journals.unizik.edu.ng/jcpl/index ISSN: 2736-0342
NNAMDI AZIKIWE UNIVERSITY, AWKA
JOURNAL OF COMMERCIAL AND PROPERTY LAW Vol. 12(3), July, 2025

SECURING HUMAN RIGHTS IN CYBERSPACE: IN THE LIGHT OF THE CYBERIZATION OF OWNERSHIP, TRADE, AND ECONOMIC RIGHTS

Kenekayoro .T. Peter*

Abstract

This research adopts the black letter methodology in assessing the exercise of, and protection of human rights in *cyberspace. The exercise of rights in cyberspace is a consequence of the cyberization process spearheaded by the Fourth Industrial Revolution. Consequently, the adoption of various aspects of reality, into digitalized formats, has not only created another dimension for transacting, executing rights, and performing economic, political and social functions; it has correlatively created a new epicenter for criminal acts and abusive practices. On that account, the State's responsibility to protect, now possesses a cyber-dimension that is jurisprudentially embodied in cyber laws and cyber security regulations. Thus, this research adopts a five-paradigm approach for assessing security concerns as well as the exercise of rights in cyberspace. Hence, emphasis is placed on the protection of ownership and exclusive rights; ensuring the legality of activities executed on cyber platforms as well as the proscription of criminality; the legitimacy of administrative activities executed on the internet; ensuring the functionality of cyber platforms; and right to access in cyberspace. Reference is also made to the economic dimension of cyber-security. Thereby urging States to take unilateral and multilateral steps towards guaranteeing human rights in cyberspace. This research also emphasizes on the imperativeness of ensuring that cyber laws and regulatory strategies adopted by governments are pragmatic and advanced enough, to cope with, or to tackle the challenges, complexity, efficiency, progress and accelerated development of cyber-technology.*

Keywords: Rights, cyberspace, economic, security, crime

1. Introduction

Human rights are legal entitlements, and fundamental freedoms of the human person.[1] From the historical recognition of the natural rights theory, to more contemporary recognitions of human rights under the aegis of international and national institutional frameworks, rights have often been address in the context of concomitant duties.[2] Thus, human rights became the premise of states responsibility to respect, and protect; as well as the aspirational basis for maintaining law and order in the world.[3] Thus, rights not only involve liberties or freedoms, they correlatively necessitate regulations, to curb disruptive, destructive, and abusive actions that procure the violation of rights.[4] Consequently, the paradox of human rights law is that it guarantees, as well as limits human rights, on the basis of legitimate objectives.[5] So human rights inexorably procure correlative expectations on states and the society in general to provide satisfactory conditions, and an enabling environment for persons to exercise their liberties for the execution of autonomous actions, undertakings, and individual projects.[6]

The aforementioned state of affairs is not limited to physical reality, because the social and economic dynamics of physical reality are adopted and engineered into formats that are replicable within digital

***Kenekayoro .T. Peter,** Lecturer, at Faculty of Law, University of Africa. Toru-Orua, Bayelsa State, Nigeria. E-mail: Kenekayoroxoxo@gmail.com. Phone No: 08054813928

[1] Articles 2, 3 and 4 of the African Charter on Human and Peoples' Rights (Ratification and Enforcement) Act Chapter A9 (Chapter 10 LFN 1990) (No 2 of 1983) Laws of the Federation of Nigeria 1990

[2] BH Weston, 'Human Rights' [1984] 6(3) *Human Rights Quarterly* 258; LC Ledlie, 'Ulpian' [1903] 5(1) *Journal of the Society of Comparative Legislation* 22; R William, 'Hugo Grotius' [1905] 6(1) *Journal of the Society of Comparative Legislation* 77; J Rehman, *International human rights law* (2nd edn, London: Pearson, 2010) 8

[3] A Peters, 'Corruption as a Violation of International Human Rights' [2019] Vol. 29(4) The European Journal of International Law 1258; JT Gathii, Defining the Relationship between Human Rights and Corruption. [2009] Vol. 31(1) *U. Pa. J. Int'l L.* 127; LL Fuller, *The Morality of Law* (2nd ed. Yale University Press: Virginia 1964) 6, 10, 11

[4] Article 29(2) of the Universal Declaration of Human Rights Adopted and proclaimed by General Assembly resolution 217 A (III) of 10 December 1948

[5] BH Weston, 'Human Rights' [1984] 6(3) *Human Rights Quarterly* 263

[6] African Charter on Human and Peoples' Rights (Ratification and Enforcement) Act, Article 1 and 27

spheres in the cyberspace.[7] Just as the First Industrial Revolution caused rapid urbanization that made industrial hubs the new epicenter of social and economic exchanges; the Fourth Industrial Revolution is progressively creating a new epicenter, characterized by digitalization.[8] Thus, the cyberspace is the new digital hub, where social and economic exchanges are executed all over the world, within a borderless space. Consequently, a wide range of human rights are exercised/executed digitally. On that account, the exercise of human rights in a cyber-setting is bound to create the same needs and rights-oriented guarantees that are required to enable persons exercise their rights, and to advance their legitimate interests within a secure space. That is the basis of these two issues of interest –

(1.) How can human rights be guaranteed, and securely exercised on the cyberspace? and

(2.) What are key considerations to be adopted, in the context of a paradigmatic approach to human rights in cyberspace? Or in other words, what are the cyber rights of netizens?

2. Cyberspace

The cyberspace is a service oriented, transactional, and digitalized platform, meant for engineering specific kinds or experiences, or for enabling the efficacious execution of designated tasks, in a cyber-environment where humans act and communicate through software;[9] Software which are programmed and engineered to operate within computers or other smart devices. Thus, the crux of the cyberspace as identified by the College of Engineering and Technology (MRCET), is the interplay between 'people, software, and services.'[10] The cyberspace is utilized by all facets of society including businesses, organizations, governments, clubs and associations, religious sects, regional, sub-regional and global institutions, individuals and ideological movements. Owing to its developmental nature, the cyberspace is bound to become more complex as technology progresses.[11] According to Ajiji, the cyberspace is synonymous to the internet.[12] Nonetheless, it encompasses all digital platforms in which humans communicate and execute actions through software.

3. The Modernization of Security

Security is the consequence of an efficacious or successful act of protecting a space, a person or people. It involves the practice of organizing an efficacious framework for protection, through active, proactive, or reactive measures that are suited to the demands or exigencies of a situation. Hamourtziadou conceptualizes freedom as the guaranteed exercise of one's rights. He further emphasizes that the primary purpose of security is the protection of fundamental or basic human rights.[13] On that account, security is an indispensable requirement for ensuring the respect for, as well as the fulfilment of rights. Thus, the duty to protect, is what creates a vital link between human rights and security. Thereby, making them mutually reinforcing, due to the recognition of 'the ethical and political importance of securing the holders' of human rights and fundamental freedoms.[14]

Hamourtziadou also adopts human rights as a frame of reference for defining security: So he explained the modern concept of security to mean the successful and progressive practice of protecting the rights and liberties of the human person.[15] Based on that analogy, he further notes that the imperativeness of

---

[7] J Bishop, All's well that ends well: A Comparative Analysis of the Constitutional and Administrative Frameworks of the Cyberspace and United Kingdom [2012] <https://pdfs.semanticscholar.org/2954/5a5995e33b7c768e24a1e80d7a2cd956b023.pdf p.254> Accessed May, 4, 2025 254

[8] X Min, M Jeanne, M., and S Hi, The Fourth Industrial Revolution: Opportunities and Challenges [2018] Vol. 9(2) *International Journal of Financial Research* 90

[9] MRCET, Digital Notes on Cyber Security [2020] <https://mrcet.com/pdf/Lab%20Manuals/IT/CYBER%20SECURITY%20(R18A0521).pdf> Accessed May, 4, 2025 19

[10] ibid

[11] ibid

[12] YM Ajiji, 'Cyber Security Issues in Nigeria and Challenges' [2017] 7(4) *International Journal of Advanced Research in Computer Science and Software Engineering* 315

[13] L Hamourtziadou, 'Security challenges of the 21st century: new challenges and perspectives' [2019] 6(2) *Journal of Global Faultlines* 121

[14] ibid

[15] Ibid; AI Sadykova1, AP Sokolov, RA Rutskoi et al, Economic Security as a Tool for Ensuring National Economic Development [2023] <https://www.shsconferences.org/articles/shsconf/pdf/2023/13/shsconf_cildiah2023_00121.pdf> Accessed May, 4, 2025 1, 2

securing the exercise of all classes of rights, procures a new dimension of what constitutes a threat.[16] Consequently, a threat is not solely what is potentially ruinous to the civil rights of the individual, it is rather a multidimensional phenomenon that expresses itself in various ways, but with the one rigid and common feature of being a potential danger to the rights and liberties of a person. Therefore, security threats are not limited to physical acts of aggression.[17]

3.1 Economic Security

The International Committee of the Red Cross (ICRC) recognizes the economic dimension of security. The ICRC relates economic security to a state of existence in which, individuals or collectives are capable of sustainably catering for their 'essential needs and unavoidable expenditures' amidst their current socio-cultural and environmental conditions with due regard to the level of psychological, human capital, and financial wherewithal required to survive or thrive in such circumstances.[18] Economic security has been linked to sustainability, as well as progress. Thus, it is related to a stable state of affairs, and positive outcomes such as economic growth, price stability, affordable costs of living, an adequate standard of living, the integrity of the market, access to economic opportunities and adequate sources of livelihood, a supportive public policy and institutional framework for stimulating economic progress,[19] as well as an efficacious framework for detecting and neutralizing threats, and for proper management/limitation of the ramifications of adverse situations.[20]

Economic security is a vital issue of interest, not only physically, but also on the internet – which is an integral part of the economy and livelihood of people all over the world, who leverage the economies of scale afforded by the cyberspace, to supply goods and services; and for the execution of other related transactions that need to be executed securely and effectively, without threats to the integrity of such transactions.

3.2 Cybersecurity

Cybersecurity is centered on the formulation, adoption, implementation, or enforcement of measures aimed at neutralizing security threats on the cyberspace.[21] The process of securing the cyberspace involves a wide range of activities including 'computer network operations, information assurance, law enforcement', administrative regulations, access management, data protection, privacy restrictions, conditional access, identity authentication, preventive measures, 'threat reduction, international engagement' and collaborative arrangements aimed at guaranteeing safety and security within the cyberspace.[22]

The College of Engineering and Technology (MRCET) defines cybersecurity, as 'the body of technologies, processes, and practices designed to protect networks, computers, programmes and data from attack, damage, or unauthorized access.'[23] So in-line with MRCET's definition, cyber security can be explained as the digitalization of security, and its operationality within digital spheres of influence, with the aim of ensuring safety and integrity. Thus, it inevitably involves the adoption of security strategies and principles from physical reality, and transforming them into guiding principles for protecting and regulating the realm of virtual reality, internet spaces, or other cyber platforms. That is a feat that is achieved through the interpretation and application of security principles and strategies, in a way that ensures their functionality and adaptability to the demands and nuances of the cyberspace.

---

[16] Ibid; ICRC, Economic Security [2013] <https://www.icrc.org/sites/default/files/topic/file_plus_list/economic-security-delegate.pdf> Accessed May, 4, 2025 2

[17] Hamourtziadou 'n 13'

[18] ICRC 'n 16'

[19] See Section 16

[20] AI Sadykova1, AP Sokolov, RA Rutskoi et al, Economic Security as a Tool for Ensuring National Economic Development [2023] <https://www.shsconferences.org/articles/shsconf/pdf/2023/13/shsconf_cildiah2023_00121.pdf> Accessed May, 4, 2025 1, 2

[21] MRCET, Digital Notes on Cyber Security [2020] <https://mrcet.com/pdf/Lab%20Manuals/IT/CYBER%20SECURITY%20(R18A0521).pdf> Accessed May, 4, 2025 5 ibid

[22] ibid

[23] ibid

4. Cybercrime

Simplistically, cybercrime is the execution of criminal activities, via the internet or through other cyber platforms. For example, the first reported case of cyber murder was committed in the United States of America, through the alteration of prescriptions via the hacking of a hospitals computer system.[24] That consequently sabotaged a minor surgery process, and led to a casualty. That exemplifies how a cyber-security threat can lead to the violation of the right to health, and concomitantly, the right to life, which are rights guaranteed under the International Covenant on Civil and Political Rights (ICCPR),[25] and International Covenant on Economic, Social and Cultural Rights (ICESCR).[26]

The rising rate of cybercrime is a negative development that is thriving partly as a result of the anonymity afforded by internet platforms, which makes tracking criminals more difficult. Other factors frustrating the fight against cybercrime includes the swift and dynamic nature of online transactions, which reduces the possibility of effective tracking; 'lack of functional databases' especially in African countries that have weak institutions, which are plagued by substandard systemic practices, and record keeping problems.[27] Ajiji notes that 'it will always be a loosing battle if security professionals are way behind the cyber criminals in terms of technological knowledge.'[28]

4.1 The Cybercrimes (Prohibition and Prevention) Act, 2015

The Cybercrimes (Prohibition and Prevention) Act (CCPPA) is a Nigerian legislation, aimed at creating a legal, regulatory, and institutional framework for the effective prevention, prohibition, prosecution and punishment of cybercrimes.[29] In order to guarantee cyber security, the CCPPA attempts to regulate cybercafés by ordering their mandatory registration with the Corporate Affairs Commission, and with the Computer Professionals' Registration Council.[30] It also mandates the maintenance of a compulsory register, which contains the details and signature of users, and its availability to law enforcement officers on demand, for investigative purposes.[31] The CCPPA prohibits a wide range of offences, including the interception of electronic messages and transactions, unlawful system interferences, tampering with software infrastructure, intentional acts of misdirecting electronic messages, unlawful interceptions, computer related forgery, theft, unauthorized modifications, cyber terrorism, identity theft, etc.[32]

4.2 Human Rights and Cybersecurity

Human rights has progressed over the years, as a consequence of which the divisionary lines that separate different classes of rights has been blurred due to the dominant view of interdependency and indivisibility of rights.[33] In the same vein, even the concept of security has evolved from the realm of solely preventing physical harm, to broader socio-economic dimensions.[34] Hence, the economic and social factors which enable the human person to execute his legitimate aspirations must be secured and protected by law.[35] The most popular theme of publications on the cyberspace is the issue of security. Shailendra defines cyber law as 'the law governing the digital world' – in the context of 'security and

---

[24] YM Ajiji, 'Cyber Security Issues in Nigeria and Challenges' [2017] 7(4) *International Journal of Advanced Research in Computer Science and Software Engineering* 315

[25] Article 6(1) of the ICCPR

[26] Article 12(1) of the ICESCR

[27] YM Ajiji, 'Cyber Security Issues in Nigeria and Challenges' [2017] 7(4) *International Journal of Advanced Research in Computer Science and Software Engineering* 315

[28] ibid 318

[29] Section 1 of the Cyber Crimes (Prohibition and Prevention) Act, 2015

[30] ibid Section 7

[31] ibid Section 7

[32] ibid Section 8 - 18

[33] V Frans, 'Africa's Contribution to the Development of International Human Rights and Humanitarian Law' [2001] Vol. 1 *African Human Rights Law Journal* 20; J Rehman, *International human rights law* (2nd edn, London: Pearson, 2010) 9; AJ Schlesinger, 'Origins of the Cold War' [1967] Vol. 46(1) *Foreign Affairs* 38

[34] P Chigora, 'The Challenges Facing African Union in Achieving Continental Security: Towards a Comprehensive Analysis of Some Enlightening Views at the New Millennium' [2008] 10 (1) *Journal of Sustainable Development in Africa* 70

[35] AA Joy, 'Post-Colonial Colonialism: An Analysis of International Factors and Actors Marring African Socio-Economic and Political Development' [2010] Vol. 3(10) *The Journal of Pan African Studies* 67; C Percyslage, 'Facing African Union in Achieving Continental Security: Towards a Comprehensive Analysis of some Enlightening Views at the New Millennium' [2008] Vol. 10(1) *Journal of Sustainable Development in Africa* 70

privacy of information; and crimes relating to damages'[36] On that account, cyber law is a tool for maintaining cyber security, and for deterring criminal activities, which concomitantly undermine human rights.[37] Nonetheless, Singh and others have identified factors that undermine cyber security:

(1.) According to Singh, a major problem is the inadequacy of existing laws, specifically in the area of adapting existing legal principles to suit the exigencies of the cyberspace; and the lack of sufficient judicial precedents to guide the decisions of the court in regard to issues concerning the cyberspace.[38]

(2.) Singh considers the issue of privacy as another hurdle which constrains the authority of investigative agencies, and hampers their capacity to access and gather relevant information and evidences for the effective prosecution of cases.[39]

(3.) Singh also points out an existing deficit in the popular legitimacy of law enforcement authorities – Consequently, there is a sense of distrust, existing between law enforcement agencies and computer professionals, and also netizens that hinders effective collaboration in the area of cyber security.[40]

(4.) Pandey et al explains that one problem procured by the novel nature of the cyberspace, is the lack of firm boundaries in regard to what constitutes criminality in the context of the cyberspace.[41] So the amorphous nature of certain cybercrimes[42] makes it difficult for IT professionals to detect when it is necessary to report such activities to law enforcement agencies.[43]

(5.) The jurisdictional complication, in the sense that the cyberspace is global, however, crime is relativistic, because the content of criminal legislation is jurisdictionally defined. Thus, a crime in one country, maybe a legal act in another.

(6.) The anonymity afforded by the cyberspace gives criminals the privilege of perpetrating criminality with a low possibility of being exposed.

(7.) The proliferation of viruses that alter the integrity of computer software.

5. Cases on Cybercrime and Cybersecurity

The Pune Citibank Mphasis Call Center Fraud,[44] is a case of sourcing engineering, in which employees who gained the confidence of customers, obtained their PIN numbers, under the guise of helping customers in difficult situations, which they probably could not solve without expert assistance. However, the PIN numbers were rather used for the purpose of committing fraud: '$350,000 from accounts of four US customers were dishonestly transferred to bogus accounts.'[45] Although, in this case the administration set up a thorough system to curtail such malpractices, yet the perpetrators came up with innovative ways to circumvent the proactive security measures implemented by Mphasis. Nevertheless, the complaints of the customers were effectively addressed because all the transactions were executed with Pune accounts, which made it easier to trace the perpetrators of the crime.[46] Consequently, the accounts of the perpetrators were frozen. The court held that the case falls within the purview of cybercrime, as the crime involved unauthorized access of electronic accounts, contrary to the Information Technology Act, 2000.[47]

---

[36] G Shailendra, 'Cyber Crime, Cyber Threat, Cyber Security Strategies and Cyber Law in Nepal' [2019] Vol. 9(3) *Pramana Research Journal* 663

[37] T Singh, 'Cyber Law & Information Technology' [2007] <https://delhidistrictcourts.nic.in/ejournals/CYBER%20LAW.pdf> Accessed 13th May, 2024 1

[38] See T Singh, ibid 1

[39] ibid

[40] ibid

[41] US Pandey, K Verinder, and PS Harman, *Cyber Crimes and Laws* (Mumbai: Himalaya Publishing House Pvt. Ltd. 1st ed. 2017) 2

[42] See T Singh, 'Cyber Law & Information Technology' [2007] <https://delhidistrictcourts.nic.in/ejournals/CYBER%20LAW.pdf> Accessed 13th May, 2024 2

[43] ibid

[44] Lawful Legal, *Pune Citibank Mphasis Call Centre Fraud Case* [2024] <https://lawfullegal.in/pune-citibank-mphasis-call-centre-fraud-case/?amp=1> accessed on 2nd June, 2025

[45] T Singh, 'Cyber Law & Information Technology' [2007] <https://delhidistrictcourts.nic.in/ejournals/CYBER%20LAW.pdf> Accessed 13th May, 2024 7

[46] 'n 44'

[47] ibid

Tamil Nadu v Suhas Katti,[48] involved posting of obscene and defamatory massages about a divorcee woman in a yahoo message group; and the creation of a false e-mail account opened in the name of the victim, to serve as an avenue for obtaining private information. The accused was found guilty of violating sections 469, and 509 of the Indian Penal Code, and 67 of the Information Technology Act, 2000.[49]

In the case of *National Association of Software and Service Companies (Nasscom) v Ajay Sood & Others*,[50] the Delhi High Court, confirmed the illegality of 'phishing on the internet', thereby granting an injunction and recovery of damages.[51] The unique fact about the case is that although no specific legislation criminalized the act of phishing under Indian law, the court defined its illegality in the context of fraudulent misrepresentation, and exposing the victim to immense harm based on the possibility of using names, identities, and passwords for unlawful or unauthorized purposes.[52] Thus, 'the court held the act of phishing as passing off and tarnishing the plaintiff's image.'[53]

6. The Regulatory Dynamics of the Cyberspace

Johnathan Bishop, alluded to the dichotomy between the jurisdictional nature of constitutional and administrative law, and the internet which is 'a world without forties.'[54] In the same line of thought, John Perry Barrow has questioned the normative legitimacy of nation-states imposing laws on the virtual, and borderless cyberspace.[55] Nevertheless, the authoritative force of the state, which is based on an all-encompassing responsibility to maintain law and order, tilts the argument in the favour of public administrative systems/institutions of the government; considering that by virtue of legislative actions at the state level, and intergovernmental cooperation at regional and global administrative levels, there are national and international laws regulating the internet.

The reason-centric nature of laws as alluded to by Cicero, St. Paul, and St. Thomas Aquinas;[56] the universal ethics of human rights jurisprudence as recognized by Maurice Cranston;[57] and the normative value of Jus Cogens and preemptory norms of international law verifies that there are fundamental and inviolable principles of law, which are universally applicable.[58] Thus, legal principles are relevant and simultaneously applicable – in the real world, and on the cyberspace.

Johnathan Bishop, pointed out the existence of commonalities between the real world, and the cyberspace, for instance 'there are commonalities in the way they function.'[59] Thus, commonality in function, correlatively implies commonality of regulatory norms (laws) to ensure legality and proper functionality of specific spheres of influence/jurisdictions of activity.[60]

---

[48] C No. 4680 of 2004

[49] Indian Law Portal, *Suhas Katti v. State of Tamil Nadu* [2021] <https://indianlawportal.co.in/suhas-katti-v-state-of-tamil-nadu/> Accessed May 25, 2023

[50] See Indian Cyber Security, *Nasscom v. Ajay Sood & Ors*. [2013] <https://www.indiancybersecurity.com/case_study_nasscom_ajay_sood.php> Accessed May 23, 2025

T Singh, 'Cyber Law & Information Technology' [2007] <https://delhidistrictcourts.nic.in/ejournals/CYBER%20LAW.pdf> Accessed 13th May, 2024 13

[51] ibid

[52] ibid

[53] ibid

[54] J Bishop, All's well that ends well: A Comparative Analysis of the Constitutional and Administrative Frameworks of the Cyberspace and United Kingdom [2012] <https://pdfs.semanticscholar.org/2954/5a5995e33b7c768e24a1e80d7a2cd956b023.pdf p.254> Accessed May, 4, 2025 254

[55] ibid

[56] P Gasiokwu, 'State, Law and the Challenges of Good Governance: Law, Politics and Diplomacy in Contemporary Nigeria' [2010] <https://www.researchgate.net/publication/342277563> Accessed 21 April 2025 250

[57] M Cranston, *What are Human Rights* (1st edn. London: The Bodly Head) 23

[58] Gasiokwu 'n 56'; J Rehman, *International human rights law* (2nd edn, London: Pearson, 2010) 30

[59] 'n 54'

[60] ibid

6.1 A Five Paradigm Approach to Human Rights on the Cyberspace

The legal regulation of the cyberspace, and the human rights concerns in regard to ethics and economic considerations, can be explained in the context of four key paradigms, viz. ownership, legality, legitimacy, functionality, and accessibility.

(1.) Ownership

Ownership is an elevated right, in the sense that ownership accords privilege or exclusivity to owners or title holders, to the exclusion of all other persons, for instance: legal property rights under land law, commercial property rights under sale of goods law, and intellectual property rights under Trade Related Aspects of Intellectual Property (TRIPS) and copyright law.[61] Ownership rights also apply to the cyberspace, in regard to the ownership of exclusive copyrights,[62] websites, web pages, and social media accounts, which in a general sense affords the web-owners and users, the prerogative right to control, regulate, and administer the affairs of their pages and websites. Ownership rights on the cyberspace can be acquired by:

(a.) Creating a website;
(b.) Purchasing a website;
(c.) Creating a private or business account on an already existing website;
(d.) Renting a space on a website, by virtue of periodic subscriptions; and
(e.) Gaining exclusivity in-line with trade-marks,[63] copyright laws, or other related rights.

Thus, in the context of the cyberspace, ownership guarantees freedom to carry out any legal act, transaction, or function on a website, and to benefit commercially by virtue of exclusive ownership rights. In *Chinda v Amadi*,[64] it was held that 'acts of ownership are derivative from the ownership. Ownership forms the quo warranto of those acts as it gives legality to the acts which would have otherwise been' a trespass or a breach of the rights of others.[65] Section 1(c) of the Cyber Crimes (Prohibition and Prevention) Act, 2015 (CCPPA) is aimed at protecting intellectual property and privacy rights. Section 25(1) of the CCPPA, states that –

> *Any person who, intentionally takes or makes use of a name, business name, trademark, domain name or other word or phrase registered, owned or in use by any individual, body corporate or belonging to either the Federal, State or Local Governments in Nigeria, on the internet or any other computer network, without authority or right, and for the purpose of interfering with their use by the owner, registrant or legitimate prior user, commits an offence.*

(2.) Legality

All activities carried out on the cyberspace are expected to be lawful. Hence, there are limitations to the exercise of ownership rights and freedoms on the internet. As earlier noted, the cyberspace cannot be divorced from society. Consequently, all acts which are criminalized by statutory law, are also by extension – prohibited on the cyberspace, and liable to the sanctions prescribed by criminal legislations, for instance, fraud, libel, mobilizing terrorism, identity theft, forgery, and other crimes, which can be executed on the cyberspace or internet.

Section 6(1) of the CCPPA prohibits the orchestration of unauthorized access to computer systems, for fraudulent purposes. Section 22 of the CCPPA criminalizes identity theft. Section 23 of the CCPPA criminalizes the electronic distribution of child pornography. Section 24 of the CCPPA prohibits acts of bullying, threatening or harassing other persons, 'where such communication places another person in fear of death, violence or bodily harm.'

---

[61] *Multichoice (Nig.) Ltd. v. M.C.S.N Ltd.Gte.* [2020] 13 NWLR (Pt. 1742) 535, paras. E-F

[62] The right of owners or exclusive licensees to sue for copyright infringements is recognized by Section 16(1) of the Copyright Act. Copyright simply means the 'the right to make copies of a given work.'; *African Songs Ltd v. Adegeye* (2019) 2 NWLR (Pt. 1656) 387 para. B; *Ubom v. Globacom* (Nig.) Ltd. (2025) 6 NWLR (Pt. 1985) 196 paras. C-D

[63] 'A trade mark, if registered, gives its proprietor the exclusive right to use the trademark in in marketing or selling his goods.'; *Ferodo Ltd. v. Ibeto Ind. Ltd.* (2004) 5 NWLR (Pt. 866) 347, paras. D-G

[64] (2002) 7 NWLR (Pt. 767) 505

[65] ibid 523 para. G

(3.) Legitimacy

All regulatory, prohibitive, and administrative actions executed on the cyberspace, are expected to be aimed at executing legitimate objectives, without unethically or unlawfully interfering with the ownership or user rights of other persons. Thus, any act that unjustly or unjustifiably interferes with the user rights of other persons, is inconsistent with the principle of legitimacy. So, there is an implied expectation on web-administrators, as well as users, to act in-line with the terms and conditions regulating the services or activities executed therein. In-line with *Lawan v FRN*,[66] a legitimate action is conceptualized as the practice of adhering to a laid down procedure;[67] which according to practice is usually based on reasonable and objective criteria.[68]

Section 10 of the CCPPA criminalizes acts abuse of office/position, by the staff of private organization or financial institutions, who abuse their privileged access to execute intentional acts of tampering with any critical infrastructure, electronic mails, or to commit 'any act which he is not authorized to do by virtue of his contract of service or intentionally permits' such practices. Section 17(c) of the CCPPA prohibits the forging of electronic signatures for purposes of executing fraudulent acts or other forms of misrepresentation.

(4.) Functionality

The proper functioning of a websites is a necessity for the execution of social and economic exchanges therein. Thus, service providers have a duty to ensure the proper functioning of websites, which they are authorized to manage and administer. While owners or administrators of websites are actively responsible for the efficiency and functionality of their websites; third parties on the other hand, have a passive responsibility, to avoid interfering with the functionality of websites – third parties can interfere with the proper functioning of websites by maliciously spreading computer viruses that cause websites or web pages to malfunction, by hacking accounts, or through other malevolent and intrusive activities. Section 1(c) of the CCPPA is aimed at protecting computer systems and networks, electronic communications, data and computer programs. Section 8 of the CCPPA provides that –

> *Any person who without lawful authority, intentionally or for fraudulent purposes does an act which causes directly or indirectly the serious hindering of the functioning of a computer system by inputting, transmitting, damaging, deleting, deteriorating, altering or suppressing computer data or any other form of interference with the computer system, which prevents the computer system or any part thereof, from functioning in accordance with its intended purpose, commits an offence.*

Section 9 of the CCPPA prohibits the unlawful destruction or abortion of electronic mails, or the sabotage of any functional process through which money or valuable information is being conveyed. Section 16(1) of the CCPPA criminalizes the unlawful and unauthorized act of directly or indirectly modifying any data held in any computer system or network.

(5.) Accessibility

This is one of the most fundamental and controversial issues on the internet today, considering the indispensability of internet access to the execution of socio-political and economic affairs in contemporary society.[69] The principal question in this context is: can there be any justification for barring an individual from major platforms on the cyberspace, considering the economic, social and political ramifications involved? This is a digital era where people transact, trade, communicate, and source information on the internet, so an individual's right to access and existence on the cyberspace is fundamental to achieving success in this digital era of the Fourth Industrial Revolution. Thus, there is a persuasive argument in favour of a guaranteed right to access the cyberspace, which might be subject to the payment of specified subscription fees; and limited for the purpose of prohibiting criminality.

---

[66] (2022) 7 NWLR (Pt. 1829) 322, paras. E-G

[67] ibid

[68] Ibid; *Karnel Singh v Canada* Communication No. 208/1989 para 4.4

[69] BBC News, Twitter 'permanently suspends' Trump's account [8th January, 2021] <https://www.bbc.com/news/world-us-canada-55597840> Accessed 5th June, 2025

Section 40 of the CCPPA alludes to the unethicality of the failure of service providers to perform certain duties. Section 28 of the CCPPA makes reference to the importance of password, access codes for securing the exclusive access of persons to services, experiences and opportunities provided therein.

7. Global Regulatory Cooperation

Due to the jurisdictional and territorial fluidity of the cyberspace and the internet, a state-centric or isolationist approach to regulating the cyberspace might not be the most efficient policy initiative.[70] Thus, multilateralism and regulatory cooperation, through international institutions that are by design – endowed with the capacity to solve 'problems without borders', might serve as an effective platform for regulating and policing the cyberspace.[71] Multilateralism can aid the regulation of the cyberspace through harmonization of policies, and the formulation of pragmatic rules, and means of enforcing litigation judgments.[72]

Thus, if cyber regulatory laws are universal, harmonized, and domestically ratified by countries, the universal enforceability and territorial fluidity of cyber laws, will be made compatible with the borderless nature of the cyberspace. Hence, complaints or court orders can be directed to jurisdiction where enforcement of judgments is most achievable. Nonetheless, the success of such a policy measure will depend on the political will and investment of states in ensuring the success of such global policy objectives.[73] Nevertheless, if existing laws and regulatory principles for policing the cyberspace are implemented and interpreted prudently for example as held in the case of *National Association of Software and Service Companies (Nasscom) v Ajay Sood & Others*,[74] the cyberspace will be more secure.

8. Conclusion

The Fourth Industrial Revolution has fostered the trend of digitalization and the rise of the cyberspace, which has correlatively led to the cyberization of various human rights, which are exercised on the internet or through other digital platforms. The interdependency of human rights and security is the basis of the importance of cybersecurity as a means of guaranteeing the exercise of rights on the cyberspace. In the light of the interconnectedness of all aspects of human life and human endeavor, the reality of the interdependency of rights has been affirmed severally.[75] For example by the preamble of the African Charter on Human and Peoples' Rights, emphasizes that the right to development, as well as 'civil and political rights cannot be dissociated from economic, social and cultural rights in their conception as well as universality and that the satisfaction of economic, social and cultural rights is a guarantee' for the advancement and actualization of civil and political rights. In the same line of thought, Article I (5) of the Vienna Declaration and Programme of Action,[76] emphasizing that 'all human rights are universal, indivisible, interdependent and interrelated.'

Adopting the same approach, the concept of security has correlatively been modernized, and expanded from the erstwhile limited approach, which was centered on threats of violence and physical aggression, to new dimensions that are suited to the exigencies and challenges of contemporary society. According to the United Nations, the modern concept of security inter-alia, possesses economic, health, personal, community, political, and environmental dimensions, in-line with the objective of ensuring 'freedom

[70] YM Ajiji, 'Cyber Security Issues in Nigeria and Challenges' [2017] 7(4) *International Journal of Advanced Research in Computer Science and Software Engineering* 315

[71] M Wilson, The Evolution of Multilateralism in the Post-Cold War Era: Successes and Failures [2024] *International Journal of Research and Review Techniques (IJRRT)* 19

[72] ibid

[73] See M Wilson, The Evolution of Multilateralism in the Post-Cold War Era: Successes and Failures [2024] *International Journal of Research and Review Techniques (IJRRT)* 19, 22, 24

[74] Indian Cyber Security, *Nasscom v. Ajay Sood & Ors*. [2013] Vol. 3(2) <https://www.indiancybersecurity.com/case_study_nasscom_ajay_sood.php> Accessed May 23, 2025; T Singh, 'Cyber Law & Information Technology' [2007] <https://delhidistrictcourts.nic.in/ejournals/CYBER%20LAW.pdf> Accessed 13th May, 2024 13

[75] See Preambles of the Universal Declaration of Human Rights, 1948; International Covenant on Economic, Social and Cultural Rights, 1966; International Covenant on Civil and Political Rights, 1966

[76] Adopted by the World Conference on Human Rights in Vienna on 25 June 1993

from fear and want' that 'has been proclaimed as the highest aspiration of the common people.'[77] In the light of the cyber exercise of human rights, and the empirical and normative issues involved, this research adopted five concepts for explaining and assessing the exercise of human rights on the cyberspace, which are – (1.) Ownership; (2.) Legality; (3.) Legitimacy; (4.) Functionality; and (5.) Accessibility, in addressing the normative and empirical nuances concerning:

(a.) the exercise of ownership rights;
(b.) the legality of acts perpetrated on the cyberspace;
(c.) the legitimacy of administrative practices enforced therein;
(d.) the functionality of websites; as well as (e.) their accessibility.

These factors make cyber security an important issue of interest. Especially in the context of the modern concept of security as recognized by the United Nations, which now possesses socio-cultural, and economic dimensions.[78] Thus, States are burdened with the task of ensuring cybersecurity and the efficacious exercise of human rights on the cyberspace. That is a feat which among other things, can be achieved through legislation, regulatory cooperation and multilateralism, and adapting to the trends of the fourth industrial revolution, and the modern cyberization process. Consequently, 'it will always be a loosing battle if security professionals are way behind the cyber criminals in terms of technological knowledge.'[79] On that account, states are encouraged to adopt a technologically incline legal approach, for ensuring that the normative and empirical legitimacy of cyber laws are advanced, standardized, and pragmatic enough to cope with the cyberspace.

Another important issue of interest is accessibility, considering the indispensability of internet access: to the execution of various socio-economic and political activities. Thus, at the multilateral level, it is important for States to consider how the liberality of the cyberspace can be guaranteed, for the benefit of all persons.

[77] 'n 75'; L Hamourtziadou, 'Security challenges of the 21st century: new challenges and perspectives' [2019] 6(2) *Journal of Global Faultlines* 122
[78] ibid
[79] YM Ajiji, 'Cyber Security Issues in Nigeria and Challenges' [2017] 7(4) *International Journal of Advanced Research in Computer Science and Software Engineering* 318i