

The Regulation of Cybercitizens' Conduct on Cyberspace: The Constitutionality and Applicability of the Nigerian Cybercrimes Act 2015

Felix E. Eboibi*

Faculty of Law, Niger Delta University, Wilberforce Island, Yenagoa, Bayelsa State, Nigeria

Abstract

Globally, domestic laws have been enacted subjecting activities on cyberspace to existent regulation. In this regard, the Nigerian Federal Government enacted the Nigerian Cybercrimes Act 2015. This Act has generated controversy as to the constitutionality and consequent application throughout the Nigerian federation, especially where the duty to legislate on the subject matter of cybercrime and/or criminal matters is not specifically stated in any of the lists provided in the Constitution of the Federal Republic of Nigeria, 1999 (As Amended), on one hand. On the other hand, the literature seems to have arrogated to the State Houses of Assembly the power to legislate on criminal matters. This scenario is the recent basis for the current Delta State Cybercrimes (Prohibition, Prevention etc.) Bill 2016 before the Delta State House of Assembly. This paper argues in an attempt to forestall the ongoing controversy and fill the gap in the literature, by critically examining the Nigerian Constitution, Cybercrimes Act and comparative legislations to unequivocally portray that the Nigerian National Assembly is the appropriate body to legislate on cybercrime, hence the Nigerian Cybercrimes Act 2015 is constitutional and applicable throughout the Federal Republic of Nigeria.

Keywords: Cyberspace, regulation, cybercitizens, constitutionality of Nigerian Cybercrimes Act 2105, application of Nigerian Cybercrimes Act 2105, cybercrime

***Author for Correspondence** E-mail: felixeboibi@mail.ndu.edu.ng, lixboibi@yahoo.com

INTRODUCTION

The cyberspace is a network of millions of computers where information, communication and a wealth of online activities are offered to cybercitizens [1]. The feature of modern life is being defined by cyberspace [2]. From September 2012 to October 2017, internet usage in Nigeria have increased from 27,967,723 (Twenty-Seven Million, Nine Hundred and Sixty-Seven, Seven Hundred and Twenty Three) to 93,887,184 (Ninety Three Million, Eight Hundred and Eighty Seven, One Hundred and Eighty Four) people [3]. Today, cyberspace provides information relating to almost all topics one can think of. There is no doubt about the availability of academic information on cyberspace; however, it has suddenly and increasingly metamorphosed into an information center for public sector bodies, government departments, individuals and commercial enterprises [4]. Cyberspace avails communication with people globally for just the price of a local call

through e-mail; shopping online has become a very big business on the web; one can chat in real time with internet users globally; one can use his or her web browser to hear "live" radio broadcasts; use of a newsreader to read and post to newsgroups has become a common phenomenon; international businesses trade goods and services in cyberspace, moving assets across the globe in seconds [5]. Persons who engage in the above activities or other activities on cyberspace are referred to as "cybercitizens" or members of the "cybercommunity."

Despite the avalanche of advantages that cyberspace presents for cybercitizens, it also empowers those who would disrupt and destroy. The global scope of cyberspace gives adversaries, otherwise known as cybercriminals' broad avenue for exploitation and attack [6]. These cyber threats and attacks have been made possible and easier, arguably due to far-reaching unhindered accessibility of

tools employed for hacking. The development of sophisticated tools and techniques by cybercriminals are widespread, and these potentials are bought very cheap on the internet. Consequently, cybercriminals are able to engage in cyber financial or monetary fraud; launch sophisticated attacks into systems, networks and critical infrastructures which cause grave physical damage; economic disruption and impacts negatively on national security [7].

Considering these enormous disadvantages that the cyberspace can be used to perpetrate, should the activities or conducts of cybercitizens not be regulated? The regulation of the conduct of cybercitizens on cyberspace has been seriously linked to the interplay between the worldwide availability on the web of data or information perceived to be harmful or offensive to fundamental values in the regulating State and the Constitutional legislative powers of a federal State, which the data is made possible.

Though, there is a debate in the literature as to whether or not cyberspace should be regulated. Commentators against regulating cyberspace argue that it should be left freely for cybercitizens use and that they intend to create a space which would be free and unregulated by traditional nation-state rules. They buttress their argument on the ground that cyberspace does not possess borders hence regulations made are bound to fail; since the internet is everywhere, no sovereign state should be allowed by its laws to exclusively restrict cybercitizens to her laws; it will be unfair to subject conducts outside domestic coverage on domestic regulation; confusion and lack of knowledge to be faced by cybercitizens while on cyberspace. They advocate for self-regulation by cybercitizens [8].

However, commentators have questioned the proponents of self-regulation of the internet and consequently asked: Would it mean that every regulatory area related to the internet would be left to self-regulation? Would the entire net community be regulated by self-regulating regimes or only some specific subsets within it? Quite a number of problems have been raised that will work against self-regulation: from enforcement to lack of

physical force in place. If there is no physical force in place, what means does the net community have to enforce its own guilt rules? Answers proffered from this perspective are a valid tool of deterrence but admitted that the issue is yet to be resolved [9].

This work is not set out to determine the veracity or otherwise of the current debate in the literature on the regulation of cyberspace. It thus agrees with the proponents for the regulation of cyberspace. The political and legal institution is the proper regulatory body to carry out the task of regulating cyberspace. The State based on elected governments combined with the rule of law, exhibits a proven democratic legitimacy and encompasses the institutional mechanisms to enforce the regulations needed to manage cyberspace. Cyberspace being a product of an advanced telecommunications technology national regulation of cyberspace transaction is legitimate and feasible [10]. In short, in today's world, cybercrime prevention is a necessity.

For the purposes of regulating the conduct of cybercitizens on cyberspace, the Federal Government of Nigeria enacted the Nigerian Cybercrimes Act 2015. Specifically, section 2 of the Act made the provisions of the Act applicable throughout the Federal Republic of Nigeria. The problem with the Act and its application is that Nigeria operates a federal system of government whereby several tiers of government with authorized constitutional legislative powers exist under the legislative lists within the federated order [11]. The question is which level of government should ordinarily exercise the legislative power to enact a law regulating the conduct of cybercitizens, or put differently, which level of government should legislate on cybercrime in Nigeria? Nigeria is a federation that consists of 36 States and a Federal Capital Territory. There is a division of power in the federation between the central (federal) and the States. The Constitution of the Federal Republic of Nigeria, 1999 (As Amended) separates the powers of the Federal Republic of Nigeria between the federal government and the State governments. The legislative power of the Federal Republic of Nigeria is vested in the National Assembly while that of a State is in the House of Assembly of the State [12].

Generally, there would have been no legislative problem in determining which government's legislative house has the duty or power to legislate on a particular subject matter in the Federal Republic of Nigeria if the item is listed specifically under (the exclusive legislative list meant for the National Assembly and concurrent list meant for the Houses of Assembly of the States) any of the list provided in the Nigerian Constitution [13]. However, cybercrime and/or criminal law is not listed either in the Exclusive or in the Concurrent legislative lists. Again, the Nigerian Cybercrimes Act 2015 does not state under which of the constitutional provisions the National Assembly promulgated the Act, especially where the existing literature arguably implies that any matter not mentioned in either the exclusive or concurrent list is deemed to be residual such as matters of criminal law which are for the States [14]. It is on this basis that the current Delta State Cybercrimes (Prohibition, Prevention etc.) Bill 2016 is before the Delta State House of Assembly for consideration. One need to ask: Is the promulgation of a Cybercrime Law within the constitutional legislative power of the Nigerian State Houses of Assembly? Can cybercrime be equated to ordinary or traditional crimes under the purview of criminal law?

It is quite obvious that it is not within the confines of the Federal Republic of Nigeria through the National Assembly to exercise legislative power by enacting any legislation, deliberately or by necessary implication, which will impinge on the legislative powers and authority of States if it is unascertainable from the Constitution that the Federal Government's action was unavoidable in the overall interest of Nigeria and was constitutional. Section 2 of the Nigerian Cybercrimes Act 2015 provokes to a large extent the determination of the validity or invalidity of the said Act. Can the Nigerian Cybercrimes Act 2015 be applied throughout the Federal Republic of Nigeria if it is not constitutionally valid?

Presently, there is no judicial construction or pronouncement on the validity or otherwise of the Nigerian Cybercrimes Act 2015. There is the dire need to prevent the Nigerian polity from being littered with Cybercrime laws and

policies by both the National Assembly and State Houses of Assembly which may lead to conflict and confusion as to which law is the extant law on cybercrime and superior for obedience by Nigerians. Consequently, this paper argues that the Nigerian Cybercrimes Act 2015 enacted by the Federal Republic of Nigeria through the National Assembly draws its validity from the Constitution of the Federal Republic of Nigeria, 1999 (As Amended). It outlines the basis for arriving at the conclusion and thereafter contends that the provisions of the Act as it is applicable throughout the Federal Republic of Nigeria. It takes a comparative posture of what is obtainable in other jurisdictions in similar footing. Thereafter, this paper examines the incompetency of the Nigerian State Houses of Assembly to enact a Cybercrime Law for the States and in the same vein show that the Delta State Cybercrimes (Prohibition, Prevention etc.) Bill 2016 before the Delta State House of Assembly ought not to be passed into law or if eventually passed into law is invalid. This paper ends with deductions and conclusion.

LEGISLATING ON CYBERCRIME IN NIGERIA: IS THE NIGERIAN CYBERCRIMES ACT 2015 CONSTITUTIONAL?

The legitimacy of any law, rule or enactment in the governance of Nigeria is determined by the Nigerian Constitution [15]. Examining the legitimacy or otherwise of the Nigerian Cybercrimes Act 2015 which this part is set out to do is most challenging since it bothers on the Nigerian federal system of government. Under this system, there is a division of legislative powers and responsibilities between the federal units which is vested in the legislature. Neither the central government (federal) nor the regional governments (States) can confer or impose responsibilities on either functionaries of the other without its chief executive giving consent in that respect [16]. Moreover, one government is restricted from interfering with the management of another government in course of exercising its powers [17].

From the Federal government perspective, the National Assembly which comprises two legislative houses: the Senate and House of Representative are vested with the powers to

make laws for the federation [18], while from the State government perspective, legislative powers are vested in the House of Assembly of the State [19]. The Nigerian Constitution distributes legislative powers and responsibilities through the Exclusive legislative list and Concurrent legislative list. The Exclusive legislative list comprises of matters that are within the competence of the federal government to the exclusion of the State governments by virtue of section 4(3) of the Constitution of the Federal Republic of Nigeria, 1999 (As Amended). Part 1 of the Second Schedule to the Constitution sets out 68 items as matters in the exclusive legislative list. The Concurrent list comprises matters that both the federal government and state governments can exercise legislative powers. Part II of the Second Schedule to the Constitution sets out 30 items as matters in the concurrent legislative list. A third legislative list is discerned from the literature, although not specifically mentioned in the Nigerian Constitution, as residual legislative list [20]. It gives the States, legislative powers to make laws on matters not stated in both the exclusive and concurrent lists.

As stated elsewhere in this work, the Nigerian Cybercrimes Act 2015 was enacted by the Nigerian National Assembly and was made applicable throughout the Federal Republic of Nigeria by virtue of section 2 of the Act. The Act is made for the prohibition, prevention, detection, response, investigation and prosecution of cybercrimes and for other related matters [21]. Cybercrime and/or criminal law is not specifically enumerated among the 68 items under the exclusive legislative list neither is it stated in the 30 items under the concurrent legislative list. The Nigerian cases of *Emelogu v. The State* [22] and *Sele v. The State* [23] give the impression that since criminal matters are not mentioned under both the exclusive and concurrent legislative lists, it is deemed to be a residual matter which automatically falls under the legislative competence of the State Houses of Assembly. Due to the fact that the legislative list in the Nigerian Constitution is fashioned after the Constitution of the Commonwealth of Australia, this argument has been supported by the position taken by the Australian courts, in

construing the constitutional provisions of Australia which is alleged to be similar to that of Nigeria. In the cases of *McArthur v. Williams* [24]; *R v. Kidman* [25] and *R v. Bernasconi* [26], the Australian courts have consistently held that the Commonwealth (Federal) Parliament had no legislative authority to deal with general matters of criminal law.

Irrespective of the foregoing, it is herein argued that the Nigerian Cybercrimes Act 2015 enacted by the Federal Republic of Nigeria through the National Assembly draws its validity from the Constitution of the Federal Republic of Nigeria, 1999 (As Amended) and consequently, the provisions of the Act as it is applicable throughout the Federal republic of Nigeria. The following are the basis for arriving at the conclusion:

Cybercrime is Incidental to Items in the Exclusive Legislative List

No doubt the exclusive legislative list did not specifically mention cybercrime under the 68 items in Part 1 of the Second Schedule to the Constitution. However, item 68 of the said legislative list of the Constitution allows the enactment of legislation under the heading “incidental powers”. Item 68 reads thus: “Any other matter incidental or supplementary to any matter mentioned elsewhere in this Act”. The inclusion of “incidental and supplementary” matter in the exclusive legislative list emphasizes the well-known principle of law that every grant of power includes by implication all such other powers as are reasonably incidental thereto and not expressly excluded [27]. This is fortified by section 10(2) of the Nigerian Interpretation Act [28]: “An enactment which confers power to any act shall be construed as also conferring all such other powers as are reasonably necessary to enable that act to be done or are incidental to the doing of it” and the United States Supreme Court in *Mcculloch v. Maryland* where it was contended that creating a corporation exceeded congress power on the ground that it was not expressly stated as part of powers granted to it by the Constitution [29]. It was held by the court that Congress power provided for in the Constitution, suggest, as a requisite incident, power to use all suitable avenues for carrying the powers into force, and that because

creating the corporation is not a substantive and independent power, it is implied in the powers expressly granted.

Moreover, in answering the question whether the Nigerian Cybercrime Act 2015 is valid, section 2 (a) Part III of the Second Schedule to the Nigerian Constitution must be resorted to. It states: “in this schedule, references to incidental and supplementary matters include without prejudice to their generality to offences”. This section is arguably inserted in the Constitution to give qualification to item 68. Based on section 2, the National Assembly is competent to enact the Nigerian Cybercrimes Act 2015 which includes cybercrime offences and penalties. The only caveat here is that the offences created must be incidental and supplementary to matters falling within the legislative powers granted to the National Assembly to enact laws. For instance, in the celebrated case of *Belewa v. Doherty* [30], the Judicial Committee of the Privy Council held that: “no offence can be created...unless the creation... is incidental or supplementary to some other matter... that the matter does not become incidental to another matter merely by being closely connected with it; the latter must actually have been acted (*sic*) or legislated upon before something else, like creation of offences can be said to be incidental to it”.

Again, the Nigerian Supreme Court in *Attorney-General Ondo State v. A.G Federation* held thus [31]:

The provision of section 2(a) of Part III of the Second Schedule to the 1999 Constitution was enacted in order to expound the effect and the extent of the provision of item 68 of Part I of the Second Schedule. It is by virtue of that provision that offences may be created by the National Assembly if it is shown that such offences as may be created are incidental and supplementary to matters on which the National Assembly is vested with power to enact laws [32].

Based on the foregoing, can it be authoritatively stated that cybercrime is incidental to items in the exclusive legislative list? The answer is in the affirmative because most of the items in the exclusive legislative list attracts cybercrime perpetration. The

development in information and communication technology and innovations of computers ensures that most of the items mentioned in the exclusive legislative list are carried out with the help of the cyberspace and computers. In this regard, these devices become targets for cybercriminals hence the need for the Nigerian Cybercrimes Act 2015 which has made provision for cybercrime offences and penalties. The Act covers a broad spectrum of cybercrime offences punishable with penalties and fines in Part III, which includes: Offences against critical national information infrastructure [33]; Unlawful access to a computer [34]; System Interference [35]; Interception of Electronic messages, e-mails, electronic money transfer [36]; Tampering with critical infrastructure [37]; Willful misdirection of electronic messages [38]; Unlawful interceptions [39]; Computer related forgery [40]; Computer related fraud [41]; Theft of electronic devices [42]; Unauthorized modification of computer systems, network data and system interference [43]; Cyber-terrorism [44]; Fraudulent issuance of e-instructions [45]; Identity theft and impersonation [46]; Child pornography and related offences [47]; Cyberstalking [48]; Cyber squatting [49]; Racists and xenophobic offences [50]; Importation and fabrication of e-tools [51]; Breach of confidence by service providers [52]; Manipulation of ATM/POS terminals [53]; Phishing, spamming, spreading of computer virus [54]; Dealing in card of another [55]; Purchase or sale of card of another [56]; Use of fraudulent device or attached e-mails and websites [57].

Trade and commerce is one of the items in the exclusive legislative list [58]. Today, virtually all commercial transactions are carried out online. Since the responsibility of regulating trade and commerce is within the powers of the Federal government, the National Assembly is competent to create offences that impinge on the effectiveness and efficiency of electronic commerce through the Nigerian Cybercrimes Act 2015. Electronic commerce in cyberspace takes place in a borderless internet without reference to a State or national boundaries and most cybercrimes perpetrated in Nigeria are related to electronic commerce [59]. This automatically excludes the state

House of Assembly from enacting a law in that respect. Commercial and Industrial Monopolies [60]; currency coinage and legal tender [61]; are also items in the exclusive legislative list that are directly or indirectly related to commerce.

Banks, Banking Bills of exchange and promissory notes [62]; copyright [63]; customs and exercise duties [64]; Diplomatic, consular and trade representation [65]; Defense [66]; Evidence [67]; Exchange control [68]; Export duties [69]; External affairs [70]; Extradition [71]; Finger Prints, Identification and criminal records [72]; immigration and emigration from Nigeria [73]; implementation of treaties relating to matters in this list [74]; passports and visas [75]; patents, trademarks, trade or business names, industrial designs and merchandise marks [76]; police and other government security services established by law [77]; posts, telegraphs and telephones [78]; public relations of the Federation [79]; Weights and measures [80]; Wireless, broadcasting and television other than broadcasting and television provided by the Government of a State; allocation of wavelengths for wireless, broadcasting and television transmission [81], are other items in the exclusive legislative list which relates to cybercrime and are covered by the provisions of the Nigerian Cybercrimes Act 2011.

Wireless networks which is mentioned as part of the items in the exclusive legislative list gives credence to the validity of the Nigerian Cybercrimes Act 2015 and the fact that it is incidental to the powers of the National Assembly. The development in electronic, computer technologies and wireless communications has resulted to the proliferation of wireless networks. These include amongst others, cellular, vehicular, body area, underwater, mobile ad hoc and sensor networks. The use of wireless networks and communications emanating from any device anywhere and anytime has engineered cybercrimes. Unless there is a regulation, these cyber threats, crimes and vulnerabilities will continue on wireless networks. The Nigerian government has taken a bold step by enacting the Nigerian Cybercrimes Act 2015 which also works to curtail crimes perpetrated through

wireless networks. The Act prohibits fraud by wireless networks; facsimile, telex, modem and internet transmissions. It also imposes criminal penalties on persons who engage in illegal interception; protects unlawful access to stored communications; protects the confidentiality, integrity, and availability of communications stored by service providers. The Act also prohibits identity theft and generally internet crimes. Phishing (where for instance a cybercriminal uses fraudulent e-mails to obtain bank account numbers and passwords) is prohibited and provides modalities for prosecuting cybercriminals who are in the habit of sending volumes of unsolicited commercial e-mail. The Act also addressed computer related offences. It penalized access to information that is classified in a computer; financial records or credit stored in a financial institution; theft of property arising from a pattern to defraud through the computer; altering, destroying or damaging data belonging to another [82].

The discourse shows that there is sufficient connection between the cybercrime offences and penalties created in the Nigerian Cybercrimes Act 2015 and most of the items mentioned in the exclusive legislative list to be regarded as being incidental and supplementary. It was held in the case of *Attorney General v. Great Eastern Railway* that anything that is fairly incidental to a subject matter provided for in a statute is *intra vires* except it is explicitly forbidden [83]. "Incidental power" denotes a power, though not explicitly granted must exist as a result of its germaneness to achieve the explicit power [84]. The court in *International Shoe Co. v. Pinkins* expressed the view that whatever is implied in a Constitution is as much part of it as that which is expressed [85]. Basically, it is difficult to say that cybercrime offences and penalties cannot be justifiably created or found to be incidental or supplementary in respect to the items in the exclusive legislative list (except few) pursuant to a relevant subject-matter. There is no gainsaying that if cyber and/or computer related attacks are made against the performance or execution of any of the items, it will have a great impact on the effective and adequate execution of governments program towards them.

Consequently, the National Assembly has the power and responsibility to criminalize such activities. According to the Australian judge, Higgins J in *R v. Kidman* [86].

An act making a conspiracy to defraud the Commonwealth a criminal offence may fairly be treated as an Act made ‘with respect to’ each and all of the subjects of legislation mentioned in the first thirty-eight placita of sec.51 (comparable to the items in the exclusive legislative list of the Nigerian Constitution); for a fraud on the Commonwealth affects its finances, and to cripple the finances tends to cripple, more or less, the exercise of all the law... if the frauds, and conspiracies to defraud, which are incidental to the administration of the government, as well as to all big financial undertakings have not been criminal and punishable before, parliament can make them criminal and punishable – whether they were committed before, or are committed after, Parliament legislates on the subject [87].

Based on the foregoing, it must be stated that the argument emanating from the literature that the duty to legislate on criminal matters is that of the State House of Assembly is not helpful to dislodge the discourse under consideration. The Nigerian cases of *Emelogu v. The State* [88] and *Sele v. The State* [89] are basically the basis for this conclusion and other cases have relied on them to give similar impression in the Nigerian polity. Although in *Emelogu v. The State* [90], the Supreme Court held that armed robbery is a State crime and espoused that any matter not stated in either the exclusive legislative list or concurrent legislative was automatically deemed residual. On the other hand, by virtue of *Sele v. The State* [91], it is the Houses of Assembly that have the legislative power to cover matters that bothers on the criminal code and control of offences [92].

One striking thing in the two cases mentioned above is that they dwell on armed robbery offence. Prior to this time, the offence was prohibited under the Robbery and Firearms (Special Provisions) Decree No.47 of 1970 as a federal offence during the military regime to eradicate the rampant nature of armed robbery

occurrence in Nigeria. Subsequent decrees on robbery and firearms were promulgated. Thereafter, following the departure of the military, reference was then made to the Decree as an Act on the assumption that it was an Act of the National Assembly with the general believe that armed robbery still exist as a federal offence, giving prosecutorial powers to State Attorney-General. Notwithstanding, criminal law was not accommodated either on the exclusive legislative list or concurrent legislative list under the Constitution of the Federal Republic of Nigeria, 1979. Consideration was given to it as a residual matter with Houses of Assembly competent to legislate on same. The issues brought for determination before the full court in *Emelogu v. The State* [93] were: (1) whether offences under the Robbery and Firearms (Special Provisions) Act No. 47 of 1970 are Federal offences or not; (2) whether if they are Federal offence, the State Attorney-General had the *locus standi* to prosecute without express delegation of powers by the Federal Attorney-General. Eso JSC expressed the majority view on the issues before the court as follows: (1) Decree No. 47 of 1970 as amended was regarded as a Law and assumed to be enacted by a State House of Assembly as at 1st October 1979 and consequently “Robbery” *per se* was seen to be a residual matter [94]. (2) Decree No. 47 of 1970 as amended is ascribed a Federal legislation and to be seen as a legislation equipped to operate in each State of the federation and the power to institute and undertake armed robbery proceedings is accorded the State Attorney-General by virtue of section 191 of the Constitution of the Federal Republic of Nigeria, 1979 [95]. Meanwhile, the issues determined by the court in *Emelogu v. The State* [96] were not in issue *per se* in *Sele v. The State* [97]. However, Karibi-Whyte JSC remarked that armed robbery is circumscribed under the legislative competence of the State Houses of Assembly [98].

No matter how persuasive the *Emelogu* and *Sele* cases maybe, they do not dwell on the cardinal issue under consideration as it relates to the germaneness of the provisions of the Constitution of the Federal Republic of Nigeria, 1999 (As Amended) as set out in this

work bothering on the constitutional legislative competence of the National Assembly to create cybercrime offences and penalties arising from the Nigerian Cybercrimes Act 2015. It is obvious that this discourse has nothing to do with the legality or otherwise of the National Assembly taking responsibility of the criminal code or core criminal law jurisdiction as the case maybe generally under which armed robbery exist. Consequently, there is no cogent argument premised on the decision of *Emelogu* and *Sele* cases that has any effect or impact whatsoever on the legislative powers of the National Assembly derived from the Constitution of the Federal Republic of Nigeria, 1999 (As Amended) to enact the Nigerian Cybercrimes Act 2015. From a legal point of view, the National Assembly validly created cybercrime offences and penalties pursuant to her legislative powers under the Nigerian Constitution. In addition, item 67 of the exclusive legislative list granted the National Assembly general powers to legislate on matters which are not expressly stated in the exclusive legislative list [99]. Item 67 reads: "Any other matter with respect to which the National Assembly has power to make laws in accordance with the provisions of this Constitution" [100].

Moreover, cybercrime offences are not like the ordinary or traditional crimes, e.g. armed robbery, murder, stealing etc. that should be left for the State Houses of Assembly to legislate on. Under the Nigerian criminal jurisprudence ordinary or traditional crimes have three elements: conduct (*actus reus*), intent (*mens rea*) and a forbidden result or "harm". In the physical or real world, crimes committed ought to possess the three elements. The object of criminal law is to impose liability and sanctions (e.g., death, incarceration, fines) in respect to acts that cause injury to persons or property or the unauthorized taking of another person's property. Cyberspace is a place that exists differently from the physical or real world [101]. Consequently, the criminal law principles cannot effectively take care of criminal activities perpetrated on cyberspace. Cyberspace is borderless and interconnected hence the criminal activities that occur there

are without reference to a particular State boundary. It is not possible for any particular state to allege that the enactment of the Nigerian Cybercrimes Act 2015 is an interference with the duty of State House of Assembly to criminalize activities occurring within the State.

The implication is that in the absence of any specific constitutional provision empowering States with the power to enact law on cybercrime offences and penalties, the issue of the federal government through the National Assembly interfering with the States independence or autonomy is not tenable. Obviously, interference by the federal government is impracticable in the absence of an available function or power of the States in respect to cybercrime offences. Most importantly, the Nigerian Cybercrimes Act 2015 did not give any responsibilities or powers to any state functionary to warrant any investigatory or scrutinizing powers of the National Assembly on such functionary [102]. Therefore, the Delta State Cybercrimes (Prohibition, Prevention etc.) Bill 2016 which is a duplication of the Nigerian Cybercrimes Act 2015 being considered before the Delta State House of Assembly is a usurpation of the powers of the National Assembly; unconstitutional and an exercise in futility.

The Need for Peace, Order and Good Government of the Federation

It is the primary duty of every government to make provision for security and welfare of the people physically and in cyberspace (cybercitizens). Any unruly act or behavior of any person with the ability to undermine the well-being of the citizenry or cybercitizens must be legislated against [103]. Section 4 of the Nigerian Constitution acknowledges this by ensuring the need for peace, order and good government in respect to Nigeria as a nation [104], and similarly acknowledges the need for peace, order and good government in respect to all the States of the federation distinctly [105]. It is on this premise that the National Assembly is accorded powers and responsibilities to enact laws for the purposes of actualizing this goal or intention. Considering the nature of cyber-attacks and cybercrime perpetration, if they are not

checked like the Nigerian Federal government seem to have done through the enactment of the Nigerian Cybercrimes Act 2015, the peace, order and good government of the federation or any part thereof will be threatened.

The fact that States have similar powers to make law for the peace, order and good government within the state, which they have exercised in respect to stealing, murder, malicious destruction of property, robbery etc. does not apply to cybercrime offences. An exclusive federal role and responsibility is obviously the appropriate way to go. The rationales are comprehensible. The cyberspace is borderless and interconnected hence the criminal activities that occur online or through the computer (as a tool or target) are without reference to a particular State (or international) boundaries; the duty of obeying numerous cybercrime laws separately may attract different kinds of prohibition and punishment which could be onerous, complicated and catastrophic; it is the federal government that has the might to deal with foreign threats. This is so because the result of a cyber attack from abroad can lead to a military attack that uses traditional kinetic weaponry and it may be of a war than mere crime [106].

When taken from the foregoing perspective, cybercrime is a national security and defense issue that affects the welfare of Nigerians as against mere alleged criminal matter within the legislative powers of States. It is on this premise that section 14(2) (b) of the Nigerian Constitution which seeks the protection of the security and welfare of the people by government has been incorporated into the exclusive legislative list by virtue of item 60(a) of the Nigerian Constitution. Item 60 reads thus: "The establishment and regulation of authorities for the Federation or any part thereof, (a) to promote and enforce the observance of the fundamental Objectives and Directive Principles contained in this Constitution". The implication of item 60(a) arguably is that the perpetration of cybercrime as a security matter under the fundamental objectives and directive principles of state policy in chapter II of the Constitution has been placed in the exclusive legislative list and a call on the National Assembly to exclusively

legislate on it to give legal backing to the policy [107]. For the purpose of this argument, "security" in section 14(2)(b) is herein referred to as the duty to make provision for internal and external security and protection of the Federal Republic of Nigeria and this falls appropriately under the power of the National Assembly to enact a law. On the other hand "welfare" underscores "the general welfare of Nigeria" which therefore requires a law on social, economic or political matters should it become impracticable for distinct States to legislate to take care of specific issues [108]. These lead credence to the validity or constitutionality of the Nigerian Cybercrimes Act 2015.

It might be argued that "State" as used in section 14(1) ("The Federal Republic of Nigeria shall be a State based on the principles of democracy and social justice") [109] of the Nigerian Constitution for actualizing section 14(2)(b) of the directive principle on security implies the Federal, State and Local Government. On the contrary, the reference to "State" in the subsection arguably simply means the Federal Republic of Nigeria equipped with the duty to activate the policy to prevent intrusions into the security of Nigeria that tend to undermine the security of cybercitizens. It is on this premise that section 4(1) of the Nigerian Constitution empowered the National Assembly to legislate for the benefit of the Federal Republic of Nigeria and not the Federation as a universal element of federalism. Hence, sections 4(2) and (3) vested the power on the National Assembly to enact laws for the peace, order and good government of the Federal Republic of Nigeria concerning any matter in the exclusive legislative list to the exclusion of the Houses of Assembly unless otherwise provided by the Nigerian Constitution. For this reason, the legislative power to enact a law bothering on cybersecurity or cybercrime as exhibited through the Nigerian Cybercrimes Act 2015 is the National Assembly to the exclusion of the State Houses of Assembly.

The issue of cybercrime in the Nigerian polity is not just within the country. It is more than a local affair. It has a national impact, which ordinarily should be curtailed by the

government of the Federal Republic of Nigeria. The protection and regulation of the nation's cyberspace is paramount considering the important nature of Nigeria's economy and the activities of government. Cyber and terrorist attacks; radicalism and violent extremism are rife through cyberspace. The expanding nature of Nigeria's resort to digital infrastructure ignites the threat to national security, especially as Nigeria loses about N127 billion naira, which is about 0.08% of Nigeria's Gross Domestic Product (GDP) yearly to cybercrime perpetration [110]. Its attributes amongst others are seen in: adverse reduction of competitive strength of corporate organizations; unnecessary time wasting and sluggish economic/financial growth; delays production and increases cost; tarnishes Nigeria image; facilitates the growth of terrorists' activities; it has impact on consumer trust; it enhances money laundering; it encourages fraud on social media; it is a danger to our national security [111]. Commentators, in domestic and international reports have referred to Nigeria as the hub of cybercrime and cybercrime perpetrators, giving Nigeria an embarrassing international reputation [112]. The global rating of Nigeria between 2002 and 2014 by the internet cybercrime report further shows the prevalent nature of the menace of cybercrime in Nigeria (Table 1):

Table 1: Representation of Nigeria's Ranking in Cybercrime.

(Source: Internet Cybercrime Report from 2002 to 2014 [113])

Year	Global Ranking	Africa Ranking
2002	Second (2nd)	First (1st)
2003	Third (3rd)	First (1st)
2004	Third (3rd)	First (1st)
2005	Second (2nd)	First (1st)
2006	Third (3rd)	First (1st)
2007	Third (3rd)	First (1st)
2008	Third (3rd)	First (1st)
2009	Third (3rd)	First (1st)
2010	Third (3rd)	First (1st)
2011	Not ranked among top ten	-
2012	Twenty fifth (25th)	First (1st)
2013	Third (3rd)	First (1st)
2014	Twenty fourth	Second (2nd)

In the above highlighted circumstances, how can the menace of cybercrime be tackled in Nigeria? It is obviously through the enactment

of criminal offences and penalties stating that everyone would be held liable to punishment in breach of any act or omission contrary to the Nigerian Cybercrimes Act 2015. This way, the menace of cybercrime would be nationally tackled for peace, order and good government of the federation. The Nigerian Cybercrimes Act 2015 has also empowered certain cybercrime institutions; Office of the President of the Federal Republic of Nigeria [114]; Office of the National Security Adviser [115]; Attorney General of the Federation [116]; Financial Institutions [117]; Law Enforcement Agents [118]; Service Providers [119]; Cybercrime Advisor Council [120] and National Cyber Security Fund [121] to coordinate, implement and enforce the Act [122]. Specifically, section 41(1) of the Act recognizes the Office of the National Security Adviser as the coordinating body for all security and enforcement agencies. The office is obligated to provide support to all relevant security, intelligence, law enforcement agencies and military services to prevent and combat cybercrimes in Nigeria; formulate and effect the implementation of a comprehensive cyber security strategy and a national security policy for Nigeria; establishment and maintenance of a National Computer Emergency Response Team (CERT) Coordination Center for the management of cyber incidences in Nigeria; establishment and maintenance of a National Computer Forensic Laboratory; building capacity of all security agents for the discharge of their functions on cybercrime in Nigeria. Section 42(2) of the Act empowers the Attorney General of the Federation to strengthen and enhance the legal framework so that Nigeria's cybercrime and cybersecurity laws and policies conform with regional and international standards; maintain international cooperation required to prevent and combat cybercrimes and promote cybersecurity and ensure the effective and efficient prosecution of cybercrimes and cybersecurity matters.

It is obvious that the cybercrime institutions mentioned above fall under the exclusive control and preserve of the Nigerian Federal Government and by virtue of section 4(2) of the Nigerian Constitution the National Assembly is empowered to legislate under

item 60(a) of the Nigerian Constitution for the purpose of establishing and regulating cybercrime and its institutions for the federation. This is exactly what the National Assembly has done by enacting the Nigerian Cybercrimes Act 2015. By implication the established cybercrime institutions are by virtue of item 60(a) of the Nigerian Constitution empowered to promote and enforce the observance of the Fundamental Objectives and Directive Principles of State Policy on security pursuant to section 14(2) (b) provided for in Chapter II of the Nigerian Constitution. Without doubt, the cybercrime institutions cannot employ force or coercion to enforce the observance of the Fundamental objectives neither can they legislate. What the cybercrime institutions require is the enactment of a legislation, if for any reason they must enforce observance of the Fundamental Objectives through coercion or any other means. The power to enact a legislation is that of the National Assembly.

In the Indian case of *Mangru v. Commissioners of Budge Budee Municipality* [123] where the Indian court decided on Directive Principles of State Policy in Part IV of the Indian Constitution which is akin to the Nigerian Constitutional provision under reference that legislation is needed for Directive principles to be implemented, and in the absence of an enacted law to execute the policy stipulated in a Directive, no State or individual can be held in breach of any prevailing law or lawful right in whatever guise of following a Directive [124]. The Nigerian Supreme Court in *Attorney-General, Ondo State v. Attorney-General Federation* [125] stated that “courts cannot enforce any of the provisions of Chapter II until the National Assembly has enacted a specific law for their enforcement...” [126]. The Court per Uwaifo JSC stated that:

Section 14(2)(b) can be legislated upon under item 60(a) for other variety of circumstances in which coordinated effort under national guidance would warrant it is not difficult for me to accept. Such a circumstance could be a state of emergency of national importance, such as real necessity or national disaster: see *Attorney-General for Ontario vs. Canada Temperance*

Federation(1946) AC 193; or of war when it would become imperative for the Federal Republic to be protected or defended: see *Co-Operative Committee on Japanese Canadians vs. Attorney General for Canada* (1947) AC 87; or the care and protection of the people require to be centrally motivated: see *Russel vs. The Queen* (188) AC 396. I must however point out that those circumstances are adequately directly provided for under subsections (1) and (3) of section 11 of the Constitution [127].

The negative impact of cybercrime perpetration in Nigeria activated the necessity and seriousness of the Federal Republic of Nigeria exhibition of interest and reaction pursuant to section 14(2)(b) of the Nigerian Constitution. It took the national interest and integrity of Nigeria as a nation paramount. This show of concern outwits and is beyond local and state governments. Consequently, the prohibition of cybercrime is a national one, especially where its negative impact explained above robs every Nigerian irrespective of religion, tribe and state of origin. The Nigerian Cybercrimes Act 2015 was enacted based on national interest and for the enforcement of Fundamental Objectives and Directive Principles to engender the peace, order and good government of Nigeria. In *Awule v. The Queen* [128], where the 1st appellant and 10 others were arraigned in court for criminal breach of trust in breach of section 315 of the Penal Code. They were eventually found guilty, convicted and sentenced by the trial court. On appeal, Mr. Fiberesima, counsel for the 1st appellant argued that since banking is an item under the exclusive preserve of the Federal parliament to legislate, section 315 of the Penal Code which stipulated 14 years as a term of imprisonment in a case of criminal breach of trust committed by a banker, was unconstitutional. The Federal Supreme Court, per Ademola, C.J.F held thus:

We are of the opinion that section 315 of the Penal Code is constitutionally valid in so far as it includes bankers in the category of persons liable to heavier punishment for criminal breach of trust. We are of the view that this is not legislation in respect to Banks and banking but merely an incidental provision in penal legislation enacted for the

peace and good government of Northern Nigeria. We therefore reject the submission of bankers and that it is null and void [129].

The Nigerian Supreme Court in arriving at the constitutionality or validity of the Corrupt Practices and Other Related Offences Act 2000 and that the issue of corruption cannot be left for individual States in *Attorney-General, Ondo State v. Attorney-General Federation* [130] on the ground of national interest and general welfare of Nigeria placed reliance on the United States of America cases of *Helvering v. Davies* [131]; *Heart of Atlanta Motel v. United States* [132], Canadian Cases of *Russel v. Queen* [133]; *Toronto Electric Commissioners v. Snider* [134]; *Attorney General for Ontario v. Temperance Federation* [135]; *Reference Anti-Inflation Act* [136], and the Constitutional Court South Africa case of *Cape Metropolitan Council and Anor v. Irene Grootboom & Ors.* [137]. The Nigerian Supreme Court reasoned thus:

There may be occasion and probably always would, when what appears a local problem assumes such a proportion as, a whole. In such a case it may turn out to be inevitable to regard the matter as affecting the peace, order and good government of the country which ought to be addressed by means of a uniform law [138].

Though, section 4(7)(a) of the Nigerian Constitution empowers the House of Assembly of a State to make laws for the peace, order and good government of the State in respect to matters not included in the Exclusive Legislative List set out in Part 1 of the Second Schedule. Based on the foregoing, cybercrime or cybersecurity is a matter under the Exclusive Legislative List and also incidental to the matters in the Exclusive Legislative List. Consequently, any law on cybercrime offences and penalties or cybersecurity purported to have been made or in the process of being made by the House of Assembly of a State is unconstitutional, null and void [139]. The implication is that the current Delta State Cybercrimes (Prohibition, Prevention etc.) Bill 2016 before the Delta State House of Assembly is an exercise in futility as it contravenes the Nigerian Constitution. It is a repetition, duplication,

addition and subtraction of the provisions of the Nigerian Cybercrimes Act 2015 contrary to the Nigerian Supreme Court decision in *Attorney-General of Abia State vs. Attorney-General of the Federation* [140]. For instance, section 58 of the Nigerian Cybercrimes Act 2015 which is the interpretation section is reproduced verbatim as section 2 of the Delta State Cybercrimes Bill 2016; Part II of the Nigerian Cybercrimes Act 2015 is reproduced verbatim as Part I of the Delta State Cybercrimes Bill 2016 except that in place of the names of President and National Security Adviser, Governor and Security Officers of the State are inserted respectively; Part III of the Nigerian Cybercrimes Act 2015 which deals with cybercrime offences and penalties is reproduced verbatim as Part II of the Delta State Cybercrimes Bill 2016; Part IV of the Nigerian Cybercrimes Act 2015 which examines the duties of financial institutions is reproduced verbatim as Part IV of the Delta State Cybercrimes Bill 2016; Part V of the Nigerian Cybercrimes Act 2015 that deals with administration and enforcement is reproduced verbatim as Part V of the Delta State Cybercrimes Bill 2016 except that in place of the National Security Adviser – Chief Security Officer of the State is inserted, a joint function of coordination is given to both Chief Security Officer and Attorney-General of the State for all security and enforcement agencies unlike the Nigerian Cybercrimes Act 2015 that solely gave the coordination of security agencies to the National Security Adviser; Part VI of the Nigerian Cybercrimes Act 2015 which deals with Arrest, search, seizure and prosecution is reproduced verbatim as Part VI of the Delta State Cybercrimes Bill 2016 except that in place of the Attorney-General of the Federation, Attorney-General of the State is inserted; Part VII of the Nigerian Cybercrimes Act 2015 which deals with jurisdiction and international co-operation is reproduced verbatim as Part VII of the Delta State Cybercrimes Bill 2016 except that in place of Federal High Court, State High Court is inserted and Part VIII of the Nigerian Cybercrimes Act 2015 which deals with miscellaneous is reproduced verbatim as Part VIII of the Delta State Cybercrimes Bill 2016 except that in place of Attorney-General of the Federation, Attorney-General of the State is inserted.

The provisions of the Nigerian Constitution discussed in this work and section 2 of the Nigerian Cybercrimes Act 2015 implies coverage of the subject matter of cybercrime or cybersecurity by the federal government through the National Assembly. Moreover, the cybercrime institutions (law enforcement agents/security officers; service providers; financial institutions etc.) provided under the Delta State Cybercrimes Bill 2016 are under the exclusive control and responsibility of the federal government. Most importantly is the issue of inconsistency of the Delta State Cybercrimes Bill 2016 with the Nigerian Cybercrimes Act 2015. In *Attorney-General Abia State v. Attorney-General Federation* [141], the Nigerian Supreme Court while determining the implication of a federal law with the intent to cover a subject matter relied on the doctrine of covering the field generally attributable to the Australian courts and held thus:

The doctrine of covering the field is attributed to the Australian Courts. See *Ex parte Mclean* (1930) 43 CLR 472; *The State of Victoria & Ors. vs. Commonwealth of Australia & Ors.* (1937) 58 CLR 618 at 630, where Dixon J. explained the doctrine of inconsistency thus: Subsequently, it amounts to this. When a state law, if valid, would alter, impair or detract from the operations of a law of the Commonwealth Parliament, then to that extent it is invalid. Moreover, if it appears from the terms, the nature or the subject-matter of a Federal enactment that it was intended as a complete statement of law governing a particular matter set of rights and duties, then for a state law to regulate or apply to the same matter or relation is regarded as a detraction from the full operation of the commonwealth law and so is inconsistent [142].

Again, in *Military Governor, Ondo State v. Adewunmi* [143], the court held that where a matter has been validly legislated upon by the Federal Government any legislation made by a State based on the same matter which is inconsistent with the legislation made by the Federal Government will be void to the extent of the inconsistency.

APPLICATION OF THE NIGERIAN CYBERCRIMES ACT 2015

It is beyond doubt that one of the intentions of the Nigerian National Assembly's enactment of the Nigerian Cybercrimes Act 2015 is to prevent, prohibit and punish perpetrators of cybercrime in all facets throughout Nigeria. This position is obviously captured in Section 2 of the Act when it stated that "the provisions of this Act shall apply throughout the Federal Republic of Nigeria." The promotion and enforcement of the observance of the provision of section 14(2)(b) of the Nigerian Constitution is another reason for the promulgation of the Act.

Considering the express provision of section 2 of the Act making the operation and applicability of the Act throughout the Federation, the Attorney-General of the Federation is empowered by virtue of section 174 of the Nigerian Constitution to institute criminal proceedings against any person before any Federal High Court in Nigeria other than a court-martial, in respect to any of the offences provided in the Act; to take over and continue any such criminal proceedings that may have been instituted by any other authority or person and to discontinue at any stage before judgment is delivered any such criminal proceedings, instituted or undertaken by him or any other authority or person [144]. Moreover, the powers conferred on the Attorney-General can be exercised himself or through officers of his department [145]. The Attorney-General shall have regard to the public interest, the interest of justice and the need to prevent abuse of legal process in course of exercising his powers [146]. The decision of the court in *The State v. Ilori* [147] is apt in the sense that the manner of the exercise of the powers conferred on the Attorney-General pursuant to section 174 of the Nigerian Constitution cannot be controlled by the court neither can he be asked not to exercise his powers on the premise that his authority does not expand to any specific State in Nigeria. The implication is that the power of the Attorney-General is not limited by section 174 of the Nigerian Constitution [148]. The operation of the Act binds all States of the

Federation. Section 47(1) of the Nigerian Cybercrimes Act 2015 in addition to the powers of the Attorney-General to prosecute cybercrime offences gives law enforcement agencies in Nigeria similar powers subject however to the powers of the Attorney-General. The only exception is in respect to offences in sections 19 and 21 of the Act [149] which requires the prior approval of the Attorney-General [150].

This argument is germane because the court gives the impression in *Fawehinmi v. Babangida* [151] that an incidental matter under a federal legislation is a residual matter, consequently, the law assumes a state law applicable and applies only in the federal capital territory. This is supported by the earlier referred position that the federal government through the National Assembly has no legislative power in respect to criminal law or crime. Unfortunately, this discourse has shown that this position is not true for cybercrime or cybersecurity. Although, cybercrime or cybersecurity is not directly mentioned under the Exclusive Legislative List, cybercrime offences created by the Nigerian Cybercrimes Act 2015 are directly linked to items like Defense and national security; Currency and banking and others earlier stated in this work, thereby empowering the National Assembly by virtue of items 68, 67, 60(a) of the Exclusive Legislative List; section 2(a) Part II of second schedule and section 14(2)(b) of the Nigerian Constitution to legislate on.

It must be noted that similar criminal offences have been enacted by the National Assembly which enjoys applicability throughout the federation. To mention but a few; the Terrorism Act [152] which is invariably linked to defense and national security and the Money Laundering Act [153] linked to currency and banking [154]. The Nigerian Cybercrimes Act 2015 cannot be different as it has same link with defense and national security; currency and banking and other items hence its applicability throughout the federation is valid.

The application of the provisions of the Nigerian Cybercrimes Act 2015 throughout

the federation cannot be said to be an interference with States affairs. Cybercrime perpetration cuts across all States of the federation and outside the Nigerian borders. In this regard, it is the federal government through the National Assembly that is in the best position to enact a law on cybercrime pursuant to the Nigerian Constitution. For purposes of emphasis and appreciation, the Nigerian Cybercrimes Act 2015 is enacted; to create room for justiciability through legislation on a stipulated State Policy in order to prevent, prohibit and punish cybercrime; to pay attention to grave interests arising from both national and international domains about cybercrime; to give a national drive campaign against cybercrime without undermining the States; to curtail and provide penalty for specified cybercrime offences plus the ones that occur outside Nigerian borders by Nigerians [155]. The exercise of the Federal government's legislative power is not in any way geared towards assuming a general responsibility towards legislating on criminal law. The prohibition of cybercrime in Nigeria through the Nigerian Cybercrimes Act 2015 will enhance good government in Nigeria [156].

Other jurisdictions have similar Act that has effect throughout the Federation. For instance, in the United States of America, congress enacted the Social Security Act 1935 in respect to social security. It involved a policy of old age benefits where payments are made in that respect through an account to be made available by Treasury to actualize the benefits. In this regard, the Act empowered the taxation of employees' income and an excise tax on employers which required payment "with respect to having individuals, in his employ" at least 8 in number while tax by employees, the employers were mandated to collect same through deductions of an amount upon payment of wages. The United States Constitution, Article 1, section 8 stated thus: "The Congress shall have power to lay and collect taxes, duties, imports and excises, to pay the debts and provide for common defense and general welfare of the United States". Pursuant to the Act, a corporation shareholder instituted an action to restrain the corporation from making the deductions. The Circuit Court of Appeals held the provisions of the Act empowering the deductions to be void being

an interference of States powers granted under the US Constitution [157]. However, in the case, i.e. *Helvering vs. Davies* [158] the US Supreme Court took a different view when it held that on the basis of catering for the “general welfare” Congress is entitled to spend money which is not fixed. Here, the general welfare of old people was seen to be the general welfare of United States pursuant to the US Constitution. Mr. Justice Cardozo stated *inter alia*: “...The problem is plainly national in area and dimensions. Moreover, laws of the separate states cannot deal with it effectively...a system of old age pensions has special dangers of its own, if put in force in one state and rejected in another... only a power that is national can serve the interests of all” [159].

CONCLUSION

Cyberspace offers a lot of positive online activities to millions of cybercitizens. Due to its availability and anonymity, cybercriminals have found solace in the commission of offences against cybercitizens. The prevention of these vices has ignited possibilities of nation States to regulate cyberspace for the security and welfare of their citizens. Nigeria has a peculiar problem because it operates a federal system of government where there is a division of power between the central (federal government) and regions (states government). Moreover, there is the general view emanating from the literature that the responsibility to legislate on crime or criminal matters is that of House of Assembly of a State. However, the Nigerian National Assembly enacted the Nigerian Cybercrimes Act 2015 to regulate the activities of cybercitizens and made the operation of the provisions of the Act throughout the federation. This paper examined these from the perspective of the validity and/or constitutionality of the Nigerian Cybercrimes Act 2015. It is the position of the paper that although cybercrime is not specifically mentioned in the Exclusive Legislative List of the Nigerian Constitution, the appropriate authority of government to legislate for the regulation of a borderless and interconnected cyberspace applicable to Nigeria is the federal government through the National Assembly. This conclusion is arguably inferred from item 68 in Part 1 of the Second Schedule to the Constitution; section

10(2) of the Nigerian Interpretation Act; section 2 (a) Part III of the Second Schedule to the Nigerian Constitution; item 67 of the exclusive legislative list; Section 4 of the Nigerian Constitution; section 14(2) (b) of the Nigerian Constitution; item 60(a) of the Nigerian Constitution; sections 2 of the Nigerian Cybercrimes Act 2015; domestic and comparative(foreign) case laws.

REFERENCES

1. Brian Cooper, *et al. Essential Internet Guide*. London: Dorling Kindersley Limited; 2000; 10p.
2. United States of America Department of Defense Strategy, Department of Defense Strategy for Operating in Cyberspace [internet]. 2011; 2p. [cited 2017 Dec 20]. Available from: <https://csrc.nist.gov/CSRC/media/.../DOD-Strategy-for-Operating-in-Cyberspace.pdf>
3. Nigeria Communication Commission, Internet Subscriber Data [internet]. [cited 2017 Dec 28]; Available from: <https://www.ncc.gov.ng/stakeholder/statistics-reports/industry-overview#view-graphs-tables-5>
4. Brian Cooper, *et al.* As above, note (1).
5. Ibid
6. United States of America Department of Defense Strategy, Department of Defense Strategy for Operating in Cyberspace [internet]. 2011; 2p. [cited 2017 Dec 20]. Available from: <https://csrc.nist.gov/CSRC/media/.../DOD-Strategy-for-Operating-in-Cyberspace.pdf>
7. Ibid
8. Johnson DR, Post DG. The New “Civic Virtue” of the internet. [internet]: 11p. Available from: <http://www.cli.org/paper4.htm> cited in Antonio Segura-serrano, Internet Regulation and the Role of International Law. *Max Planck UNYB*. 2006; 10: 195p. Reidenberg JR. Governing Networks and Rule-Making in Cyberspace. *Emory Law Journal*. 1996; 45: 911–915p. In Antonio Segura-serrano, As Above; Johnson DR, Post DG. Law and Borders: The Rise of Law in Cyberspace. *Stanford L Rev*. 1996; 48: 1367p. Trotter Hardy I. The Proper Legal Regime for “Cyberspace:” *University of Pittsburgh Law Review*. 1994; 55: 993p. Peritt HH Jr. Cyberspace Self-

- Government: Town Hall Democracy or Rediscovered Royalist? *Berkeley Technology Law Journal*. 1997; 12: 413p. In Antonio Segura-serrano,
9. Antonio Segura-serrano. Internet Regulation and the Role of International Law. *Max Planck UNYB*. 2006; 10: 196p. Mayer-Schonberger V. The Shape of Governance: Analyzing the World of Internet Regulation. *Va J Int'l L*. 2003; 43: 622–623p. Lemley MA. The Law and Economics of Internet Norms. *Chicago-Kent Law Revie*. 1998; 73: 1257, 1268–1269p.
 10. Goldsmith JL. Against Cyberanarchy. *U Chi LR*. 1998; 65: 1199, 1243–1244, 1249p. Goldsmith JL. The Internet and the Abiding Significance of Territorial Sovereignty. *Ind. J Gobal Legal Stud*. 1998; 5: 475–476p. Ratner. New Democrats, Old Atrocities: An Inquiry in International Law. *Geo LJ*. 1999; 87: 707, 740p. Mayer-Schonberger V. The Shape of Governance: Analyzing the World of Internet Regulation. *Va J Int'l L*. 2003; 43: 612p. Stein AR. The Unexceptional Problem of Jurisdiction in Cyberspace. *Int'l Law*. 1998; 32:1167, 1174p. Hughes J. The Internet and the Persistence of Law. *Boston College Law Review*. 2003; 44: 359, 364p.
 11. Madu VC. Judicial Review of Legislation. *NIALS International Journal of Legislative Drafting (NIJLD)*. 2012; 1(1): 159–160p.
 12. Adebayo AM. 1999 *Constitution of the Federal Republic of Nigeria (As Amended) Annotated with Cases*. Lagos: Princeton Publishing Co; 2012; 11p.
 13. Sunday Oloyede v The State (2013) LPELR–22215(CA).
 14. Emelogu v The State (1988) NSCC (Vol. 19, pt. 1) 869. Ikechukwu Okoh v State (2008) LPELR–8352(CA). Aminu Tanko v The State (2009) LPELR–3136 (SC). George v FRN (2011) 10 NWLR (pt.1254), 1 at 12, 72–73p.
 15. Aminu Tanko v. The State (2009) LPELR–3136 SC.
 16. Attorney General Ogun State & Ors v. Attorney General of the Federation & Ors (1983) 3 NCLR 583.
 17. Per Nasir. PCA in Federal Ministry of Internal Affairs & Ors v. Shugaba (1983) 3 NCLR 915; see also the Australian cases of Malbourne Corporation v Commonwealth (1947) 74 C.L.R 31 at 82–93p. R v Commonwealth Court of Conciliation and Arbitration, *ex-parte* Victoria (1942) 66 CLR 488 and American case of New York Vs United States (1946) 326 US 572 at 587.
 18. Constitution of the Federal Republic of Nigeria, 1999 (As Amended), s.4(1)(2). Ogun State v. The Federation (1982) 3 NCLR 166 at 178; AG Ogun State v. Aberuagba (1985) 1 NWLR (pt.3) 395 at 413.
 19. Ibid. s.4(7). Olafisoye v. FRN (2004) 4 NWLR (PT.864) 580.
 20. AG Federation v. AG Abia State (2002) 6 NWLR (pt.764) 542. AG Abia State v. AG Federation (2006) 16 NWLR (pt.1005) 265. s.4(7)(a) &(c).
 21. Cybercrimes (Prohibition, Prevention, etc.) Act, 2015, long title.
 22. (1988) 2 NWLR (pt.78) 524.
 23. (1993) 1 NWLR (pt.269) 261.
 24. (1963) 55 CLR 324 at 339.
 25. (1915) 20 CLR 425 at 448.
 26. (1915) 19 CLR 629 at 634–635.
 27. AG Ondo State v. AG Federation (2002) 9 NWLR 9 (pt.772), 244, ratio 12.
 28. Interpretation Act, Cap. 192, Laws of the Federation (LFN), 1990, s.10(2).
 29. 4 Wheat. 316 (1819).
 30. (1963) 2 SCNLR 256–(1963) 1 WLR 949.
 31. Supra at 468.
 32. Ibid.
 33. Cybercrimes (Prohibition, Prevention, etc) Act, 2015, s.5.
 34. Ibid. s.6.
 35. Ibid. s.8.
 36. Ibid. s.9.
 37. Ibid. s.10.
 38. Ibid. s.11.
 39. Ibid. s.12.
 40. Ibid. s.13.
 41. Ibid. s.14.
 42. Ibid. s.15.
 43. Ibid. s.16.
 44. Ibid. s.18.
 45. Ibid. s.20.
 46. Ibid. s.22.
 47. Ibid. s.23.
 48. Ibid. s.24.
 49. Ibid. s.25.
 50. Ibid. s.26.
 51. Ibid. s.28.

52. Ibid. s.29.
53. Ibid. s.30.
54. Ibid. s.32.
55. Ibid. s.34.
56. Ibid. s.35.
57. Ibid. s.36.
58. CFRN. Part 1 of the Second Schedule, Item 62.
59. Mike Amadi v. Federal Republic of Nigeria (2008) 12 S.C (pt.III) 55; Harrison Odiawa v. Federal Republic of Nigeria (2009–2010) ECLR 19–99; (2008) All FWLR (pt.439) 436.
60. CFRN, Part 1 of the Second Schedule, Item 10.
61. Ibid. item 15.
62. Ibid. item 6.
63. Ibid. item 13.
64. Ibid. item 16.
65. Ibid. item 20.
66. Ibid. item 17.
67. Ibid. item 23.
68. Ibid. item 24.
69. Ibid. item 25.
70. Ibid. item 26.
71. Ibid. item 27.
72. Ibid. item 28.
73. Ibid. item 30.
74. Ibid. item 31.
75. Ibid. item 42.
76. Ibid. item 43.
77. Ibid. item 45.
78. Ibid. item 46.
79. Ibid. item 52.
80. Ibid. item 65.
81. Ibid. item 66.
82. Cybercrimes (Prohibition, Prevention, etc.) Act, 2015, Part III: Cybercrime offences & Penalties.
83. (1880) 5 Appeal Cases 473 HL.
84. Blacks Law Dictionary. 7th Edn.
85. 278 US 261, 73 L. ed. 495 in AG Ondo State v. AG Federation (supra) at 298.
86. Supra; AG Ondo State v. AG Federation (supra) at 399.
87. Ibid.
88. (1988) 2 NWLR (pt.78) 524.
89. (1993) 1 NWLR (pt.269) 261.
90. (1988) 2 NWLR (pt.78) 524.
91. (1993) 1 NWLR (pt.269) 261.
92. See generally AG Ondo State v. AG Federation (supra) at 413–414p.
93. Supra.
94. Supra at 538.
95. AG Ondo State v. AG Federation (supra) at 413–414p.
96. (1988) 2 NWLR (pt.78) 524.
97. (1993) 1 NWLR (pt.269) 291.
98. AG Ondo State v AG Federation (supra) at 414.
99. CFRN, Part 1 of the Second Schedule, Item 67.
100. Ibid.
101. Susan Brenner. *Crime vs. Cybercrime: Is the Law Adequate?* [Cited 2017 May 24]. Available from: http://www.circleid.com/posts/20050506_crime_vs_cybercrime_is_law_adequate/.
102. AG Ondo State v. AG Federation (supra) at 300.
103. Aminu Tanko v. The State (2009) LPELR–3136 SC.
104. CFRN 1999 (As Amended), s.4(2).
105. Ibid. s.4(7).
106. Glennon Michael J. State-level Cybersecurity. *Policy Review*. [Internet]. Feb–Mar 2012. [cited 2017 May 6]. Available from: <http://www.hoover.org/research/state-level-cybersecurity>
107. AG Ondo State v. AG Federation (supra) at 383.
108. Ibid. at 384.
109. The Emphasis is Mine.
110. Adebayo Shittu, FG Moves to Curb Cybercrime Threat to National Security. [Internet]. [cited 2017 May 13]. Available from: <https://www.thisdaylive.com/index.php/2016/08/03/fg-moves-to-curb-cybercrime-threat-to-national-security/>
111. Hassan AB, *et al.* Cybercrime in Nigeria: Causes, Effects and the Way Out. *ARNP Journal of Technology Science and Technology*. 2012; 2(7): 629p. Hemraj Saini, *et al.* Cyber-Crimes and their Impacts: A Review. *International Journal of Engineering Research and Applications*. 2012; 2(2): 205–207p. Maitanmi Olusola, *et al.* The Impact of Cyber Crimes on Nigerian Economy. *The International Journal of Engineering and Science*. 2013; 2(4): 45–51p. Nuhu Ribadu. Cybercrime and Commercial Fraud: A Nigerian Perspective, Modern Law for Global Commerce. *Proceedings of the Congress to Celebrate the Fortieth Annual Session of UNCITRAL*. [Internet]. Vienna. 9–12

- Jul 2007; 287–290p. [cited 2017 Mar 3]. Available from: https://www.uncitral.org/pdf/english/congress/09-83930_Ebook.pdf. Ehimen OR, *et al.* Cybercrime in Nigeria. *Business Intelligence Journal*. 2010; 3(1): 94p.
112. Wolf Pack, Digital Jewels. The Nigerian Cyber Threat Barometer Report 4, 6; 2014. [Internet]. [cited 2015 April 4]. Available from: <https://www.digitaljewels.net/index.php/resource-center/djlnews/129-the-2014-nigerian-cyber-threat-barometer>. ALoucif Kharouni, Africa: A New Safe Harbor for Cybercriminals? Trend Micro Incorporated Research Paper; 2013; 1p. [Internet] [cited 2015 April 10]. Available from: <http://www.trendmicro.nl/media/misc/africa-new-safe-harbor-for-cybercriminals-en.pdf>. Adomi EE, Adomi SE. Combating Cybercrime in Nigeria. *The Electronic Library*. 2008; 26(5): 718p. Internet Crime Complaint Center, 2010 *Internet Crime Report* (National White-Collar Crime Complaint Center: United States, 2011), 11 [Internet] [cited 2015 April 9]. Available from: <http://www.nw3c.org> or www.ic3.gov. Seun Ayantokun. Nigeria needs Anti-Cybercrime Law now—Minister. *Tribune*. [Internet]. Tuesday 15 Nov 2011. [cited 2015 April 3]; Available from: <http://www.tribune.com.ng/index.php/tele-info/31205-nigeria-needs-anti-cyber-crime-law-now-minister>. Agih L, Mibzar B. Nigeria: Cybercrimes-Nation Ranks Third in the World. *All Africa*. [Internet]. Feb 3, 2010. [cited Apr 2, 2015]; Available from: <http://www.alafrica.com/nigeria>. Eric Agwe-Mbarika Akuta, *et al.* Combating Cyber Crime in Sub-Saharan Africa: A Discourse on Law, Policy & Practice. *Journal of Research in Peace, Gender and Development*. May 2011; 1(4): 129, 132p. Okonigene Robert Ehimen, Adekanle Bola. Cybercrime in Nigeria. *Business Intelligence Journal*. 2009; 3(1): 95, 97p.
 113. See generally National White Collar Crime Center, 2002 to 2014 Internet Crime Reports. [Internet]. [cited 2015 July 10]. Available from: <http://www.ic3.gov/media/annualrepor>.
 114. Cybercrimes (Prohibition, Prevention, etc.) Act, 2015, s.3.
 115. Ibid. s.41(1).
 116. Ibid. s.41(2).
 117. Ibid. s.37.
 118. Ibid. Part VI.
 119. Ibid. s.38–40.
 120. Ibid. s.42–43.
 121. Ibid. s.44.
 122. See generally Eboibi FE. A Review of the Legal and Regulatory Frameworks of the Nigerian Cybercrimes Act 2015. *Computer Law & Security Review: The International Journal of Technology Law and Practice*. 2017; 33(5): 713–716p.
 123. (1951) 87 CLJ 369.
 124. Basu DD. *Commentary on the Constitution of India*. 5th Edn. Vol. 2. 311–312p. In AG Ondo State v. AG Federation (*supra*) at 305.
 125. (*supra*) at 383–384.
 126. Ibid.
 127. Ibid. Section 11(1): “The National Assembly may make laws for the federation or any part thereof with respect to the maintenance and securing public safety and public order and providing, maintaining and securing of such supplies and services as may be designated by the National Assembly as essential supplies and services.” Section 11(3): “During any period of when the federation is at war the National Assembly may make such laws for the peace, order, and good government of the federation or any part thereof with respect to matters not included in the Exclusive Legislative List as may appear to it to be necessary or expedient for the defense of the federation.
 128. (1963) 1 SCNLR 385.
 129. Ibid. Emphasis Mine. Per Mohammed JSC. In AG Ondo State v. AG Federation (*supra*) at 349–350.
 130. Ibid at 402–407.
 131. 301 US 619(1937). “that congress may spend money in aid of the general welfare and that the concept of general welfare was not static. The general welfare of old people as considered sufficiently proximate to the general welfare of the United States.”
 132. 379 US 241 (1964).
 133. (1882) AC 829.

134. (1925) AC 396 at 412, Lord Haldane.
135. (1946) A.C 193 at 205.
136. (1976) 68 DLR (Ed) 452.
137. (2001) 1 CHR 261: “that suitable and adequate shelter, suitable and adequate food, reasonable national minimum living wage, old age care pensions, and unemployment, sick benefits and welfare of the disabled are provided for all citizens.”
138. AG Ondo State v. AG Federation (supra) at 404–410, Emphasis Mine.
139. Constitution of the Federal Republic of Nigeria, 1999 (As Amended), ss.4(3) & 4(5). Military Governor, Ondo State v. Adewunmi (1988) 3 NWLR (Pt.82) 280 at 283.
140. (2002) 9 NSCQLR 670, 785, 788. In Naidike T. Doctrine of Covering the Field in Federal Constitutional Theory. [Internet] [cited 2017 May 6]. Available from: <https://tnaidike.wordpress.com/doctrine-of-covering-the-field-in-federal-constitutional-theory/>
141. (2002) FWLR (Pt.101) 1419.
142. Per Ogundare JSC. Attorney-General Abia State v. Attorney-General Federation (2002) FWLR (Pt.101) 1419; Emphasis mine.
143. (1988) 3 NWLR (Pt.82) 280 at 283.
144. CFRN, s.174(1) (a, b, c). Cybercrimes (Prohibition, Prevention, etc) Act, 2015, s.50.
145. Ibid. s.174(2).
146. Ibid. s.174(3).
147. (1983)! SCNLR 94.
148. AG Ondo State v. AG Federation (supra) at 418–419.
149. The Offences deals with financial institutions posting and authorized options (s.19) & reporting of cyber threats (s.21).
150. Cybercrimes (Prohibition, Prevention, etc.) Act, 2015, s.47(2).
151. (2003) 12 WRN 1, 30–31.
152. Terrorism (Prevention) Act 2011 amended by the Terrorism (Prevention) (Amendment) Act 2013.
153. Money Laundering (Prohibition) Act 2011(As Amended).
154. Naidike T. Doctrine of covering the field in Federal Constitutional Theory. [Internet]. [cited 2017 May 6]. Available from: <https://tnaidike.wordpress.com/doctrine-of-covering-the-field-in-federal-constitutional-theory/>
155. Cybercrimes (Prohibition, Prevention, etc.) Act, 2015, Part III; s.50(1) & AG Ondo State vs. AG Federation (supra) at 417.
156. Ibid
157. Helvering v. Davies 301 US 619 (1937).
158. Ibid.
159. AG Ondo State v. AG Federation at 403–404.

Cite this Article

Eboibi Felix E. The Regulation of Cybercitizens’ Conduct on Cyberspace: The Constitutionality and Applicability of the Nigerian Cybercrimes Act 2015. *National Journal of Cyber Security Law*. 2018; 1(1): 37–55p.