International Journal of Business and Management Invention (IJBMI)
ISSN (Online): 2319 – 8028, ISSN (Print): 2319 – 801X
www.ijbmi.org || Volume 8 Issue 05 Series. I || May 2019 || PP 20-26

Regulating Cyberspace: An Examination of Three Theories

Dr. Bernard Oluwafemi Jemilohun
Faculty of Law, Ekiti State University,Ado-Ekiti, Nigeria

ABSTRACT: *Cyberspace belongs to no man. It is another estate that those who partitioned territories and empires did not and could not have contemplated. Today it is possible for someone located within a physical territory thousands of miles from another to do things or transact businesses or commit crimes that will seriously affect the fortunes or livelihood of the other. Regulating interactions in this realm has not been a straightforward matter as the dynamic nature of cyberspace has enabled novel and hitherto uncontemplated acts which are both developmental and debilitative. In the light of several efforts made to regulate this realm, the arguments have shifted between territorial/national regulation, international/regional regulation and self/company regulation. This paper attempts to analyse the three key theories and ends up suggesting that while territorial regulation is good, more efforts should be made towards having global treaties that are acceptable and binding on all nations.*

Keywords: *Cyberspace, Regulation, Law-making, Treaties,*

Date of Submission: 05-05-2019 Date of acceptance: 20-05-2019

I. INTRODUCTION

The realm of cyberspace is wide yet local in the sense that while the reach of the internet is global, it has reduced the world into a village with people living thousands of miles apart from each other physically yet being able to interact as next door neighbours by the medium of information communication technology. This has created issues in governance and control with the possibilities of abuse and misuse and other negative consequences. Cyberspace governance is generally not as easily regulated as real space simply because in real space, the boundaries are delineated, as opposed to cyberspace where there are no boundaries (at least, physically). In the language of Greenleaf (1998), "Because cyberspace does have characteristics that distinguish it from real space, they make it more difficult for us to develop a coherent approach to how it should or should not be regulated by law".

There exists a number of theoretical issues that one will wish to explore in this article. Scholars like Fromkin (1997), Reidenberg (1998), (1998), Johnson & Post, (1996) are divided as to the need and the possibility of regulating cyberspace via the normal legislative mechanisms (Lessig, 1997). The technology of cyberspace and the mode of its development have been advanced as reasons against normal regulations. In the words of Boyle (1997), '…it was not so much that nation states would not want to regulate the Net, it was that they would be unable to do so, forestalled by the technology of the medium, the geographical distribution of the users, and the nature of its content. This tripartite immunity came to be a kind of Internet Holy Trinity, faith in which was a condition for acceptance into the community'.

But it will be out of place and a total absurdity to conceive an environment created by man but which man has resigned to uncontrollability. While the means of controlling or administering cyberspace may differ from the traditional means of governance, it must be stated that a realm perceived as uncontrollable by reason of its dynamic and changing nature will result in to an anarchical society.There are three major theories of Cyberspace regulation which have been propounded by various groups and scholars, this paper attempts to examine them with a mind to suggest the preferred model.

II. THE THEORY OF CYBERSPACE SELF–GOVERNANCE (DIGITAL LIBERTARIAN THEORY):

The first theory to be discussed is the theory of Self Governance in Cyberspace. This theory postulates that the electronic nature of cyberspace does not call for governmental regulation through territorial law making; rather the Internet should be allowed to formulate rules and regulations to govern it. The leading proponent of this theory is John Perry Barlow of the Electronic Frontier Foundation. (The Electronic Frontier Foundation is a donor supported membership organization working to protect fundamental rights in cyberspace). Barlow strongly feels the evolution of the Internet is without governmental influence and should be without governmental control. He wrote:

"Governments of the Industrial World, you weary giants of flesh and steel, I come from Cyberspace, the new home of Mind. On behalf of the future, I ask you of the past to leave us alone. You are not welcome

among us. You have no sovereignty where we gather.We have no elected government, nor are we likely to have one, so I address you with no greater authority than that with which liberty itself always speaks. I declare the global social space we are building to be naturally independent of the tyrannies you seek to impose on us. You have no moral right to rule us nor do you possess any methods of enforcement we have true reason to fear. Government derive their just powers from the consent of the governed. You have neither solicited nor received ours. We did not invite you. You do not know us, nor do you know our world. Cyberspace does not lie within your borders. Do not think that you can build it, as though it were a public construction project. You cannot. It is an act of nature and it grows itself through our collective actions."

The totality of Barlow's declaration was about 16 paragraphs and it was written in response to the Telecommunications Act, 1996 of the United States. Barlow believed that the Internet was beyond borders and, therefore, no one country had the mandate to apply laws to it. He attacked countries like China, Germany, France, Russia, Singapore, Italy and the United States of trying to ward off the 'virus' of liberty by erecting guard posts at the frontiers of cyberspace. He concluded by saying that a civilisation of the mind would be created in cyberspace and expresses the hope that it would be more humane and fair than the world that normal governments had made before.

Netanel (2000) opines that Barlow's impassioned call for cyberspace independence cannot just be dismissed as meaningless chatter ("theatrical whimsy of a former lyricist for the Grateful Dead"). According to Netanel, (2000) proponents of the Cyberspace self-governance theory (he calls them Cyberians)view cyberspace as a realm in which "bottom-up private ordering" can and indeed should supplant rule by the distant, sluggish, and unresponsive bureaucratic state. In his view, the argument of these theorists is supported by three main ideas

(i) Firstly, that cyberspace independence will maximise welfare. The idea here is that the multiple, decentralised, interconnected sites for digital communication that make up cyberspace create greatly enhanced possibilities for flexible decision making, transacting and norm creation that more efficiently allocate resources than centralised bureaucratic state regulation.
(ii) Secondly, that state regulation of cyberspace is essentially futile and thus the state should not attempt it. With the decentralized character and global reach of digital network communication, any nation's effort to impose its stamp on that communication would simply be met by regulatory arbitrage and evasion.
(iii) And lastly, that self-governance more fully realizes liberal democratic ideals than do regulations by even a liberal democratic nation state. In their contention, they maintain that in contrast to a "top-down" state regulation, cyberspace rule making would epitomize a political order based on the primacy of local norms and individual choice.

In support of this theory, Johnson and Post (1996) argue that the rise of an electronic medium that disregards geographical boundaries throws the law into disarray by creating entirely new phenomena that need to become the subject of clear legal rules but that cannot be governed satisfactorily by any current territorially based sovereign. Similar to this line of reasoning is the assertion that 'the internet is as inevitable and overwhelming as the incoming tide which confronted King Canute, and renders the traditional approach of regulation and prohibition futile'(Waters & Carver, 1996). In conceiving of cyberspace as a distinct place outside yet all over the real world, they argue for self-governance by envisioning the Internet as a self-regulating space separated from its surroundings in the broader social order.

In their line of reasoning, they posit that though privacy on the net may be a familiar concept, analogous to the privacy doctrine for mail systems, telephone calls and print publications, electronic communications create serious questions regarding the nature and adequacy of geographically based privacy protections. They surmise that because events on the Internet occurs everywhere and nowhere in particular, and are engaged in by only personae who are both realin the sense that they possess reputations, they are able to perform services and deploy intellectual assets,and intangible, not necessarily or traceably tied to any particular person in the physical senseand concerns things that are not necessarily separated from one another by any physical boundaries, no jurisdiction has a more compelling claim than any other to subject these events exclusively to its laws.

Johnson & Post (1997) argue further for what they call 'net federalism' or 'decentralised, emergent law'. They reason that the most likely to be successful model of Internet governance is *de facto* rules which may emerge as an outflow of the complex interplay of individual decisions by various types of system administrators and by users. In their words,

"Net federalism looks very different than what we have become accustomed to, because here, individual network systems, rather than territorially based sovereigns, are the essential governance units. The law of the net has emerged, and we believe can continue to emerge, from the voluntary adherence of large numbers of network administrators to basic rules of law (and dispute resolution systems to adjudicate the inevitable inter-network disputes), with individual users voting with their electron to join the particular systems they find most congenial."

Similar to this theory and in agreement with Johnson and Post (1997), Reidenberg (1998) argues that the technological architectures of networks impose a set of rules for the access to and use of information distinct from law. He opines that the set of rules for information flows imposed by technology and communication networks form a *Lex Informatica* that policy makers must understand, consciously recognise and encourage.It seems from the introduction of Reidenberg's work that *Lex Informatica* appears to have taken its coinage from the *Lex Mercatoria*, the laws that merchants evolved among themselves in the earlier days of cross border trading when they needed to create trust and confidence for robust international trade. These rules were independent of local sovereign rules and assured commercial participants of basic fairness in their relationships. In other words, rather than making laws for cyberspace interaction the normal way, the architecture and technological design of the internet should be reinvented and adapted to become a law unto the different players in cyberspace.

On the other hand Greenleaf (1998) feels that despite the many examples of the similarity between normal legislation and the technological architecture of cyberspace, Reidenberg (1998) failed to provide a sufficiently general approach to determining the most effective way of regulating cyberspace. Greenleaf further criticised digital libertarians' argument that law is destined to be ineffective in cyberspace, as a particular application of anti-law arguments to the new frontier of cyberspace, which to a large extent borrows from their earlier anti-law streams.

But beyond Greenleaf's (1998) criticism of Reidenberg's (1998) *Lex Informatica*, the theory of Cyberspace self-governance has been substantially disproved. Lessig (1996), in reacting to the argument that government cannot keep up with or understand the technology, or that any attempt to regulate or tax the Internet will strangle innovation, notes that "to argue that real space law should leave cyberspace alone, needs a normative argument – an argument about why it is good or right to leave cyberspace alone". There is nothing about technology of cyberspace that law-making agencies cannot understand. The most optimistic versions of the argument stress the potential for forms of self-regulation in cyberspace which are to a large extent an emphasis on social norms as regulations. (Greenleaf, 1998)

Cohen, DeLong and Zysman (2000) argue that the World Wide Web is getting inextricably entangled in the webs of law, custom and commerce – the tissue of our daily lives. The Internet affects too many interests and raises too many social questions to continue as a policy free zone. What happens in the virtual world can have serious impacts on everyone, including those who have never used a computer. Since the Internet has become ubiquitous and unavoidable, it becomes necessary that laws are made to regulate the same.

Kobrin (2001) points out that contrary to the assertion of Barlow that the Internet originated outside of governmental influence, the well-known history of the Internet shows that it did not arise spontaneously from market forces, and there was no laissez-faire about its origins. It was purely a public good supplied by the state. The Internet began in the late 1960s as a communications infrastructure called ARPANET as a result of efforts by the Advanced Research Projects Agency (ARPA) of the United States Department of Defense. He argues that the Internet has been transformed beyond what anybody could visualize some thirty years ago and its public origin raises questions about the presumption that it is or should be beyond regulatory structures. The fact that the private sector has taken over much of the business on the internet should not keep governmental regulation out. The development of commerce over the years have been made largely possible through the oversight of government and the instrumentality of legislations and regulations.

III. THE THEORY OF GOVERNMENTAL REGULATION VIA LEGISLATION:

This second theory is directly opposite the first one considered above. The regulation of cyberspace is agreed to by almost every scholar except that as pointed above, some scholars prefer self-regulation. For instance, the origin of the European Data protection regime stems from the idea that computers and their pervading influences must be regulated by law. With the ubiquitousnature of cyberspace, the need for regulation becomes more real than apparent.

One of the arguments in favour of governmental regulation was put forward by Netanel (2000). Even though he does not agree that state intervention is always appropriate, he opines that the benefits of state intervention must be balanced against possible harms to speech and association interests that themselves have inherent value for liberal democracy. He concludes that democratic institutions of territorial nation-states are far more likely to effectively protect liberal rights and to further the liberal ideal of government by consent of the governed. If one may take this reasoning further, it means then that the very reasons why the digital libertarians want free non-governmental control of cyberspace will be better served by governmental regulation via legislation.

Reed (2007), is of the opinion that the making of Information Technology-specific provisions in laws and regulations by legislators and regulators is a consequence of the permeating influence of information technology. He points out that the fundamentality of information technology to both commercial and non-commercial activity demands its regulation. He argues that though the experiences of those working with

Information Technology regulation sometimes show that regulations are unsatisfactory because in spite of the best efforts of regulators, Information Technology regulation has consistently failed to cope with the rapid changes in the technology; there are ways to cure defects in the legislation. He suggests that regulators must develop an understanding of how Information Technology is used and secondly, the regulations must address human behaviour directly rather than institutions, structures or status.

With respect to data protection, Akinsuyi (2007) is of the view that data protection legislation has been enacted to identify the responsibilities of organizations that collect, transmit, store and process personal information. In other words, legislation in cyberspace has become necessary to delimit the ability of organizations and other individuals from encroaching on the rights of others. Akinsuyi's line of reasoning is that it is the consciousness of the value of information in cyberspace that has led to much data protection legislation. He cited instances of criminal prosecution of individuals who used other people's information to commit fraud on the internet. (USDOJ, 2012) The prosecutions were based on legislations made to govern interactions in cyberspace. The import of the foregoing is that an absence of legislations governing interactions in cyberspace will create a lacunae in the legal framework and thus an inability for law enforcement.There can be no stronger argument for legislation of cyberspace.

In concurring with the role of law in cyberspace, Greenleaf posits that law typically regulates individual behaviour directly, and does so by threatening ex post facto sanctions. He goes further to argue that it is in both real space as well as cyberspace that law regulates individuals indirectly by aiming to change markets, norms or code. In other words, law does not only affect individual behaviour directly by prohibiting certain conduct but also indirectly by seeking to change markets, norms and architectures.

It is worth noting that since about the year 2000 till the present moment, the cyber-libertarian tendency has retreated and it has become well established that nation states have both the right to regulate and an interest in regulating the internet. This is more so as the internet has ceased to be a plaything only of academics, researchers and computer experts, but now a continually all-embracing part of our daily social, financial, medical and family life. The possibilities of multi-dimensional interactions in cyberspace and the far-reaching consequences that flow therefrom makes regulation by legislation an imperative. Law as an instrument of regulating social interactions has always checked the likelihood of excesses and abuse of rights and privileges.

IV. THE THEORY OF INTERNATIONAL REGULATION

This third theory postulates that the global nature of the Internet and the fact that it is a realm beyond natural borders calls for international cooperation for effective governance and administration of cyberspace. The proponents of this theory postulate that the realm of cyberspace is not within the reach of any single nation or national government and thus it will amount to a futility for individual nations to attempt to legislate for a realm that is not within their physical control.

One of the leading proponents of this theory is Judge Schjolberg (2011) from Norway. In his words,

"Cyberspace, as the fifth common space, after land, sea, air and outer space, is in great need for coordination, cooperation and legal measures among all nations. It is necessary to make the international community aware of the need for a global response to the urgent and increasing cyber-threats. Peace, justice and security in cyberspace should be protected by international law through a treaty or a set of treaties under the United Nations. The progressive developments of global cyberattacks, such as massive and coordinated attacks against critical information infrastructures of sovereign states, must necessitate an urgent response for a global treaty".

While citing examples of some countries that have suffered severe attacks against their critical information infrastructure, Schjolberg (2011) points out that the cyber-attacks on sensitive national information infrastructure are rapidly emerging as one of the most alarming national security threats, and a most serious cybercrime of global concern.

Ghernaouti-Hélie (2010) earlier stating what is in agreement with Schjolberg (2011), argues that the international community needs to set up a United Nations Cyberspace Treaty. She states further that, "Nowadays, there is a real and urgent need for an international agreement, for a coherent and global approach to deal with cybersecurity and cybercrime issues. Organizations, businesses and states face significant risks in relation to the inappropriate disclosure, misappropriation and destruction of data and information and such incidents, when viewed at a macroscopic level, can be viewed as posing a potential threat not just to the competitiveness or reputation of a business but also at a national level to public safety, national security or democracy itself.

She submits that the issue cannot be handled at local levels because the world we live in is only one and it is dominated by the intensive use of Information Communication Technology devices, infrastructures and services. Nowadays citizens, organizations and states are dependent on Information Communication Technology infrastructures for everything they need. It is a complex dependency with multiple interdependencies involving several types of actors distributed all over the world. In her view, the interconnectedness of information

communication technologies across territorial and national boundaries makes national legislation inadequate.

Hughes (2010), argues for the need of a cyberspace treaty from the perspective of impending cyber-wars. He opines that though an all-out cyber-war is yet to be waged, cyber-experts and military strategists anticipate that a major interstate cyber-battle would be fought within the next few years. Forasmuch then as the global community now depends more on cyberspace for its most basic and most critical functions, there is the need to prevent a full-scale cyber-attack as the social and economic impact would cripple a modern networked state. It appears that Hughes envisaged a phenomenon now known as cyber-terrorism. Beyond terrorists' use of the internet to plan, initiate, coordinate and further their acts of terrorism against humanity, cyber terrorism involves acts of terrorism within cyberspace that may not have immediate direct consequences on everybody.

However, the foregoing has been objected to, nay, disagreed with by some other writers. Duggal (2010) argues that though it is true that all countries need to realize that the Internet and cyberspace are shared by all of us, and that we need collaboration at the international level to counter the broad range of threats, yet the reality is that the world's nations do not have the luxury of time to formulate new sweeping international agreements. He suggests that a more practical measure would be greater international cooperation between cybercrime units and law-enforcement agencies, not limited by national borders. While agreeing that the Council of Europe's Convention on Cyber Crime is an example of an effective international treaty, he argues that there are a large number of practical obstacles to progress particularly at the international level. Top of this is the high level of mistrust between governments that do not wish to share information related to their national security or internal policies.

Duggal (2010) concludes by saying that since there are different legislative approaches to dealing with cyber deterrence in different countries, and dramatically different legislative approaches to such issues as freedom of expression and human rights, he believes that the only way forward is by discussion, debate and collaboration. Countries have to learn to share their strategies for cyber deterrence, thus contributing to a far more cohesive international approach to the subject that should produce more cybersecurity for all in the future.

Agreeing with Dugal (2010) on the non-feasibility of cyberspace treaty are authors Segal and Waxman(2011). Segal & Waxman argue pointedly that the cyberspace treaty is nothing but a pipe dream because "different interests among powerful states – stemming from different strategic priorities, internal politics, public private relationships and vulnerabilities – will continue to pull them apart on how cyberspace should be used, regulated and secured. With the United States and European democracies at one end and China and Russia at another, states disagree sharply over such issues as whether international laws of war and self-defence should apply to cyber-attacks, the right to block information from citizens, and the roles that private or quasi private actors should play in Internet governance. Many emerging internet powers and developing states lie between these poles, while others are choosing sides." This goes to say that until state actors see the need to work harmoniously together to tackle the negative uses of the internet and act together in the common interest of humanity, the possibility of a cyberspace treaty may remain an illusion.

It is interesting to note that one of the major causes for divergence lies in the conceptualization of what cybersecurity is. On the part of the United States, the UK and their likeminded allies, it seems that the emphasis is on protection of computer networks from damage and theft. But on the part of the Russia, China and their counterparts, it seems that the emphasis is on information security which means the controlling of content and communication and social networking tools which may threaten regime stability. Thus while the West has operated from the viewpoint of free speech and allowed much freedom in cyberspace, the Eastern bloc has consistently refused to allow too much liberty for the individual in cyberspace resulting in much censorship of the internet generally.

V. CONCLUSION

This paper has attempted to analyse the challenges inherent in the regulation of cyberspace largely because of its ubiquitous nature and in the course of examining the three theories reasoned that a self-regulating regime may not be the best option looking at the possibilities of abuse and misuse. While a cyberspace treaty acceded to by all the nations in the world would be the most desirable, ideological differences and the unwillingness of some nations to allow others to know what they consider technological secrets will definitely be impediments.

However, it is interesting to note that virtually every country on the face of the globe has one or more legislations to govern interactions in cyberspace. From laws governing the protection of the processing of personal information popularly called 'Data Protection' to laws preserving intellectual property rights to laws regulating electronic transactions in commerce between individuals and corporate bodies to laws prohibiting, preventing and prosecuting cybercrime, national legislations and regional statutory instruments have found their ways into cyberspace.

Beyond the United States, the United Kingdom and other countries in the West where the Internet appears to have started, other nations have taken advantage of the multi-faceted advantages of the internet and

because the possibilities in cyberspace are limitless, nations have learnt to enact legislations dealing with various aspects of interactions in cyberspace. While regional bodies have spearheaded some efforts in the form of Conventions, Directives and other statutory instruments, individual nations have also set machineries in motion to promote interactions in cyberspace especially in the areas of e-commerce, the need to prevent the abuse of personal information and the prevention of cybercrime in all its facets.

The United Nations Commission on International Trade Law (UNCITRAL)has released some model laws for electronic commerce and electronic signatures while the United Nations Office on Drug and Crime has model laws curbing organised crime and other threats to peaceful existence. As far back as 2007, countries within the Economic and Social Commission for Western Asia conducted surveys on the state of cyber-legislation in the countries within the ESCWA and showed that the nations have either made adequate legislations governing interactions in cyberspace or were in the process of making relevant legislations.

The analysis shows that the following countries outside the ESCWA region have also made laws for cyberspace at varying degrees and for various sectors: Belgium, France, Luxembourg, Germany, Sweden, Switzerland, Romania, Canada, The United States of America, The United Kingdom, Malaysia and Singapore.

On a national and territorial level, Nigeria is striving not be left out of the comity of nations with sound and stable legal frameworks for cyberspace, especially when it comes to the prevention of cybercrime, the protection of personal data and the protection ofcritical national information infrastructure. Though Nigeria cannot presently compare herself with developed economies or advanced democracies like the United States of America, the United Kingdom or Canada, one can say that a step in the right progress was taken when the Cybercrime (Prohibition, Prevention, Etc.) Act of 2015 was enacted. This was after several bills in the area of information communication technology and allied matters have been presented before the law-making bodies without any success.

For developing nations such as Nigeria and other third-world countries, an expectation of a self-regulating cyberspace will be a disaster in the making. The literacy level and the criminal tendencies which are a result of underdevelopment and poverty do not warrant and indeed cannot sustain an unregulated cyberspace in such environments.

For now, the best we can have is a cyberspace that is regulated by territorial legislation yet with international cooperation to secure the private rights of individuals, prevent or curb criminal actions with appropriate penalty while making sovereign governments functional and at the same time pushing for a global treaty to secure cyberspace generally.

REFERENCES

[1]. Akinsuyi, F. F., (2007) Data Protection Legislation for Nigeria, The Time is Now! Retrieved from http://www.nigerianmuse.com

[2]. Barlow, J. P., A Declaration of the Independence of Cyberspace retrieved from https://projects.eff.org/~barlow/Declaration-Final.html

[3]. Boyle J., (1997), Foucalt in Cyberspace: Surveillance, Sovereignty and Hardwired Sensors. U. Cin. L. Rev. 66, 177

[4]. Cohen, S. S., DeLong, J. B. & Zysman, J., (2000) Tools For Thought: What is new and Important about the New Economy BRIE Working Paper #138, Berkeley, CA

[5]. Duggal, P., (2010) Cyber Deterrence: Legal Perspectives in Global Cyber Deterrence: Views from China, the U.S., Russia, India and Norway. Retrieved from www.ewi.info/system/files/CyberDeterrenceWeb.pdf

[6]. Edwards, L.,(2009) Pornography, Censorship and the Internet in Edwards L. & Waelde, C., (Eds.), Law and the Internet Hart Publishing, Oxford p. 626

[7]. Fromkin, M., (1997) The Internet as a Source of Regulatory Arbitrage. in Kahin B. & Neeson, C. (Eds.) Borders in Cyberspace MIT Press;

[8]. Ghernaouti-Hélie, S., (2010) "Need for a United Nations Cyberspace Treaty" paper presented at a High-Level Debate on Cybersecurity and Cyberspace, WISIS Forum 10-14 May, 2010 Geneva. Retrieved from www.cybercrimelaw.net/documents/SGH_CyberspaceTreaty.pdf

[9]. Ghernaouti-Hélie, S., (2010) We Need a Cyberspace Treaty InterMedia, 38 (3) Retrieved from http://www.hec.unil.ch/sghernaouti/wp-content/uploads/2010/08/We-need-a-cyberspace-treaty.pdf

[10]. Greenleaf, G., (1998) An Endnote on Regulating Cyberspace: Architecture vs Law'. U.N.S.W.Law Journal 52

[11]. Hodge, N., (2009, May 13) General: We Just Might Nuke Those Cyber-Attackers, WIRED, retrieved from http://www.wired.com/2009/05/general-we-just-might-nuke-those-cyber-attackers/

[12]. Hughes, R., (2010) "A Treaty for Cyberspace" International Affairs, 86 (2). p. 523-541. Retrieved from onlinelibrary.wiley.com/doi/10.1111/j.1468-2346.2010.00894.x/pdf

[13]. Johnson, D. & Post, D., (1996) Law and Borders: The Rise of Law in Cyberspace. Stan. L. Rev. 48, 1367

[14]. Johnson, D. & Post, D., (1997) And How Shall the Net be Governed? – A Meditation on the Relative Virtues of Decentralized, Emergent Law retrieved from http://www.cli.org/emdraft.html

[15]. Judge Stein Schjolberg, (2011), An International Criminal Court or Tribunal for Cyberspace. A paper for the EastWest Institute (EWI) Cybercrime Legal Working Group. Retrieved from www.cybercrimelaw.net

[16]. Kobrin, S. J., (2001) Territoriality and the Governance of Cyberspace Journal of International Business Studies, 32 (4) 687-704

[17]. Lessig, L., (1996) The Zones of Cyberspace Stanford L. Rev. 1403-1411

[18]. Lessig, L., (1997) The Law of the Horse: What Cyberlaw Might Teach available at http://cyber.law.harvard.edu/works/lessig/law_horse.pdf ;

[19]. Lessig, L., (1997) Constitution and Code. Cumberland Law Review (27), 1-15, Lessig, L., (1997) Reading the Constitution in Cyberspace. Emory L. J. 45, 869-910

[20]. Netanel, N. W., (2000) Cyberspace Self-Governance: A Skeptical View from Liberal Democratic Theory Calif L. Rev. 88, 395. Retrieved from http://cyber.law.harvard.edu/ilaw/Contact/Netanel_Full.html
[21]. Reed, C., (2007) The Law of Unintended Consequences – Embedded Business Models in IT Regulation JILT 2
[22]. Reidenberg, J., (1998) 'Lex Informatica: The Formulation of Information Policy Rules through Technology Texas L. Rev 76 553-593,
[23]. Reidenberg, J., (1996) Governing Networks and Rulemaking in Cyberspace. Emory L. J. 45 912-930;
[24]. Segal, A. & Waxman, M. C., (2011) Why a Cybersecurity Treaty is a Pipe Dream Council on Foreign Relations. Retrieved from http://www.cfr.org/cybersecurity/why-cybersecurity-treaty-pipe-dream/p26325
[25]. Waters, P. & Carver, L., (1996) The Internet and Telephony: The Impact of Uncontrollable Technology on Traditional Telephony Regulation https://www.gtlaw.com.au/ cited in Greenleaf, G,

Dr. Bernard Oluwafemi Jemilohun" Regulating Cyberspace: An Examination of Three Theories"International Journal of Business and Management Invention (IJBMI), vol. 08, no. 05, 2019, pp 20-26