names, addresses, emails, telephone numbers, website addresses, social media handles and posts. These data are mostly collected from beneficiaries, staff, volunteers, donors, vendors, board and individuals who are only interested in receiving information (newsletters) about what your organisation does.

In developing the NDPR, it is clear that the regulators were not thinking about nonprofits, their primary target seem to be companies in the business of collecting data however a further analysis of the broad scope of the rules capture almost any organisation who touches or processes data.

When linked with the European Union General Data Protection Regulation (GDPR) which by extension have implications for the work of nonprofits. The GDPR defines personal data as "any information relating to an identified or identifiable natural person." It applies to any organisation that collects the data of EU residents, irrespective of whether payment is required.

As soon as personal data of an EU resident is collected, it triggers the GDPR -- and the associated fines for non-compliance regardless of a company's location. For example, if an EU resident signed up for your newsletter because they were interested in your research, course or programs and you send them information material, then the GDPR applies to you.

For civil society data protection is essential. Clearly, organisations within this space must comply with data protection policies either with the NDPR or the EU-GDPR. Anecdotal evidence suggests that very few civil society organisations are aware of the impact of NDPR or GDPR to their operations.

As already noted, civil society organisations were not the targets of regulators (NITDA or EU regulators) and it could take some time for the NDPR which was issued in 2019 to establish

the regulatory mechanism to enforce the policy, nonprofits especially those critical of government could be a target of implementation if and when this is done.

In essence, civil society organisations must approach data collection with care while ensuring that anyone visiting their organisation's website, attending their events or doing business with them regardless of where they come from will be protected as required by the NDPR or GDPR.

Board and management must work together to review and raise organisational awareness on data protection, what data the organisation collects, where they are stored and how to protect them including seeking informed consent for various use of data collected and processed.

2. THE NIGERIAN CYBERCRIME (PROHIBITION, PREVENTION ETC.) ACT 2015 AND ITS IMPACT ON CIVIL SOCIETY ORGANISATIONS IN NIGERIA

Cybercrime is defined as crimes in which a computer is the object of the crime or is used as a tool to commit an offense. Offenders may use computer technology to access personal or commercial information or use the internet for exploitive or malicious purpose.

The Nigeria Cybercrime Prohibition Act provides an effective, unified and comprehensive, legal, regulatory and institutional framework for the prohibition, prevention, detection, prosecution and punishment of cybercrimes in Nigeria. This act also ensures the protection of critical national information infrastructure and promotes cybersecurity and the protection of computer systems and networks, electronic communications, data and computer programs, intellectual property and privacy rights.

The Cybercrime Act 2015 makes provision for **identity theft** with the punishments of imprisonment for a term of 10 years or a fine of not less than #20 million or to both fine and imprisonment. Depending on the nature of the offence and the act carried out by the accused persons. Offences include, amongst others: producing, procuring, distributing and possession of child pornography.

The Cybercrime Act also makes provision for Outlaws **cyber-stalking** and **cyber-bullying** and prescribes punishment ranging from a fine of not less than #2 million or imprisonment for a term of not less than 1 year or to both fine and imprisonment up to a term of not less than 10 years or a fine of not less than #25 million or both fine and imprisonment depending on the severity of the offence.

The Nigerian Cybercrime Act 2015 gives the President the power to designate certain computer systems, networks and information infrastructure vital to the national security of Nigeria or the economic and social well-being of its citizens, as constituting Critical National Information Infrastructure and to implement procedures, guidelines, and conduct audits in furtherance of that.

The Cybercrime Act also prescribes the **death penalty** for an offence committed against a system or network that has been designated critical national infrastructure of Nigeria that results in the death of an individual (amongst other punishments for lesser crimes).

Under the cybercrime Act 2015 in Nigeria, hackers if found guilty, of unlawfully accessing a computer system or network are liable to a fine of up to #10 million or a term of imprisonment of 5 years (depending on the purpose of the hack). The same punishment is also given out to internet fraudsters who perpetuate their acts either by sending electronic messages or accessing and using data stored on computer systems.

Nigerian Cybercrime Act 2015 prohibits **cybersquatting**, which is registering or using an internet domain name with bad faith intent to profit from the goodwill of a trademark belonging to someone else, or to profit by selling to its rightful owner. Individuals who engage in this are liable on conviction to imprisonment for a term of not less than 2 years or a fine of not less than #5 million or both fine and imprisonment.

The Cybercrime act mandates that service providers shall **keep all traffic data and subscriber information** having due regard to the individual's constitutional right to privacy and shall take appropriate measures to safeguard the confidentiality of the data retained, processed or retrieved. The act forbids the distribution of **racist and xenophobic material** to the public through a computer system or network (e.g. Facebook and Twitter).

It also prohibits the use of threats of violence and insulting statement to persons based on race, religion, colour, descent or national or ethnic origin. Persons found guilty of this are liable on conviction to imprisonment for a term of not less than 5 years or a fine of not less than #10 million or to both fine and imprisonment. '

The act also allows for interception of electronic communication by way of a court order by a Judge where there are reasonable grounds to suspect that the content of any electronic communication is reasonably required for the purposes of a criminal investigation or proceedings.

The act specifically creates **child pornography offences**, with punishments of imprisonment for a term of 10 years or a fine of not less than #20 million or to both fine and imprisonment depending on the nature of the offence and the act carried out by the accused persons. Offences include amongst others: producing, procuring, distributing and possession of child pornography. The

Implication for civil society organisations

Civil society organisations hold sensitive data about people, staff, board, volunteers and more, it is important to keep this information safe and secure from cyber-attacks. Nonprofits depend on external organisations, individuals, or volunteers for their IT services from website designs, email setup to management. Increasingly, they depend on digital technology to deliver on their vision and mission.

Like businesses, civil society organisations are relying on technology and are falling victim to a range of malicious cyber activity. Losing access to this technology, having funds stolen or suffering a data breach through a cyber-attack can be devastating, both financially and reputationally.

We have had incidences of website details (username and passwords) being held by vendors or staff owing to disputes or grievances. Generally, nonprofits are complacent about their use of technology and risk of cyber-crime often transferring their risks to their IT service providers without clear protocols and procedures. Attacks on civil society organisations have been steadily rising from phishing, malicious emails, computer misuse, virus, malware, email and social media hacks/extortion to website and identity theft.

With the growing influence of civil society organisations and the huge amount of resources they mobilise in support of the vulnerable in communities across the coun attractive targets of cyber-criminals. Cyber-crime is multi-faceted involving human factor hence organisations need to ensure that they are cyber-security proof with appropriate controls and mechanism in place.

Faced with low resources (operating on very tight budget) and the use of free software applications including the use of volunteers for their IT services, making them particularly vulnerable as IT staff joggle responsibilities to keep the office systems running with less time to focus on security, civil society organisations need to protect themselves from online threats by prioritising skills development and training needs to combat cyber-attacks

Cybercriminals, however, are relentlessly focused on finding their way into computer systems through system vulnerabilities, circumventing established safeguards or by social engineering (tricking) employees into unwittingly disclosing sensitive information. Awareness of cyber-crime among its human resources must be prioritised. Ignoring the risks associated with cyber-crime could lead to damages – financial loss, reputational damage and ability to operate.

A sector wide approach to cyber-crime is more than ever before an important imperative and a governance priority for the Boards of individual civil society organisations -dedicating more time and resource to preventing cyber-attacks and also ensuring that staff members are not using the organisation's systems and technologies in contravention of the cyber-crimes act.

Civil society organisations have flagged Section 24 and 38 of the Act as problematic. Section 24 is seen as cyberstalking and has been repeatedly used to harass and persecute journalists and critics. It is arguably the most dangerous provision against freedom of speech, opinion and inquiry according to digital rights experts. Section 38 provides the duties of a service provider vis-a-vis data retention and contains provisions that are vague and borderline unconstitutional.

The constitutionality of the provisions of the Act has been challenged by 3 organisations ((Media Rights, Paradigm Initiative and Enough is Enough) in the court with both the Federal High Court (January 20, 2017) and Appeal Court (June 22, 2018) ruling that the sections were constitutional. In a concurring judgement however, one of the Justices of the appellate court agreed that the law should be reviewed to whittle-down its arbitrariness. The organisations have approached the Supreme Court asking the court to agree with them on removing the sections from the ACT in its entirety.

3. THE DIGITAL RIGHTS AND FREEDOM BILL 2019 AND ITS IMPACT ON CIVIL SOCIETY ORGANISATIONS IN NIGERIA.

Digital rights are those human rights and legal rights that allow individuals to access, use, create and publish digital media to access and use computers, other electronic devices and telecommunications networks. The concept of digital right is particularly related to the protection and realization of existing rights, such as the right to privacy and freedom of expression, in the context of digital technologies, especially the internet.

The Digital Rights Bill guarantees citizens the right to associate or assemble as a group online on social media platforms or networks. Citizens engaging in peaceful assemblies shall have the right to access the internet and other new technologies at all times without interference except when restricted under the law. The Bill provides sufficient safeguards against abuse online and opportunity for redress; it also equip the judiciary with the necessary legal framework to protect human rights online.

The Bill promotes freedom of expression, assembly and association online; it guarantees the fundamental privacy rights of citizens on the internet while ensuring their safety and wellbeing and define the legal framework regarding surveillance to protect human rights online.

It outline the provisions of lawful and authorized interception of communication within the digital environment without sacrificing the freedom and constitutional rights of citizens. The Digital Rights and Freedom Bill aims at protecting the rights of citizens online and safeguarding the rights of bloggers, data owners and Internet Service Providers (ISPs).

4. THE SOCIAL MEDIA BILL AND ITS IMPACT ON CIVIL SOCIETY ORGANISATIONS IN NIGERIA

The Social Media Bill is a bill to prevent falsehoods and manipulations in Internet transmission and correspondences in Nigeria. It is also a bill to suppress falsehoods and manipulations and counter the effects of such communications and transmissions and to sanction offenders with a view to encouraging transparency by Social Media Platforms using the internet correspondences.

The objectives of the bill is to prevent the transmission of false statements or declaration of facts in Nigeria, it aims to end the financing of online mediums that transmit false statements, Measures will be taken to detect and control inauthentic behaviour and misuse of online accounts (parody accounts), when a paid content is posted towards a political end; measures would be taken to ensure the poster discloses such information, there will be sanctions for offenders/defaulters.

According to the bill, a person must not transmit a statement that is false, transmit a statement that might affect the security or any part of Nigeria, affect public health, public safety or public finance, affect Nigeria's relationship with other countries, influence the outcome of an election to any office in a general election and cause enmity or hatred towards a person or group of persons.

Anyone guilty of the above is liable to a fine of #300,000 or three years imprisonment or both (for individual); and a fine not exceeding ten million naira (for corporate organisations). Same punishment applies for fake online accounts that transmit statements listed above. The instances of falsehood and fake news were cited as reasons for such tight control of internet activities.

This bill gives law enforcement agents the power to arrest those who are found guilty of spreading false information online. While this might be a good thing, any user of the internet whether civil society actors, individuals, social media influencers or institutions could fall on the wrong side of the proposed bill as" falsehood" or "Truth have relative meaning.

The bill is ambiguous, unconstitutional and inconsistent with Nigeria's international obligations as it legislates feelings, gags free speech and violates citizen's human rights especially those fundamental rights and principles associated with expression.

5. INTERNET CODE OF PRACTICE

The Nigerian Communications Commission, in accordance with its authority to regulate the communications sector in Nigeria as expressed in the Nigerian Communications Act 2003, is proposing the Internet Code of Practice to define the rights and obligations of Internet Access Service Providers with regard to the issues therein.

The establishment and enforcement of the Code is envisioned as a co-regulatory effort between the Commission and industry stakeholders. Specifically, the code seeks to:

a) Protect the right of Internet users to an Open Internet;
b) Provide clear guidelines to Internet Access Service Providers on the use of traffic management practices;
c) Outline the obligations of Internet Access Service Providers in relation to the protection of consumers' personal data;
d) Outline the obligations of Internet Access Service Providers in the handling of offensive and potentially harmful content, and the protection of minors and vulnerable audiences online; and
e) Ensure adequate safeguards are put in place by Internet Access Service Providers against unsolicited Internet communications.

Included in the code are the rights of citizens to open internet, information and content distribution, standards for open access, traffic management, non-discrimination, no blocking, no throttling, no preferential data prioritisation, zero-rating, privacy and data protection, data breach, online protection of minors and vulnerable dependents, reporting mechanisms, parental control safeguards against unsolicited internet communications and unlawful content amongst others.

Monitoring and enforcement of the Code is expected to be exercised in accordance with the Nigerian Communications (Enforcement Processes, etc.) Regulations 2019. With respect to any penalties for contravention of applicable provisions, the Commission will be guided by the considerations set out in the Regulations.

The Commission hopes to receive complaints from consumers about non-compliance with the Code from their Internet Access Service Provider through a consumer web portal. Complaints submitted to the portal will be reasonably investigated by the Commission in accordance with its complaints adjudicatory processes.

The Internet Code of Practice shows Governments commitment to allowing citizens the freedom to engage, have robust access and associate freely online—an important building block for true democracy. This important Code helps to keep the internet free and open in ways that ensures citizens and citizen organisations can access information, communicate, and collaborate across borders and creation of new industries.

Elements of network neutrality or net neutrality or anti-discrimination policies are also embedded in the Code based on the principle that Internet Service Providers should treat all data equally, and not discriminate based on the user, content, website, platform, application, equipment being used, or method of communication.

6. NIGERIA BROADCASTING CODE (6th edition)

In 2019, Nigeria's National Broadcasting Commission ("the Commission") pursuant to its powers under Section 2 (h) of the National Broadcasting Commission Act (NBC Act), published the 6th edition of the Nigeria Broadcasting Code (hereinafter referred to as "the NBC Code"). The Code represents the minimum standard for broadcasting in the Federal Republic of Nigeria.

The Code shall be applied in the spirit as well as in the letter in accordance with the professional ideals of broadcasting. The code focuses on social, cultural, economic, political, technological and professional objectives. It details the broadcasting regulations, industry challenges, legal framework and standards.

The Code has advanced from its first edition in 1993 to the 6th edition in 2020 including key amendments on web/online broadcasting, character of local content, acquisition of sports right, prohibition of exclusive licensing and access for Pay TV platforms. The Code provides for the establishment of nonprofit or community radio - the third tier of broadcasting- as recognised by the African Charter on Broadcasting.

It set out regulations on licensing, content, funding, governance language and ownership of this type of radio station. This is an important provision of strengthening and amplifying citizens' voices in issues that matters to them and their development. Community radio acts as a vehicle for the community and voluntary sector, civil society, agencies, NGOs and citizens to work in partnership to further community development aims, in addition to broadcasting.

Community media focus on community participation with the goal of transforming society. They are conceived to inform people and allow them to participate in decisions that affect them. They can facilitate the empowerment of vulnerable communities – populations who are isolated geographically, culturally or linguistically and whose representation is generally ignored by mainstream media – such as women for example.

The objective is to create a public social sphere where anybody can contribute and be heard. but they are enabling isolated communities across Africa to voice their concerns and to access news on issues of local interest. These local stations have the unique ability to inform and educate while being anchored in the community's history and traditions.

A new provision smuggled into the 6th edition of the Code is the hate speech fine which was increased from 500,000 Naira to 5,000,000 Naira. The increase was announced by the Minister for Information and Culture, Alhaji Lai Mohammed, at the unveiling ceremony of the revised National Broadcasting Code by the National Broadcasting Commission (NBC) on the 4th of August 2020.

Under the new code, the commission has also threatened sanctions on media houses for allowing their platforms to be used for "insulting" public officials, Vanguard reported. According to the minister, the review was carried out according to Presidential directive in the wake of the 2019 general elections, which sought for an inquiry into the regulatory role of NBC.

Stakeholders and civil society organisations are concerned about this new amendment to the Code, worry that this new amendment stifles freedom of expression and thought. The Code has claimed its first victim (radio station) already-- an indigenous radio station Nigeria Info, 99.3FM, the regulator sanctioned the radio station for allowing its platform to be used for promoting Hate Speech. The NBC in a statement published on Thursday, August 13 2020 and published by Naijanews wrote:

"The National Broadcasting Commission has noted with grave concern, the unprofessional conduct of Nigeria Info 99.3FM, Lagos, in the handling of the Programme, "Morning Cross Fire", aired on August 10, 2020, between 8.30am and 9.00am.

"The station provided its platform for the guest, Dr. Mailafia Obadiah, to promote unverifiable and inciting views that could encourage or incite to crime and lead to public disorder.

"Dr. Mailafia Obadia's comments on the "Southern Kaduna Crisis", were devoid of facts and by broadcasting same to the public, Nigeria Info 99.3FM, is in violation of the following sections of the Nigeria Broadcasting Code:

"In line with the amendment of the 6th edition of the Nigeria Broadcasting Code, Nigeria Info 99.3FM Lagos, has been fined the sum of N5,000,000.00 (Five Million Naira), only.

"This is expected to serve as a deterrent to all other broadcast stations in Nigeria who are quick to provide a platform for subversive rhetoric and the expositions of spurious and unverifiable claims to desist from such.

The new code has implications shrinking civic space and preventing citizens from providing critical feedback to government and to hold them accountable.

CONCLUSION: THE ROADMAP FOR CIVIL SOCIETY

Technology has proven to be a dual-edged sword: It has advanced the world in ways that have radically improved the operations and activities of civil society organisations--- and it has altered sometimes the fabric of our society and created difficult, new challenges like fake news, deep fakes, hate speech, disinformation, cyber bullying, cyber-crime and misinformation among others.

Events of the past 6 months (the advent of COVID-19) have had enormous impact on civil society. These past months have witnessed an increase in the use of technology by all sectors including civil society. Given the importance of technology to civic space, the result of this research should inspire action among the leadership and management of civil society organisations across the country.

It also provides compelling evidence for civil society organisations to follow. For example, with the work from home policy now one of the responses for addressing COVID-19, organisations are more at risk of violating data protection regulations and susceptible to cyber-attacks as staff members make use of their personal computer and internet connections for work.

What does this mean?

The preceding pages of this report have shown that our understanding and use of technology as a sector comes with responsibilities requiring urgent attention founded on common respect for human dignity including respect for fundamental freedoms and principles. Based on our analysis, we make the following recommendations:·

→ We recommend that as a matter of urgency, civil society organisations adopt specific policies to support full compliance with data protection regulations and put in place anti-cybercrime systems and policies.

→ We urge the Board and management of civil society organisations to institute an organisation-wide review of how the digital technology laws and regulations impacts on their organisational activities including emerging technologies and trends.

→ Investments should be made in both human capacity and physical infrastructure in the use of digital technologies by civil society organizations including improved interest in the governance of these technologies.

→ Respect for human rights – including privacy – is fundamental. Civil society organisations must join the debate on the passage of the digital rights bill and be on the watch to safeguard laws and regulations that protects citizens and citizen organisations fundamental freedoms and principles.

REFERENCES

1. Analysis: What social media bill means to Nigerians, 9 March 2020, available at https://www.orderpaper.ng/analysis-what-social-media-bill-means-to-nigerians/

2. Charities complacent over cybercrime, 3 March 2020, available at https://thirdforcenews.org.uk/tfn-news/charities-complacent-over-cyber-crime

3. CSOs head to Supreme Court over Cyber Crimes Act, 2 August 2018, available at https://www.orderpaper.ng/csos-head-to-supreme-court-over-cyber-crimes-act/

4. Cyber Security Intelligence, Cybercrime is an Increasing Risk for Charities, 11 November 2019, available at https://www.cybersecurityintelligence.com/blog/cyber-crime-is-an-increasing-risk-for-charities-4618.html

5. Developing Communities through Radio, 20 June 2018, available at https://en.unesco.org/radioict/press/developing-communities-through-radio

6. Digital Rights Definition, available at https://en.wikipedia.org/wiki/Digital_rights

7. First Republic Bank, Why Nonprofits are Targets of Cybercrime and How They can Protect Themselves, 17 August 2018, available at https://www.firstrepublic.com/articles-insights/life-money/protect-against-fraud/why-nonprofits-are-targets-of-cyber-crime-and-how-they-can-protect-themselves

8. FG Launches Amended Broadcasting Code, Says Hate Speech Fine now #5million, 4 August 2020, available at https://www.channelstv.com/2020/08/04/fg-launches-amended-broadcasting-code-says-hate-speech-fine-now-n5m/

9. Lai Mohammed hiked hate speech fine without consultation-NBC board, 13 August 2020, available at https://punchng.com/lai-mohammed-hiked-hate-speech-fine-without-consultation-nbc-board/

10. Mailafia: NBC Fines Radio Station #5million for Unprofessional Broadcast, 13 August 2020, available at https://www.channelstv.com/2020/08/13/mailafia-nbc-fines-radio-station-n5m-for-unprofessional-broadcast/?fbclid=IwAR0b7bJ8r01iDublcxIMMtgrXDxRls2FXLBq4anT-3Jjwe5TS9eySRs407w

11. Mailafia: NBC Fines Broadcast Outfit #5million for Hate Speech, 13 August 2020, available at https://www.naijanews.com/2020/08/13/mailafia-nbc-fines-broadcast-outfit-%E2%82%A65m-for-hate-speech/

12. NCC is set to establish Internet Code of Practice, 22 June 2019, available at https://www.ncc.gov.ng/media-centre/news-headlines/589-ncc-is-set-to-establish-internet-code-of-practice

13. Nigerian CSOs kick against social media bill, 5 March 2020, available at https://allafrica.com/stories/202003050677.html

14. Nigerian Communications Commission: The Internet Code of Practice,26 November 2019,available at https://www.ncc.gov.ng/accessible/documents/878-internet-code-practice/file

15. Regulating Nigerian Content On Broadcasting Platforms: An Examination of the Amendments To The 6th Edition Of The Nigeria Broadcasting Code, 2016 available athttps://www.nta.ng/wp-content/uploads/2019/09/1494416213-NBC-Code-6TH-EDITION.pdf

16. What does GDPR mean for U.S. Based Nonprofits?,25 May 2018, available at https://www.forbes.com/sites/forbestechcouncil/2018/05/25/what-does-gdpr-mean-for-u-s-based-nonprofits/#5ec1a2c020f3

17. 10 things to know about Nigeria's cybercrime Act 2015, 3 July 2020, available at https://lawpadi.com/10-things-to-know-about-nigerias-cybercrime-act-2015/#:~:text=The%20Nigerian%20Cybercrime%20Act%202015,Information%20Infrastructure%2C%20and%20to%20implement

For more Information on NNNGO 's work on Enhancing Digital Rights of Nonprofits In Nigeria, contact:

Adeola Odunsi
Project Officer
Nigeria Network of NGOs
Tel: +234 90 6946 0107
E-mail: adeola.odunsi@nnngo.org

Oyindamola Aramide
Communication Officer
Nigeria Network of NGOs
Tel: +234 90 6946 0107
E-mail: oyindamola.aramide@nnngo.org

Cover Photo : 2019, NECA House, Lagos, Nigeria at 19th NNNGO Annual Conference

Nigeria Network of NGOs
15, Ramat Crescent,
Ogudu GRA, Lagos,
Nigeria.
Tel: +234 090 6946 0107
Email: nnngo@nnngo.org

website: https://nnngo.org/

This publication is developed with financial assistance from the International Center for Not-for-Profit Law (ICNL). The contents are the sole responsibility of Nigeria Network of NGOs (NNNGO) and can under no circumstances be regarded as reflecting the position of the ICNL.

CONNECT WITH US

nnngo.org nnngo nnngo nnngo 2349069460107