

CYBERSPACE AND HUMAN RIGHTS IN THE 21ST CENTURY: PROTECTING AND PROMOTING FREEDOM

BY

AWOTOYE TOBILOBA,* ABIOLA ABIADE,** OYANIRAN OYELEKE*** &
SAKPERE WILSON****

Abstract

The flourishing proliferation of the internet has brought in commendable global interactions and information exchange. It is the aim of this research to provide an expansive insight into the multifaceted influence of the internet on both the infringement and protection of human rights worldwide using Nigeria as a case study. As the world digitalization progresses, pivotal areas of laws such as freedom of expression and the press, the right to privacy, right to fair hearing, right to human dignity, right to education, and right to life have all experienced paradigm shifts. A pressing issue of contemporary relevance is the misuse of the internet in facilitating human trafficking, presenting a severe infringement on human rights. The research explores the spectrum of human rights concerns viz-a-viz online platforms, discusses international treaties, domestic legislations, and the role of government agencies. Furthermore, it sheds light on the hurdles faced by legal entities and organizations in curtailing online breaches and suggests viable approaches to address these concerns. In summary, this exhaustive exploration enhances comprehension of the nuanced interplay between the internet and human rights infringements. Through discerning the layered facets of online-induced breaches, the study endeavors to guide policy shifts, legal modifications, and tech-based measures, aiming to alleviate the negative repercussions of the web on upholding individuals' inherent rights.

Keywords: Internet, Human Rights, Violation, Protection

Introduction

Information Communication Technology (ICT) refers to the use of microelectronics-based computing and telecommunications systems to acquire, process, store, and distribute audible, visual, textual, and numerical information.¹ With the advent of the Information Communication

*Lecturer, Faculty of Law, Lead City University, Ibadan. Email: tobilobaawotoye@gmail.com;

Technology, the world has now become a global village where distance is no longer a barrier to commercial and social interactions². This was informed by the breakthrough and exponential growth of the Internet in 1960s, and the World Wide Web in the 1990s³. Since then, there has been continuous improvement in the legal industries and the use of ICT has better sharpen areas of laws like contracts, intellectual property infringement, and freedom of speech, among many others⁴. Approximately 93% of adults use the internet today, according to the Pew Research Centre, with 15% using it exclusively on smart phones.⁵

According to a report by Statista, it was reported that the estimated number of internet users in 2022 worldwide was 5.3 billion and that accounts for 66 percent of the global population⁶. As it stands today, nearly all the countries in the world have access to cyberspace. This implies that governments across the world, business entities and individuals are increasingly using the internet in communication, rendering of services and delivery of goods. This development may unavoidably leave gaps that would metamorphose into breach of individual fundamental human right. The advent of cyberspace has thus extended the definition of publishing of information beyond the conventional means like radio, television, newspapers, broadcasts, books, posters or handbills. Publishing now includes posting on social media platforms and it can be enforceable.

Human rights on the other hand are the a set of laws governing the inalienable rights of individuals and groups by states and non-state actors on the basis of ethical principles regarding what society considers fundamental to a decent life. These norms are incorporated into national and international legal systems, which specify mechanisms and procedures to hold the duty-

** Lecturer, Faculty of Law, Lead City University, Ibadan. Email: ask4abby@yahoo.com;

*** Lecturer, Faculty of Law, Caleb University, Lagos;

**** Lecturer, Faculty of Law, Lead City University, Ibadan. Email: sakpere.wilson@lcu.edu.ng.

¹K. Karl, 'Historical Monograph: Electronic Computers Within the Ordnance Corps. Aberdeen Proving Ground (United States Army)' (1961). . <http://ed-thelen.org/comp-hist/U-S-Ord-61.html>. accessed 28 September 2023

²Kalpesh D.K, 'ICT and its impact on Human Rights' International Research Journal of Commerce Art and Science (2015) 6 (11) page 75

³ D. Connolly 'A little history of the World Wide Web'<https://www.w3.org/History.html> accessed 28 September 2023

⁴Ifeoluwa A. Olubiyi, Ayobami J. Olaniyan and Ngozi Odiaka, 'The Role of Technology in the Advancement of Legal Education and Practice in Nigeria' (2015) <http://eprints.abuad.edu.ng/639/1/Olubiyietal_Paper.pdf> accessed 28 September 2023

⁵'Mobile Fact Sheet' (Pew Research Center: Internet, Science & Tech, 11 May 2023) <<https://www.pewresearch.org/internet/fact-sheet/mobile/#:~:text=Smartphone%20dependency%20over%20time,have%20traditional%20home%20broadband%20service.>> accessed 28 September, 2023

⁶ Number of internet users worldwide from 2005 to 2022' < <https://www.statista.com/statistics/273018/number-of-internet-users-worldwide/#:~:text=Global%20number%20of%20internet%20users%202005%2D2022&text=As%20of%202022%2C%20the%20estimated,66%20percent%20of%20global%20population.>> accessed 28 September 2023

bearers accountable and provide redress for alleged victims of human rights violations⁷. Human rights protections vary from state to state but they all must have distinct characteristics of the rights being inalienable, universality, indivisibility and interdependency. The right must be applicable to all persons irrespective of their gender, race, and creed, religious and cultural background⁸.

It is important to note that cyber laws are necessary for several reasons. These reasons center on the propensity for abuse by users. Cyber laws among others ensure adequate protection for every user of information communication technology, ensure proper governance of the cyberspace, empower regulatory agencies and limits the use of the space within the confines of human rights. The cyberspace is the future of mankind and it keeps evolving.

However, the need to protect the cyberspace has in more ways blinded states and regulators to the need to protect rights of users. States and Policy makers, in a bid to ensure adequate securitization and regulation of the cyberspace infringe on users' right to privacy by not adequately protecting data supplied to the space, thus opening the victim up to avoidable violations. A case in point is the strict cyberspace regulatory framework in China. Some other examples include the proposed social media bill in Nigeria, ban on TikTok in the United States of America and so on. This paper shall discuss how the subject of human rights and the cyberspace intertwine and how rights of users in the space can be protected within the ambit of law.

2.0 Legal and Institutional Framework for ICT and Cyberspace in Nigeria

2.1 The Constitution

As it is with any issue centering on law in any jurisdiction, the grundnorm of that state must always be the first and main legal instrument. Hence, the Constitution of the Federal Republic of Nigeria, 1999 (as amended) which is the chief legal instrument in Nigeria forms the core of the country's framework on regulating the cyberspace. This 1999 Constitution establishes its supremacy and declares that its provisions are binding on all national authorities and citizens.⁹ It further stipulates that if any other legislation conflicts with its provisions, the Constitution will

⁷ Marks S.P Human Rights: A Brief Introduction (2016) <https://www.hsph.harvard.edu/wp-content/uploads/sites/134/2016/07/Human-Rights-A-brief-intro-2016.pdf> accessed 28 September 2023

⁸ United Nations Population Fund 'Human Rights Principles' (2005) <https://www.unfpa.org/resources/human-rights-principles#:~:text=Human%20rights%20are%20universal%20and,religious%2C%20cultural%20or%20ethnic%20background> accessed 28 September 2023

⁹ Section 1(1) of the Constitution of the Federal Republic of Nigeria, 1999 (as amended)

take precedence and such legislation will be void to the degree of the inconsistency.¹⁰ Therefore, it is safe to say that no other law has more potency in terms of bindingness and effect either within or outside Nigeria than the Constitution.¹¹

One major chapter of the constitution that regulates activities within the cyberspace is Chapter 4 which provides for the fundamental rights of every human within the country. Section 37 of the Constitution provides that ‘the privacy of citizens, their homes, correspondence, telephone conversations and telegraphic communications is hereby guaranteed and protected’.¹² All these rights shall be further discussed later in this paper.

2.2 The Cybercrime Act, 2015

The Cybercrime Act is by far the most comprehensive legal document that regulates the cyberspace in Nigeria. This act which was passed by the National Assembly in 2015 offers an efficient and unified framework for Nigeria's legal, regulatory, and institutional structure for prohibiting, preventing, detecting, prosecuting, and punishing cybercrimes.¹³ Even though the Cybercrime Act sounds a bit restricted in scope by virtue of its title, its makers intends for the law to ‘the protection of critical national information infrastructure and promotion of cyber security and the protection of computer systems and networks, electronic communications, data and computer programs, intellectual property and privacy rights’ when done within the country or with Nigerian elements.¹⁴

The Cybercrime Act makes it an offence to engage in acts or omissions that can either immediately or ultimately endanger other humans within territorial space or cyberspace. Some of these offences include any act against a critical national information infrastructure¹⁵, unlawfully

¹⁰ Ibid. S, 1(3)

¹¹ Ibid. S 12.

¹² It should be noted that correspondence, telephone conversations and telegraphic communications all fall within the scope of the cyberspace when done outside the territorial space. See also Sections 39 of the CFRN, 1999 on every human's right to freedom of expression.

¹³ See Section 1(a) of the Cybercrime Act, 2015

¹⁴ Section 1(b)-(c).

¹⁵ Section 5. Critical national information infrastructure are ‘certain computer systems, and/or networks, whether physical or virtual, and/or the computer programs, computer data and/or traffic data vital to this country that the incapacity or destruction of or interference with such system and assets would have a debilitating impact on security, national or economic security, national public health and safety, or any combination of those matters’. This depends on the President's designation in a National Gazette of such computer systems as Critical National information infrastructure. See Section 3(1) of the Act

accessing a computer¹⁶, interception of electronic messages or money transfer or willfully redirecting such¹⁷, computer related forgery¹⁸, computer related fraud¹⁹, and so on.

The Act makes it the responsibility of the National Security Adviser to coordinate the implementation of this Act by establishing a National Computer Emergency Response Team (CERT) and National Computer Forensic Laboratory for a smooth enforcement of its provisions.²⁰ One of the major innovations of the Act is the establishment of the Cybercrime Advisory Council.²¹ The functions of this Council include:²²

- a) create an enabling environment for members to share knowledge, experience, intelligence and information on a regular basis and shall provide recommendations on issues relating to the prevention and combating of cybercrimes and the promotion of cyber security in Nigeria; Functions and powers of the Council.
- (b) formulate and provide general policy guidelines for the implementation of the provisions of this Act;
- (c) advise on measures to prevent and combat computer related offences, cybercrimes, threats to national cyberspace and other cyber security related issues;
- (d) establish a program to award grants to institutions of higher education to establish Cyber security Research Centers to support the development of new Cyber security defences, techniques and processes in the real-world environment; and
- (e) promote Graduate Traineeships in Cyber security and Computer and Network Security Research and Development.

Some of other laws include the Data Privacy Protection Act 2023, Criminal Code Act,²³ the Penal Code Act, Money Laundering (Prohibition) Act of 2011, the Economic and Financial Crime Commission Act of 2004, Banks and other Financial Institutions Act 2020 and the Advance Fee Fraud and Related Offences Act of 2006. Also, Nigeria is signatory to some international instruments on cybercrime such as the ECOWAS Directive on Cybercrime 2010²⁴

¹⁶ Section 6 of the Act

¹⁷ Sections 9 and 11

¹⁸ Section 13

¹⁹ Section 14

²⁰ See Section 41 of the Act

²¹ See Section 42 of the Act

²² Section 43 of the Act

²³ See particularly Section 419 of the Code.

²⁴ Directive C/DIR 1/08/11

and the African Union Convention on Cyber Security and Personal Data Protection 2014.²⁵ With the evolving and transborder nature of cyberspace, it is only logical that domestic legislations alone may not be adequate to regulate the space. Thus, there is need for international organizations, regional organizations, states and major stakeholders in the cyber world to regulate the cyberspace.²⁶ It should be noted, however, that by virtue of section 12 of the Nigerian Constitution, these international laws would not have the force of law unless and until they have been fully domesticated by the National Assembly.

Data Privacy Protection Act, 2023

Legally regulating data privacy in Nigeria has never been more extensive than with the passage of the Data Privacy Protection Act in 2023. Any data controller or processor, whether from outside of Nigeria or inside the country, is subject to the Act's protections when handling personal information on data subjects located in Nigeria.

The Act regulates the 'processing of personal data' but not to personal data solely for household purposes in as much as it does not infringe on a data subject's fundamental right. The primary objectives of the Data Privacy Protection Act 2023 are to protect the fundamental rights and freedoms, as well as the interests of individuals whose data is being processed. This protection is in accordance with the Constitution of the Federal Republic of Nigeria, 1999. Additionally, the act aims to regulate the processing of personal data. Other targets of the Act include promoting data processing practices that ensure the security and privacy of personal data, ensuring that personal data is processed in a fair, lawful, and accountable manner, protecting the rights of data subjects, and providing recourse and remedies in case of rights violations. The Act also aims to ensure that data controllers and processors fulfill their obligations to data subjects, establish an impartial and effective regulatory Commission to oversee data protection and privacy matters, and strengthen the legal framework for Nigeria's digital economy while ensuring the trusted and beneficial use of personal data in regional and global economies.

The Nigeria Data Protection Commission was established by the Act with the following duties: to oversee the implementation of organisational and technological measures to improve personal data protection; to encourage the research and development of personal data protection technologies in line with recognised international standards and relevant international law; to

²⁵ Adopted at the 23rd Ordinary Session of the Assembly of the Union held in Malabo, Equatorial Guinea from 20-27 June 2014

²⁶ E. Jensen, S. Watts, "Cyber Due Diligence" 73 *Oklahoma Law Review*, (2021) 645, p. 691. Available at <https://digitalcommons.law.ou.edu/olr/vol73/iss4/3> (accessed 20 October 2023)

keep track of important data controllers and processors; and to raise awareness about the responsibilities of these individuals. This Data Protection Commission is independent in the performance of the above duties.

Data processing will only be lawful and legal where the data subject's consent has been expressly and clearly received. If such consent is implied, forced or withdrawn, processing of such a data shall not be lawful. It is the duty of a data processor to prove that a data subject gave express consent before his data was processed. Section 64 of the same Act defines consent as 'any freely given, specific, informed, and unambiguous indication, whether by a written or oral statement or an affirmative action, of an individual's agreement to the processing of personal data relating to him or to another individual on whose behalf he has the permission to provide such consent'.

Data subjects' rights were further defined under the Act. Part ten of the Act lays out procedures for achieving justice in cases where such a right has been, is being, or is about to be violated. A data subject has an obligation to lodge a complaint or take appropriate action when they are "aggrieved by the decision, action, or inaction of a data controller or data processor in violation of this Act," as stated in Section 47 of the Act.

3.0 Human Rights in Nigeria

Chapter 4 of the 1999 Constitution (As Amended) regulates the protection of the Fundamental Human right in Nigeria. The following rights are provided for and protected under the constitution. These rights range from the right to life, right to dignity of human person, right to personal liberty and so on. Some of these constitutional provisions are discussed below:

Right to Life:²⁷ Every person's right to life is guaranteed under the Constitution of the Federal Republic of Nigeria, 1999. This right is subject to certain exceptions, such as self defence, defence of property and in execution of court sentence particularly in capital offences.

Right to Dignity of Human Person: No human being should be treated as less than one. Every human is guaranteed his or her right to the dignity of human person. This right stipulates that no

²⁷ Section 33

human shall be subjected to any inhuman or degrading treatment, held in slavery or servitude and not required to perform forced or compulsory labour.²⁸

Right to Personal Liberty: Section 35 of the Constitution provides that no person shall be denied of his right to personal liberty except in execution of a court order or sentence, where the person is a minor for his welfare or education, where the individual is held on health grounds and so on.

Right to Fair Hearing: Section 36 guarantees that individuals have the right to a just and timely trial by a legally established court or tribunal that is independent and unbiased in deciding their civil rights and obligations, including any matters involving government or authority.

Right to Privacy: The right to privacy of every person is guaranteed by Section 37 of the Constitution. The Section provides that ‘the privacy of citizens, their homes, correspondence, telephone conversations and telegraphic communications is hereby guaranteed and protected.’

Right to Freedom of Thought, Conscience, and Religion: According to Section 38, every individual has the right to freedom of thought, conscience, and religion. This includes the ability to change one's religion or belief and the ability to publicly and privately express one's religion or belief through acts of worship, instruction, practise, and observance.

Right to Freedom of Expression and the Press: According to Section 39, everyone has the right to freedom of speech, which includes the ability to express beliefs and the unhindered reception and dissemination of ideas and information. The right to privacy of internet users will be the main topic of discussion in this article.

Right to Peaceful Assembly and Association: According to Section 40, everyone has the right to peaceful assembly and association with others. In particular, he is free to create or join a political party, trade union, or other organisation to further his interests.

Right to Freedom of Movement: Every citizen of Nigeria has the right to live anywhere in the country and to travel about freely by virtue of Section 41 of the constitution. Every Nigerian citizen is protected from discrimination on the basis of sex, race, ethnicity, religion, political opinion, or place of origin under Section 42. Finally, according to Section 43 of the Nigerian

²⁸ Section 34(1) of the CFRN however provides for certain cases where this right may be subjected to exceptions: labour in execution of court sentence; labour required for members of the armed forces or the Nigerian Police Force and so on.

Constitution, every Nigerian citizen has the right to purchase and possess real estate anywhere in the country.

Right to protection of personal data is also classified as fundamental human right under the right to privacy²⁹. Meanwhile, African Union Convention on Cyber Security and Personal Data Protection (Malabo Convention) provided a robust frame work for cyber security and personal data protection in Africa. Thus, it can be regarded as one of the laws with intersect on human right and cyberspace. In the same vein, European Union's General Data Protection Regulation (GDPR) is also one of the laws in the world that intersect cyberspace and fundamental human right. It must be noted that the law is limited to European countries member states. Some countries of the world like Canada, United States of America, India, among others are also developing Net Neutrality Policies that regulates the services of Internet Service Providers on discriminating against certain users sects and giving all the users equal opportunities and platform³⁰.

3.1 ICT and Human Right Abuses

It is not far-fetched that certain activities on the cyber space can constitute abuse of fundamental human rights. The activities that appear to be more prevalent in the digital era are discussed below:

3.1.1 Right to Dignity of Human Person

Human trafficking is a type of contemporary slavery that is mostly perpetrated with the use of internet. There are four stages to human trafficking and they are recruitment, transportation, victim exploitation, and management of illegal profits.³¹ Offenders use digital technologies at each of these four stages of the trafficking cycle. These digital technologies help them carry out their business and take advantage of more victims. Traffickers have taken advantage of technological advancements in recent years to further their exploitation of their victims.³² At the end, the unsuspecting victims are subjected to forced labor, sexual exploitation and other activities that are demeaning. Victims are often deprived of their liberty and forced into

²⁹ Article 8 EU Charter of Fundamental Rights

³⁰ Net neutrality (2023) https://en.wikipedia.org/wiki/Net_neutrality#:~:text=Net%20neutrality%20is%20the%20principle,giving%20preference%20to%20any%20content. accessed 30 September 2023

³¹ YG Zabyelina, 'Human Trafficking, Human Misery: The Global Trade in Human Beings, 1st Ed., by Alexis A. Aronowitz' (2013) 14 Global Crime 113

³² S Raets and J Janssens, 'Trafficking and Technology: Exploring the Role of Digital Communication Technologies in the Belgian Human Trafficking Business' (2019) 27 European Journal on Criminal Policy and Research 215

servitude, this directly violates their right to personal freedom and security. Trafficking robs victims of their inherent dignity by subjecting them to abusive and exploitative conditions. . Some of the scenarios and case studies related to human trafficking and technology around the globe are discussed in this section.

A Bulgarian man was accused by the US Department of Justice of using social media to lure victims to the US and traffic them there in 2018. The man approached young women on social media using fictitious identities and offered them employment or scholarships in the US. The man would arrange for the ladies to be trafficked and coerced into prostitution after they gave their consent to go to the United States. The man was ultimately found guilty of human trafficking and given a 24-year prison term.³³

In 2019, the Nigerian National Agency for the Prohibition of Trafficking in Persons (NAPTIP) lrescued a 16-year-old girl who had been trafficked to Libya and forced to work as a prostitute. A trafficker recruited the girl after meeting her on a social networking site. The trafficker offered the girl a job in Libya, but when she arrived, she was forced into prostitution. After the trafficker was apprehended and punished, the girl was eventually returned to Nigeria.³⁴.

3.1.2 Abuse of Right to Privacy

Privacy is a fundamental right that is deeply intertwined with cyberspace. The digital age has brought about a surge in data collection and surveillance, often without individuals; consent. Governments, corporations, and hackers can potentially infringe upon our privacy by accessing personal data. Right to privacy in the simplest form can be defined as right against unwarranted interference to one's private affairs. The concept of the "right to be left alone" has been expanded to grant individuals a certain level of authority over their personal information, including records maintained by educational institutions, employers, credit reporting agencies, and governmental entities.³⁵ Nevertheless, these rights are particularly vulnerable to violation due to significant advancements in technology, which have expanded the capabilities of both governments and

³³Mail Online, 'Bulgarian People Trafficking Gang Jailed for a Total of 24 Years' (*Daily Mail Online*, 18 October 2019) <<https://www.dailymail.co.uk/news/article-7587923/Bulgarian-people-trafficking-gang-jailed-total-24-years.html>> accessed 9 October 2023

³⁴'How I Lost My Virginitly to Trafficking – Naptip Ambassador' (*Daily Trust*, 14 January 2023) <<https://dailytrust.com/how-i-lost-my-virginitly-to-trafficking-naptip-ambassador/>> accessed 9 October 2023

³⁵B. Smentkowski, 'Rights of Privacy' (2023). <<https://www.britannica.com/biography/William-Joseph-Brennan-Jr>>. accessed 30 September 2023

private entities to engage in surveillance, decryption, and large-scale data collecting. These activities have the potential to greatly infringe upon individuals' right to privacy.³⁶

Certain cyber activities constitute breach of fundamental human right to privacy. Some of them are doxxing³⁷, stalking³⁸, spamming³⁹, etc. In *Emerging Market Telecommunication Services V Barr Godfrey Nya Eneye*⁴⁰ Court of Appeal held that “unsolicited messages constitute infringement of the respondent’s right to privacy”. The Court held that “...unknown persons and organizations access to the respondent’s Etisalat GSM phone number to send unsolicited text messages into it, amount to violation of the respondent’s right to privacy guaranteed by Section 37 of the Constitution which includes the right to the privacy of a personal’s telephone line⁴¹”

3.1.3 Protection against the Compulsory Acquisition of Property (Section 44)

The cyberspace has opened up numerous avenues through which fundamental human rights can be breached. Several cases of online fraudulent activities have been reported in which unsuspecting persons have been defrauded of their properties and money.

3.1.4 Abuse of Freedom of Expression

Freedom of expression is a crucial fundamental right in cyberspace. The internet has democratized information dissemination, allowing individuals to share their thoughts, ideas, and opinions on a global scale. It has revolutionized the way we communicate and share ideas, opening up endless possibilities for expression and creativity. Social media platforms, blogs, and forums provide a space for anyone to express themselves. However, this right is not without its challenges. Online censorship, surveillance, and the spread of misinformation pose significant threats to freedom of expression. The challenge lies in balancing the right to freedom of expression with concerns like hate speech, disinformation, and online harassment. Striking a balance between free expression and responsible speech is a daunting task for lawmakers and internet platforms alike.

³⁶ The right to privacy in the digital age (2013). <<https://www.ohchr.org/en/stories/2013/10/right-privacy-digital-age>>accessed 30 September 2023

³⁷ This is illegal sharing of private information of someone without consent, thus exposing the person to danger/harm.

³⁸ This is an act of monitoring a social media presence of someone without their consent.

³⁹ This means sending unsolicited messages in bulk.

⁴⁰ 2018 LPELR- 46193 (CA) at 26

⁴¹T.A.M., ‘Data Protection: Whatsapp Privacy policy Changes and their Primary Consent under Nigeria Data Protection Regulatory Framework’ (2021) 11Nigerian Bar Journal 2

3.1.5 ICT and the Protection of Fundamental Rights

Technology is a two-edged sword with benefits and advantages on one side and risks and threats to users and stakeholders on the other is universally acknowledged.⁴² Our attention in this regards shall be on how the fundamental right can be protected using cyberspace. The ICT sector significantly contributes to the promotion of Human Rights, stimulation of economic growth, enhancement of aspects such as quality of life, education accessibility, environmental preservation, and facilitation of the information society's advancement.

Introduction of digital facilities will help in curbing and enforcing the abuse of dignity of human person by the police force and other security agencies. Section 234 of the Administration of Criminal justice Act has mandated the use of ICT facilities in recording of confessional statements of the accused persons. This will help a lot of proving, ensuring transparency and identification of perpetrators of fundamental human rights abuse. It must be noted that Fundamental Human Rights becomes enforceable when the rights of the victim has been breached, it is being breached or there is likelihood that the right will be breached⁴³.

The internet has democratized and helped access to knowledge, empowering individuals around the world with unprecedented opportunities for education and self-improvement. The internet provides vast amounts of information at one's fingertips, empowering individuals with knowledge about their rights and how to exercise and protect them. Cyberspace gives voice to the voiceless. Social media platforms, blogs, and online publishing enable users globally to express their views, share their stories, and advocate for causes they believe in⁴⁴.

4.0 Summary of Findings and Conclusion

Legislations on cybercrime in Nigeria recognize that corporations are capable of committing and can be held liable for crimes committed in cyberspace. A look at Nigerian legislations on use of the cyberspace shows that those legislations are reactive. Legislations in other jurisdictions such as the United Kingdom and the United States of America are more preventive. There is a jurisprudential gap on the cyberspace in Nigeria.

⁴²RE Floyd, 'Technology-A Two-Edged Sword' (2018) 37(2) IEEE Potentials 8

⁴³ Section 46, 1999 Constitution (As Amended)

⁴⁴Susana Gallego 'Impact of ICT on Human Rights' (2013) < <https://www.telefonica.com/en/communication-room/blog/impact-of-ict-on-human-rights/> >accessed 30 September 2023

It has been pointed out in the course of this paper that the cyberspace is an extension of territorial space with human beings as its major active proponents. There is no doubting the fact that the cyberspace, which is constantly and rapidly developing, is the future. This is why there are laws to regulate the cyberspace. Nonetheless, these laws and their makers more often than not ignore the rights of users of this space. This is indeed the case mainly because of the evils constantly being perpetrated by some users of the internet.

However, protecting rights of humans, either they are users of the cyberspace or not, trumps any need for enforcement and regulation. Thus, a reasonable balance must be struck by legislators, human rights organizations and other stakeholders in regulating the cyberspace and also protecting inalienable rights of human beings in the society.

5.0 Recommendations

In view of all the issues raised in this paper on human rights in the cyberspace, the following recommendations are proposed:

- a. There is a need for enhanced education among both natural and juristic users on the utilisation of cyberspace and its broader societal implications. Many individuals perceive cyberspace as a lawless place where unrestricted actions can be undertaken, sometimes overlooking the societal implications of such behaviour.
- b. It is imperative that regulators enhance their understanding of the necessity to safeguard the rights of users in the internet, akin to the protection afforded in the territorial realm.
- c. Authorities involved in law enforcement ought to receive enhanced training, resources, and financial support in order to effectively address the escalating threat.
- d. Promoting inter-agency and international collaboration is crucial for addressing cybercrimes, particularly those involving multinational organisations.