CONSTITUTIONALITY

OF THE

CYBERCRIMES (PROHIBITION, PREVENTION, ETC)

ACT 2015

BEING A PAPER PRESENTED

BY

MOFESOMO TAYO-OYETIBO[1], ACIArb

ON BEHALF OF TAYO OYETIBO, SAN, FCIARB, FNIALS

AT THE MEDIA INTERACTIVE SESSION ORGANISED BY THE SOCIO-ECONOMIC RIGHTS AND ACCOUNTABILITY PROJECT ON 'CONSTITUTIONALITY AND LEGALITY OF THE CYBER-CRIME ACT IN NIGERIA'

[1]Mofesomo Tayo-Oyetibo is the Managing Counsel of the Law Firm of Twelve Legal and an experienced Commercial Law, Dispute Resolution and Technology, Media and Telecommunications (TMT) lawyer. Email: mofe@twelvelegal.com

1.0. Proem

1.1. Crime has existed for as long as human beings have also been in existence. As human life has increased in complexity over the centuries, so have crimes and criminals also grown in complexity and relative ease. With the advent and widespread use of the internet, a new specie of crime previously unknown to and not contemplated by criminal statutes known as 'cybercrime' was birthed developed in both complexity and proliferation.

1.2. Like many other countries around the world, Nigeria could not ignore cybercrimes and had to enact specific legislation to deal with such crimes that are not necessarily captured by the general criminal statutes. This legislation is called the Cybercrimes (Prohibition, Prevention, Etc) Act 2015 (Cybercrimes Act). However, notwithstanding the noble intentions behind the enactment of the Cybercrimes Act, it has not been immune to criticism and challenge on the ground that it is unconstitutional under the Nigerian constitution.

1.3. Nevertheless, the Cybercrimes Act remains a statute in force and enforceable under Nigerian law and represents the only specific law on cybercrimes in Nigeria. However, it appears that questions as to its constitutionality are likely to linger for a while yet.

2.0. The Need for Cybercrimes Legislation

2.1. The internet has been one of the most revolutionary inventions of all time. In so many different ways, it has increased the quality of life of each and every person who has access to it by things such as bringing an unlimited amount of information to their doorstep and also giving them the opportunity to connect with people all over the world instantly and conveniently. Without the internet, life, as we know it today, would have been greatly hampered because certain functions would just be incapable of performance. Notwithstanding all of its immeasurable benefits well-intentioned users, the internet also presents an opportunity for those who have access to it and are criminally-intentioned to misuse it. It is within this realm of opportunity that the specie of crime known as cybercrime thrives.

2.2. According to the Nigerian Communications Commission[2], *"cybercrime is generally defined as a criminal offence involving a computer as the object of the crime (hacking, phishing, spamming), or as the tool used to commit a material component of the offence (child pornography, hate crimes, computer fraud)".*The nature of cybercrimes means that, although they can be perpetrated at relative ease and minimal expense, they can have devastating consequences that transcend national borders.

2.3. According to the United Nations Office on Drugs and Crime[3], cybercrimes are an evolving form of transnational crime that takes place in the border-less realm of cyberspace, the complex nature of which is compounded by the increasing involvement of organized crime groups. Since perpetrators of cybercrimes and their victims can and are many times located in different countries or even continents and its effects can reverberate all around the world, there is the pressing need for dynamic and effective policy and legislative response across the world.

3.0. The Cybercrimes Act

3.1. Before the year 2015, Nigeria did not have any specific piece of legislation to deal with cybercrimes and following the international and domestic need to ensure that cybercrimes do not continue to originate from Nigeria, in the absence of specific criminal law on the subject, the Cybercrimes Act was passed into law in 2015. According to the explanatory memorandum of the Cybercrimes Act, the Act is aimed at providing an effective, unified and comprehensive legal, regulatory and institutional framework for the prohibition, prevention, detection, prosecution and punishment of cybercrimes in Nigeria.

3.2. The Act is also to ensure the protection of critical national information infrastructure and promotion of cybersecurity and the protection of computer systems and networks, electronic communications, data and computer programs, intellectual property and privacy rights in Nigeria. By its long title, the Cybercrimes Act is an Act to provide for the prohibition, prevention, detection, response, investigation and prosecution of cybercrimes

[2]https://www.ncc.gov.ng/documents/735-nmis-effects-cybercrime-foreign-direct-investment/file
[3]https://www.unodc.org/unodc/en/cybercrime/index.html

and for other related matters. It contains 59 sections and introduces previously novel obligations and offences into Nigerian criminal law, some of which are:

a) Offences against critical national information infrastructure;
b) The criminalisation of unlawful access to computers;
c) The criminalisation ofwilful misdirection of electronic messages and unlawful interceptions;
d) The criminalisation ofcyber-terrorism and cyber-stalking;
e) The legalisation of electronic signatures; and
f) Data retention obligations on service providers.

3.3. The Cybercrimes Act also establishes the National Cyber Security Fund, although it curiously contains no provisions on how monies accruing into the Fund are to be spent.

4.0. Legislative Framework Under the Nigerian Constitution

4.1. Nigeria operates a written constitution, which is the Constitution of the Federal Republic of Nigeria 1999 (The Constitution). The constitution is the grundnorm and the basic law from which all other laws of the society derive their validity. On this point, **Kekere-EKun, JSC** described the supremacy of the Nigerian constitution in the case of **SARAKI v FEDERAL REPUBLIC OF NIGERIA**[4]in the following terms:

> ***"The Constitution is the supreme law of the land. It is the grundnorm i.e. it is the basic law from which all other laws of the society derive their validity. Section 1(1) of the 1999 Constitution (as amended) provides: 1(1) This Constitution is supreme and its provisions shall have binding force on all authorities and persons throughout the Federal Republic of Nigeria. (3) If any other law is inconsistent with the provisions of this Constitution, this Constitution shall prevail, and that other law shall, to the extent of the inconsistency be void."***

[4] (2016) LPELR-40013(SC)

4.2. Under Nigeria's constitutional framework the National Assembly, which consists of the Senate and House of Representatives, is the body or arm of government vested with the legislative powers of the Federal Republic of Nigeria[5]. Pursuant to its legislative powers, the National Assembly is fixed with the responsibility of making laws for the peace, order and good government of the Federation or any part thereof with respect to matters placed within its legislative purview by the constitution[6]. Specifically, the matters in respect of which the National Assembly is empowered to make laws, to the exclusion of the States' Houses of Assembly, are those contained in the Exclusive Legislative List set out in Part I of the Second Schedule to the Constitution[7].

4.3. In addition to this exclusive legislative power, the National Assembly also has an additional concurrent legislative power with the States' Houses of Assembly to make laws with respect to any matter in the Concurrent Legislative List set out in the first column of Part II of the Second Schedule to the Constitution[8] as well as a general power to make laws concerning any other matter with respect to which it is empowered in accordance with the provisions of the constitution[9].

4.4. As a consequence of the foregoing, and by virtue of the specific provisions of section 4(7) of the Constitution, the States' Houses of Assembly have power to make laws for the peace, order and good government of their respective states or any part thereof with respect to any matters not contained in the aforementioned Exclusive Legislative List, matters contained in the Concurrent Legislative List and generally any other matter with respect to which they are empowered by the constitution to make laws. Any matter that is not contained on either the Exclusive or Concurrent Legislative List is considered under the constitution to be a 'residual' one in respect of which only the States' Houses of Assembly have power to make laws, to the exclusion of the National Assembly.This same point was made by **Bello, JSC** in **AG OGUN STATE V ABERUAGBA**[10] as follows:

---

[5]See section 4(1) of the constitution
[6]See section 4(2) of the Constitution
[7]See section 4(3) of the constitution
[8]See section 4(4)(a) of the Constitution
[9]See section 4(4)(b) of the Constitution
[10](1985) NWLR (Pt 3) 395

> ***"A careful perusal and proper construction of section 4 would reveal that the residual legislative powers of government were vested in the States. By residual legislative powers within the context of section 4, is meant what was left after the matters in the Exclusive and Concurrent Legislative Lists and those matters which the Constitution expressly empowered the Federation and the States to legislate upon had been subtracted from the totality of the inherent and unlimited powers of a sovereign legislature. The Federation had no power to make laws on residual matters."***

4.5. The legislative powers of the National Assembly and States' Houses of Assembly are under the strict regulation of the express provisions of the constitution from which the powers are derived. Consequently, where the National Assembly or States' Houses of Assembly make any law that is not within their legislative competence under the constitution, any such legislative body will be acting outside its legislative power under the constitution and therefore *ultra vires*, as observed by **Tobi, JSC** in **OLAFISOYE V FRN**[11] as follows:

> ***"An act is ultra vires in the National Assembly when it is enacted outside the legislative powers of the National Assembly. Where the enactment of an act is within the legislative powers or the legislative competence of the National Assembly, such an act is intra vires in the National Assembly."***

4.6. Having regard to the foregoing legislative framework under the Nigerian constitution and the fact that the Cybercrimes Act is an Act of the National Assembly, to determine the constitutionality or otherwise of the Cybercrimes Act, the starting point must necessarily

[11] (2004) 4 NWLR (Pt. 864)580

be a consideration of the legislative competence of the National Assembly to pass the Act in the first place.

5.0. The Power of the National Assembly to Legislate on Cybercrimes

5.1. The determination of the constitutionality of the Cybercrimes Act, from an extrinsic perspective, turns on the important question of whether the National Assembly has the legislative competence to make a law relating to cybercrimes in Nigeria. In this regard, the starting point is invariably a consideration of the items contained in the Exclusive and Concurrent Legislative Lists, in respect of which the National Assembly is empowered to make laws for Nigeria. The Exclusive Legislative List is contained in Part I of the Second Schedule to the constitution and contains a total of sixty-eight items covering a wide spectrum of matters in respect of which the National Assembly has the exclusive power to make laws. The last two items on the list are general powers for the National Assembly to make laws in respect of any other matter with respect to which it has specific power to make laws under the constitution and any matter incidental or supplementary to any matter mentioned elsewhere in the list.

5.2. As a specific legislative item, 'cybercrime' is not expressly mentioned on the Exclusive Legislative List. It is also not an item specifically mentioned on the Concurrent Legislative List as a matter in respect of which both the National and States' legislatures have concurrent powers to make laws. The fact that cybercrimes is not expressly listed as a legislative item or matter on either the Exclusive or Concurrent Legislative Lists may lead one to generally reach the conclusion that it is a residual matter in respect of which, to the exclusion of the National Assembly, only the States Houses of Assembly have the powers to make laws. However, for certain reasons, a more critical look at the provisions of the constitution and relevant judicial authorities appear to point to a different conclusion altogether.

5.3. Firstly, there is no doubt that cybercrimes have had a significant impact on Nigerians as a people and Nigeria as a country not only in social but also economic terms. From a social standpoint, cybercrimes have had an impact on the manner in which Nigerians are

received abroad and even contributed significantly to the erosion of trust amongst and for Nigerians domestically and abroad.

5.4. Economically, cybercrimes have resulted in significant pecuniary losses to Nigerians and Nigeria as a country in terms of lost revenue and economic opportunities. A report by the Nigerian Communications Commission's Department on New Media and Information Security on the "Effects of Cyber Crime on Foreign Direct Investment and National Development"[12] puts this into some context, in the following terms:

> ***"Cybercrime has also had an implication in the foreign direct investment advancement into the country, as information flowing from the country is been characterized as questionable because of the criminal elements which make it unreliable, inaccurate and untrustworthy. Indeed, one cannot overemphasize the investment sabotage resulting from cybercrime in Nigeria. In 2014, a report by the South African based Institute of Digital Communication indicates that Nigeria is losing about $80 million dollars yearly to software piracy alone. Similarly, in 2015, an estimated customer loss of ₦2,146,666,345,014.75 ($13,547,910,034.80) was incurred to cybercrime in Nigeria. In highlighting the foreign investment consequences of cybercrime in Nigeria, Folashade and Abimbola, (2013) posits that cybercrime hinders the foreign investment opportunities of the country as it engenders lack of trust and confidence in profitable transactions, promotes denial of innocent Nigerian business opportunities abroad and causes loss of employment, revenue loss as well as capital flight. Cybercrime impedes national development as it scares away foreign investors due to the low level of confidence***

[12]https://www.ncc.gov.ng/documents/735-nmis-effects-cybercrime-foreign-direct-investment/file

> ***it has created for the Nigerian economy. Cybercrime has aided other illicit activities in Nigeria such as intellectual plagiarism, disruption of public services, drug trafficking, and terrorism."***

5.5. Having regard to the foregoing, it is an undeniable fact that the perpetuation of cybercrimes not only across the Federation of Nigeria but overseas by persons within Nigeria has become an issue of serious national concern and importance that cannot be ignored or waved away in any way. Furthermore, offences falling within the meaning of cybercrimes have been judicially noticed, such that the Court of Appeal in the case of **ODIAWA V FEDERAL REPUBLIC OF NIGERIA**[13]held the view that cybercrimes are of the same seriousness as the heinous crime of armed robbery. In that case, **Dongban-Mensem, JCA** said that:

> ***"The crime which colloquially has come to be known as "419" and the constitutive term of which is now known as Advanced Fee Fraud is a well-premeditated crime. It is like the crime of Armed Robbery. The only difference here is that words, the internet, letters and telephones, are the "arms" rather than "guns" and other lethal weapons. The criminal can commit his crime in the comfort of his bedroom. The common feature of the two crimes are the planning for the executions; like the armed robbers who sometimes use masks, with internet robbery, the perpetrators, employ all sorts of gimmicks to cover up their trails."***

5.6. Secondly and against the foregoing backdrop, as it is undeniable that the consequences of cybercrimes in Nigeria affect Nigerians on an individual basis and the Federation or Federal Republic of Nigeria as a whole, there is justifiable reason to reach the conclusion that cybercrimes pose a threat to the peace, order and good government of Nigeria, by reason of which it falls within the legislative purview of the National Assembly under

[13](2008) LPELR-4230(CA)

section 4(2) of the Constitution. This is because it is a settled principle of Nigerian constitutional law that provisions of the constitution are to be read in a wide and liberal manner with a view to giving full effect to the intentions of its framers. See **ATTORNEY-GENERAL OF LAGOS STATE V. THE ATTORNEY-GENERAL OF THE FEDERATION & ORS**[14]and **NAFIU RABIU V. THE STATE.**[15]

5.7. In this respect, the decision of the Supreme Court in the case of **ATTORNEY GENERAL OF ONDO STATE V ATTORNEY GENERAL OF THE FEDERATION AND OTHERS**[16] (The Ondo Case) provides some very useful guidance.

5.8. In the Ondo Case the government of Ondo State brought an action pursuant to the original jurisdiction of the Supreme Court to seek a determination by the court of the question of whether the National Assembly had the legislative competence to enact the Corrupt Practices and Other Related Offences Act 2000 (ICPC Act). Here, Ondo State contended that since "corruption" is not a specific subject under either the exclusive or the concurrent legislative lists and therefore a residual matter, the National Assembly had no power to legislate upon it. However, in determining the case, the Supreme Court held that the contention of Ondo State overlooked the provisions of section 4(4)(b) of the constitution, which states that the National Assembly has the power to legislate on any matter with respect to which it is empowered to make law in accordance with the provisions of the constitution. Specifically, in his contribution, Mohammed, JSC made the point that:

> ***"It is quite plain that the issue of corruption in Nigerian society has gone beyond our borders. It is no more a local affair. It is a national malaise, which must be tackled by the Government of the Federal Republic. The disastrous consequences of the evil practice of corruption has taken this nation into the list of the most corrupt nations on earth. In Re-anti-Inflation Act (1976) 9 NR 541; 68 DLR G (3d) 452 the Supreme court of***

[14](2003) LPELR-620(SC)
[15](1980) 8-11 SC 130
[16] (2002) 9 NWLR (PT772) 222

Canada saw no reason why the "emergency" principle enunciated in Japanese-Canadian's case could not apply to a situation created by highly exceptional economic conditions prevailing in times of peace. In the opinion of the Supreme Court of Canada it was observed that an urgent and critical situation adversely affecting all Canadians and being of such proportions as to transcend the authority vested in the Legislatures of the Provinces and thus presenting an emergency which can only be effectively dealt with by parliament in the exercise of the powers conferred upon it by section 91 of the British North American Act, 1867 "to make laws for the peace, order, and good government of Canada." Coming back home it is abundantly clear that the intendment of the framers of the Constitution in providing that the State shall abolish all corrupt practices and abuse of power is not to use the information media only to discourage corrupt practices. It also cannot be said that only State governments and Local government are to enforce this Fundamental Objectives. How then can the Nation tackle this evil practice? The answer is clear; a criminal law has to be promulgated providing that every person shall be liable to punishment for every act or omission contrary to the Corrupt Practices etc. Act, 2000, which he shall be found guilty of committing. This is the only way the evil of corruption can be tackled nationally."

Similarly, **Ogwuegbu, JSC** observed that:

"Section 4(2) of the constitution conferred on the National Assembly power to make laws for the peace, order and good government of the federation or any part thereof with respect to any matter included in the

exclusive legislative list set out in part 1 of the second schedule of the constitution. Section 4 of the constitution recognises the need for peace, order and good government in relation to Nigeria as a nation just as it recognises the need for peace, order and good government in relation to each separate state of the federation hence it conferred power on the National Assembly to enact laws to achieve that objective. Corrupt practices and abuse of power can, if not checked threaten the peace, order and good government of the Federation or any part thereof…I have held in this judgment that the National Assembly can exercise the powers which it does possess for the purpose of assisting in carrying out a policy which may affect matters which are directly within its legislative competence. It can also exercise powers, which it does possess for assisting in carrying out a policy, which may affect matters not directly within its legislative powers."

5.9. Having regard to the similarities in the issues concerned and the consequences of corruption and cybercrimes offences on Nigeria as a country, both domestically and internationally, there is ample legal justification for the application of the decision of the Supreme Court in the Ondo Case as authority for the proposition that the National Assembly has the legislative competence to enact a law on cybercrimes. This position is reinforced by the fact that some of the matters stated to be within the fundamental regulatory objectives of the Cybercrimes Act fall within the Exclusive Legislative List. The objectives of the Cybercrimes Act are set out in section 1 of the Act and they are to:

(a) provide an effective and unified legal, regulatory and institutional framework for the prohibition, prevention, detection, prosecution and punishment of cybercrimes in Nigeria;

(b) ensure the protection of critical national information infrastructure; and

(c) promote cyber security and the protection of computer systems and networks, electronic communications, data and computer programs, intellectual property and privacy rights.

5.10. For instance, in relation to section 1(b) of the Cybercrimes Act, which relates to critical national information infrastructure, section 58 of the same Act defines "Critical infrastructure" to mean ***"systems and assets which are so vital to the country that the destruction of such systems and assets would have an impact on the security, national economic security, national public health and safety of the country."***In this case, there is nothing in the constitution to suggest that the States' Houses of Assembly have the legislative competence to make laws for the regulation of the national economy, security and assets, which in any case transcend their geographical and legislative borders. An otherwise conclusion appears to not only be impractical but against the spirit of the constitution as a whole whereby legislative powers on matters that relate to the peace order and good government of the Federation of Nigeria are for the national Assembly.

5.11. With respect to section 1(c) of the Cybercrimes Act, there is wide enough scope to conclude that the National Assembly can legislate on "computer systems and networks, electronic communications, data and computer programs, intellectual property and privacy rights" due to the fact that they fall within the items listed as numbers 13, 43 and 66, which respectively relate to the intellectual property rights of "copyright" and "trademarks" and also "wireless".

5.12. Although there is, at present, no judicial authority on the specific question of whether the National Assembly has the legislative competence to legislate on Cybercrimes, having regard to the foregoing, there is good reason to conclude that despite the fact that cybercrimes is not expressly listed in either the Exclusive or Concurrent Legislative Lists, it is well within the legislative competence of the National Assembly to legislate on cybercrimes. An alternate conclusion that it is within the exclusive legislative competence of the States' Houses of Assembly would no doubt create an absurdity.

6.0. The Constitutionality of the Cybercrimes Act Provisions

6.1. As has already been stated above, the supremacy of the constitution over every other law is an immutable principle of Nigerian constitutional law derived from the provisions of section 1(3) of the constitution itself, which provides that:

> ***"If any other law is inconsistent with the provisions of this constitution, this constitution shall prevail, and that other law shall to the extent of the inconsistency be void."***

6.2. Based on the premise that, from an extrinsic perspective, the Cybercrimes Act is constitutional under section 4(2) of the constitution in the sense that it was validly enacted by the National Assembly, the next point of consideration is intrinsic in nature. Such a consideration has to do with the question of whether the Cybercrimes Act contains any specific provisions that are inconsistent with the provisions of the constitution and therefore void and unconstitutional under section 1(3) of the constitution to the extent of the inconsistency.

6.3. In this respect, two specific provisions of the Cybercrimes Act are particularly relevant and they are sections 24 and 38. Section 24 of the Cybercrimes Act provides for the criminalisation of the sending of certain types of offensive messages, whilst section 38 provides for the retention of traffic data and subscriber information by service providers. Before now, these two provisions of the Cybercrimes Act have been challenged in court on the ground that they are unconstitutional and consequently void by virtue of the provisions of section 1(3) of the constitution. Two of these decisions will be considered here.

6.4. The first case to be considered is the decision of the Court of Appeal in the matter of **THE INCORPORATED TRUSTEES OF PARADIGM INITIATIVE FOR PERFORMATION TECHNOLOGY DEVELOPMENT & 2 OTHERS V THE ATTORNEY GENERAL OF THE**

FEDERATION & 2 OTHERS[17](The PIPTD Case)**.** In this case, the Appellant had approached the Federal High Court seeking to nullify section 38 of the Cybercrimes Act on the ground that it is *"illegal, unconstitutional and in violation or likely to further violate the Appellants' fundamental rights to privacy, correspondence, telephone conversations and telegraphic communications as guaranteed under section 37 of the constitution."* In addition, the Appellants also sought a nullification of section 24 of the Cybercrimes Act on the ground that it is *"illegal, unconstitutional as it violates and is likely to further violate the Appellants' fundamental rights to freedom of expression and the press guaranteed by section 39 of the 1999 Constitution."*For ease of reference, the aforementioned sections 37 and 39 of the constitution generally provide for and guarantee the fundamental rights of persons to privacy and freedom of expression respectively.

6.5. The Appellants in the PIPTD case argued in the appeal that section 24 of the Cybercrimes Act seeks to curtail the rights of persons to impart and receive information and ideas of all kinds freely guaranteed as a fundamental right under section 39 of the constitution and is to that extent not reasonably justifiable in a democratic society. On section 38 of the Cybercrimes Act, the Appellants argued that the section amounts to a restriction on the right to freedom of expression by undermining the ability of internet users to communicate anonymously online and their also their privacy.

6.6. Furthermore, the Appellants were of the view that the requirement by section 38 of the Cybercrimes Act for service providers to disclose online user data to law enforcement agencies not only inhibits open communication and robust debate but also violates freedom of speech and the privacy of online users. With respect to both sections 24 and 38 of the Cybercrimes Act, the Appellants argued that the sections ought to be struck down by the court, having regard to the fact that similar provisions in laws enacted in India[18] and Kenya[19] were struck down on the ground of unconstitutionality.

6.7. In its final decision, the Court of Appeal rejected all of the Appellants' arguments and held that once an Act is passed by the legislature, there is the presumption of regularity under

---

[17] Unreported decision of the Court of Appeal (Lagos Division) delivered on 1st June, 2018 in **APPEAL NO. CA/L/556/2017**

[18]Section 66a of the Information Technology Act 2000

[19]Section 29 of the Kenya Information and Communication Act

section 168(1) of the Evidence Act 2011 that it was made with the inclination, belief and notion that it is reasonably justifiable in a democratic society under section 45(1) of the constitution and any party asserting otherwise has the burden of proving the assertion. In the PIPTD case, the Court of Appeal held that the Appellants had not discharged their legal burden of proving the Cybercrimes Act was made by the National Assembly in violation of the constitution. It was further held that the foreign authorities relied upon by the Appellants were not relevant to the determination of the constitutionality of sections 24 and 38 of the Cybercrimes Act because the constitutional provisions upon which the laws in those countries were struck down were not the same as those of Nigeria and cannot be used as precedent to achieve the same aim under the Nigerian constitution.

6.8. Specifically, the court held in respect of section 24 of the Cybercrimes Act that the section is one with a specific agenda on public welfare/well-being and has to do with correct and decent conduct. The court held that section 24 is designed to control and curb the passions of humankind and enhance public welfare/well-being, which includes the well-being of the society in matters of health, safety, order, morality, economics and politics. According to the court, the constitutional right and mandate to legislate on public welfare/well-being is vested in the legislature by sections 4 and 45(1)(a) of the constitution, by reason of which section 24 of the Cybercrimes Act is not unconstitutional but simply a piece of criminal legislation.

6.9. Concerning section 38 of the Cybercrimes Act, the court held, also based on and in addition to its decision on section 24 of the Act, that a service provider under section 38 of the Cybercrimes Act is a stakeholder in the administration of criminal justice and the said section is a veritable law enforcement tool for the detection and investigation of crime for the common good. The court decided that section 38 of the Cybercrimes Act merely accentuates what is universally accepted that every member of society must partner with law enforcement for the effective enforcement of criminal legislations. Ultimately, the court reached the conclusion that section 38 of the Cybercrimes Act is not unconstitutional. This is particularly in view of the fact that the court had already also reached the conclusion that, by reason of its subsection (4), section 38 of the

Cybercrimes Act actually safeguards the constitutional privacy of data retained, processed or retrieved pursuant to the same section.

6.10. Looking at the decision of the Court of Appeal in the PIPTD case, it is abundantly clear that the Court of Appeal was not in any way convinced that sections 24 and 38 of the Cybercrimes Act went far enough to violate the constitutionally guaranteed rights of persons to privacy and freedom of expression.

6.11. With respect to section 38 of the Cybercrimes Act, having regard to the objectives of the Cybercrimes Act stated in its section 1, the provisions of its section 38(5) and based on the fact that by section 45(1) of the constitution nothing in sections 37-41 of the constitution shall invalidate any law that is reasonable justifiable in a democratic society, it would appear that the ultimate decision of the Court of Appeal in the PIPTD case is correct on its face. This is particularly as, in this case, it does not at all appear that the Appellants had placed any specific and legally cognizable facts before the court to discharge their burden of proving that section 38 of the Cybercrimes Act was not enacted in the interest of defence, public safety, public order, public morality, public health or for the purpose of protecting the rights and freedoms of other persons.

6.12. By reason of section 38(5) of the Cybercrimes Act, it would most certainly be difficult for any court to reach the general conclusion that section 38 of the Act is unconstitutional, particularly in the absence of compelling specific factual evidence to the contrary. The said section 38(5) provides that:

> ***"Anyone exercising any function under this section shall have due regard to the individual's right to privacy under the Constitution of the Federal Republic of Nigeria, 1999 and shall take appropriate measures to safeguard the confidentiality of the data retained, processed or retrieved for the purpose of law enforcement."***

6.13. Going by the above provision, it certainly does appear that the National Assembly had spotted that section 38(1), (2) and (3) have the potential to be construed as being in

violation of the constitutional right to privacy and sought to include subsection (5) as a safeguard.

6.14. However, notwithstanding the inclusion of subsection (5) in section 38, the section still has some inherent issues relating to the privacy of persons. In this regard, section 38(2) of the Act, which makes it compulsory for service providers to release any information kept under subsection (1) to the "relevant authority", comes to mind. The phrase "relevant authority" is not defined in the Cybercrimes Act, which raises the question as to whether service providers, for fear of criminal sanctions, may be coerced into releasing ordinarily confidential information to any government authority claiming to be a "relevant authority" under the Act.

6.15. Most certainly, a better scenario would have been for the service providers to be bound to release such information to specific law enforcement agencies that require the information in the course of carrying out their legitimate law enforcement functions but subject only to the fulfilment of some stipulated procedural conditions or supervision of the court. In his concurring judgment in the PIPTD case, **Georgewill, JCA** held a similar view when, although ultimately concluding that section 38 of the Cybercrimes Act is not unconstitutional, he observed in some detail that:

> ***"In my humble opinion to leave the provisions of subsections 2(b) and 3 of section 38 of the Cybercrimes Act 2015 as it is would clearly be and indeed amount to an invitation and encouragement of unbridled interference with the rights of the citizen to the privacy of their communications at the whims and caprices of the relevant authority or law enforcement agencies…The provisions of sections 37 and 39 of the Constitution of Nigeria 1999 (as amended), though not absolute, is sacrosanct and must not be made nonsense of by provisions of any law capable of exposing those rights to jeopardy without any legal check…To provide that the request for information should be made at the whims***

and caprices of the 'relevant authority' or "any law enforcement agency" and be complied with before any consideration for the genuine purpose of such a request could be determined without any prior control measures or checks put in place in the legislation is itself akin to putting the cart before the horse…It is for the above reasons that I am of the strong view that though section 38 of the Cybercrimes Act 2015 is neither unconstitutional nor null and void, there is need for its amendment by the legislature, the 2nd Respondent, to introduce a subsection requiring the obtaining of an ex-parte order of a court of competent jurisdiction as a precondition for any request and release of information under the Cybercrimes Act 2015. In the absence of such a check or safeguard, it does appear to me that the citizens would be left at the whims and caprices of the 'relevant authority' and or 'law enforcement agency' and which undoubtedly would lead to impunity in derogation of these right as guaranteed by the constitution to the citizenry of this great nation of ours, which is not and cannot be the intention of the framers of the constitution."

6.16. The second decision to be considered here is that of the Federal High Court in the case of **OKEDARA V ATTORNEY GENERAL OF THE FEDERATION**[20]where the Plaintiff challenged section 24 of the Cybercrimes Act on the ground that it violates sections 36(12) and 39 of the constitution and is therefore unconstitutional. The arguments made by the Plaintiff in **OKEDARA's** case are very similar to those made by the Appellants in the PIPTD case and need not be reconsidered here.

[20]Unreported decision of Buba J. delivered on 7th December, 2017 in **FHC/L/CS/937/2017**

6.17. Just as in the PIPTD case, the court in **OKEDARA's** case reached the conclusion that section 24 of the Cybercrimes Act is not unconstitutional. In reaching its decision, the court held that section 24 of the Cybercrimes Act does not *"in any way conflict with section 36(12) of the 1999 Constitution of the Federal Republic of Nigeria. The offences as contained in section 24(1) of the Cybercrimes Act is (sic) quite clear and defined and penalty prescribed in the law creating same."* Further, the court held that taken together with the other provisions of the Act, section 24 of the Cybercrimes Act was made in the interest of defence, public safety, public order, public morality and public health by reason of which the said section is in the interest of the generality of the public.

6.18. Although the decision of the Court of Appeal in the PITPD case is presently on appeal to the Supreme Court, both the decision in that case and **OKEDARA's** case presently represent the position of the law as to the constitutional validity of sections 24 and 38 of the Cybercrimes Act. Nevertheless, there is significant scope to posit, specifically concerning section 24 of the Cybercrimes Act, that the courts' decisions in the PIPTD and Okedara's cases possibly ought to have been different from what they are. To illustrate this point, it is necessary to look a little closer at the specific provisions of section 24 of the Cybercrimes Act. Section 24(1) criminalises the intentional sending, by means of computers:

a. ***Messages that are grossly offensive, pornographic, indecent, obscene or menacing in character; and***
b. ***False messages for the purpose of causing annoyance, inconvenience, danger, obstruction, insult, injury, criminal intimidation, enmity, hatred, ill will or needless anxiety to another person.***

6.19. In Nigerian criminal law, two elements must generally be present for a conduct to constitute a criminal offence and they are *actus reus* and *mens rea*, which mean 'guilty act' and 'guilty mind' respectively. Essentially, for a person to be found to have committed a criminal offence, he must know what constitutes the offence and have committed the

offence with the requisite *mens rea*. This point was illustrated by the Supreme Court in the case of **IDAGU V STATE**[21] where **Augie, JSC** held that:

> ***"It is a fundamental principle of criminal law that a crime consists of both a mental and a physical element. Mens rea, a person's awareness that his or her conduct is criminal, is the mental element, and actus reus, the act itself is the physical element. The concept of mens rea, which is Law Latin for "guilty mind", developed in England around the year 1600, when Judges began to hold that an act alone could not create criminal liability unless it was accompanied by a guilty state of mind. The degree of mens rea required for a particular common law crime varied then' In other words, mens rea is a criminal intention or knowledge that an act is wrong, and today most of the crimes are defined by statutes that generally contains a word or phrase indicating the mens rea requirement."***

6.20. Using the above pronouncement of the Supreme Court as a backdrop, it is beyond doubt that any statute that criminalises a certain conduct ought to indicate both the *actus reus* and the *mens rea* element of the offence. It is against the backdrop of this fundamental principle of law that section 36(12) of the Constitution provides that:

> ***"Subject as otherwise provided by this Constitution, a person shall not be convicted of a criminal offence unless that offence is <u>defined</u> and the penalty therefor is prescribed in a written law, and in this subsection, a written law refers to an Act of the National Assembly or a Law of a State, any subsidiary legislation or instrument under the provisions of a law."*** (Underlining for emphasis)

6.21. The logical corollary of the foregoing is that for any criminal statute to meet the requirement of constitutional validity under section 36(12) of the constitution, offences

[21] (2018) LPELR-44343 (SC)

created by the statute must be clearly defined both in terms of the *mens rea* and *actus reus* elements of the offences. By this reasoning, actions that constitute criminal offences must be readily ascertainable from reading the provisions of the statute and not left to the possible lottery of judicial interpretation by the courts. This same point was aptly made by the Supreme Court in **TAFIDI V FRN** [22] where **Akaahs, JSC** held that:

> ***"Any conduct which carries a sanction of imprisonment must be expressly stated in a written law and not left to conjecture or inference by the court."***

6.22. **Does section 24(1) of the Cybercrimes Act meet the aforementioned constitutional requirement?** It appears that the answer to this question is in the negative, as will be demonstrated below.

6.23. In creating criminal offences, section 24(1) of the Cybercrimes Act uses words that are entirely subjective in meaning to describe the *actus reus* elements of the offences, despite the fact that the *actus reus* of an offence ought to be capable of objective and not subjective definition[23]. Worse still, the Cybercrimes Act makes no effort to give certainty to the meanings of any of the words used in its section 24(1) by defining them anywhere in the Act, which means that only judicial definitions can be given to those words in any case where a person is charged with an offence under section 24(1) of the Act.

6.24. From a practical standpoint, it means that a person charged with an offence under section 24(1) of the Cybercrimes Act will involuntarily be playing the lottery of judicial interpretation of the words and phrases used in that section. This is because virtually all of the words used in section 24(1) of the Act are of such personal character that, any attempt to define them is entirely subject to the whims and caprices of two different sets of people- complainants and judges. The reality of this scenario is laid bare when one considers the fact that a message that is "***grossly offensive, pornographic, indecent, obscene or menacing in character"*** to one set of people may not at all be to a different set of people. Similarly, a message that causes ***"annoyance, inconvenience danger,***

---

[22] (2013) LPELR-21859(SC)

[23] Norman J. Finkel and Jennifer L. Groscup, 'Crime Prototypes, Objective versus Subjective Culpability, and a Commonsense Balance' Law and Human Behavior Vol. 21, No. 2 (Apr., 1997), pp. 209-230

obstruction, insult, enmity, hatred, ill will or needless anxiety" to one set of people may not in any way do so to a different set of people.

6.25. As a matter of fact, it is commonplace for human beings, in the middle of a civil or even domestic dispute, to use and communicate to each other words that are deliberately intended to offend, insult or express hatred for the other person. This means that, under section 24(1) of the Cybercrimes Act, a regular civil or domestic dispute in which unsavoury words are exchanged can easily be escalated into the realm of criminality. Consequently and invariably, the manner in which a person will receive or define a message of the kind described in section 24(1) of the Cybercrimes Act would depend entirely on the person's age, gender, ethnicity, cultural background, temperament, mentality, sense of bias, etc, which are not factors contemplated by section 36(12) of the constitution in the definition of a criminal offence by a statute.

6.26. In essence, contrary to the undisputed position of the law stated by the Supreme Court in **TAFIDI V FRN**[24], it is impossible for a person to be convicted of an offence under section 24(1) of the Cybercrimes Act without conjecture or inference by the court as to the meanings of the words used in that section. Worse still, such conjecture or inference can only be imputed by the court at the point of delivering judgment in the matter, at which point the accused person will not have had the opportunity to be heard by the court as to the court's interpretation of the meanings of those words and phrases. In this respect, there will no doubt be the question of whether such proceedings do not violate the accused person's right to fair hearing under section 36(1) and (6)(a) of the constitution.

6.27. The point being made here is reinforced by the outcome of a comparison of section 24(1) of the Cybercrimes Act with 24(2) of the same Act. Unlike section 24(1) of the Cybercrimes Act, section 24(2) of the Act criminalises the commission of certain acts that are readily capable of generally acceptable objective definition. For instance, the question of whether a message places another person fear of "*death, violence or bodily harm*", threatens kidnap or threatens to harm the property or reputation of a person is hardly one that is open to such a wide spectrum of interpretation that it is incapable of general definition. Such a question is not one that will be open to speculation or conjecture by the

[24] supra

courts in the determination of whether a particular conduct constitutes a criminal offence under section 24(2) of the Cybercrimes Act.

6.28. Apart from the above, every person is constitutionally guaranteed the right to freedom of expression, including freedom to hold opinions and to receive and impart ideas and information without interference under section 39(1) of the constitution. A scenario in which a person is bound by section 24(1) of the Cybercrimes Act to second-guess the exercise of his right to freedom of expression under section 39(1) of the constitution is certainly not one contemplated by the constitution in any way. At this point, the dictum of **Adekeye, JCA** in **IGP V ANPP**[25] comes to mind, where the Court of Appeal observed that:

> ***"I hold in unison with the reasoning in the case of Shetton v. Tucker 364 US 479, 488 (1960) where the United States Supreme Court observed that "Even though the Government's purpose may be legitimate and substantial, that purpose cannot be pursued by means that broadly stifle fundamental personal liberties."…Finally, freedom of speech and freedom of assembly are part of democratic rights of every citizen of the Republic; our legislature must guard these rights jealously as they are part of the foundation upon which the government itself rests...Public Order Act should be promulgated to compliment sections 39 and 40 of the Constitution in context and not to stifle or cripple it."***

6.29. None of the foregoing points were really comprehensively considered or dealt with by the courts in the PIPTD and OKEDARA's cases, before reaching the conclusion that section 24 of the Cybercrimes Act is entirely constitutional. It is for this reason that there are good grounds to believe that there is scope for the Supreme Court to possibly take a different view on the matter and the decision of the lower courts ought to have been different, most especially concerning section 24(1) of the Act.

[25] (2007) 18 NWLR (Pt. 1066) 457 at 498 - 500

6.30. Ultimately, what the decisions in PIPTD and OKEDARA's cases show is that although fundamental rights are regarded as higher rights under Nigerian constitutional law, an Act of the National Assembly may not necessarily be found unconstitutional by the courts in the absence of a very clear and obvious conflict with the provisions of the constitution. In a different sense, perhaps, the decisions also reflect policy decisions on the part of the judiciary to ensure that an area of law, cybercrimes, which in today's world requires strict regulation, as has been done in many other countries, is not left substantially unregulated in Nigeria. However, notwithstanding the nobility behind the enactment of the Cybercrimes Act, it is clear that section 24(1) of the Act portends great danger for every person in Nigeria. This is by reason of the fact that at the time of issuing any communication in exercise of the right to freedom of expression, it is impossible for a person to determine whether or not an offence is being committed under the Cybercrimes Act. Surely, this is the exact scenario that the framers of the constitution sought to legislate against by the inclusion of the express provisions that are sections 36(12) and 39(1) of the constitution.

7.0. Do Things Need to Change?

7.1. In the context of the constitutionally guaranteed right of citizens to freedom of speech under the Nigerian constitution, there is the pressing question of whether the Cybercrimes Act is fit for the purpose pursuant to which it was enacted, particularly in view of the provisions of its section 24(1)? For the reasons aforementioned, it would appear that the answer to this poser is in the negative, which means that it is imperative for deliberate steps to be taken to remedy the situation, particularly against the backdrop of widespread complaints against the deliberate misuse and abuse of the Cybercrimes Act against certain categories of persons in Nigeria.

7.2. In this regard, this is not a matter in which long winding technical recommendations are necessary. The simple recommendation is that section 24(1) be entirely deleted from the Cybercrimes Act, due to its apparent irreconcilability with the provisions of section 36(12) and 39(1) of the constitution. This is because notwithstanding that the courts may hold firm on the view that section 24(1) does not violate the constitution, as long as that

provision remains in the statute books, it is a tool that readily lends itself to abuse and misuse by those in authority against freedom of expression in Nigeria. This is particularly because the Cybercrimes Act contains no safeguards whatsoever to the enforcement of section 24, which carries with it severe criminal sanctions.

7.3. Also, by the opening phrases of section 24(1) and (2) of the Cybercrimes Act the conducts covered by that section are only of a criminal nature where carried out ***"by means of computer systems or network"*** and not any other means. This means that two different people can carry the exact same conduct but where only one of them uses a computer system or network that person alone would be found to have acted criminally. This is certainly an absurdity that ought not to be. There is no logical or legal reason why a singular conduct should be legally dichotomized on the basis of the medium through which the conduct is carried out. What is good for the goose must also be so for the gander.

7.4. Furthermore, in the event that any of the actions now regulated by section 24 of the Cybercrimes Act does escalate from a civil or domestic matter to the realm of criminality, there are sufficient safeguards under the general criminal statutes to cover such a scenario, such that the provisions of section 24 cannot reasonably be justified in a democratic society. It is against the foregoing backdrop that the simple recommendation of deletion as opposed to amendment of section 24(1) of the Cybercrimes Act has is being made here.

8.0. Conclusion

8.1. The binding decisions of the courts the PIPTD and OKEDARA's cases, make it difficult to validly argue that sections 24 and 38 of the Cybercrimes Act are, at present, unconstitutional and void under Nigerian law, at least until a definitive pronouncement is made on the issue by the Supreme Court to the contrary. However, that notwithstanding, it is clear that, at the minimum, those provisions flirt very seductively with violation of constitutionally guaranteed fundamental rights sufficiently enough for this particular debate to continue to rage on.

8.2. Having regard to the fact that cybercrimes are not likely to go away from our soil anytime soon and the Cybercrimes Act is the only legislation of any kind specifically dealing with the subject in Nigeria, the policy decisions of the courts against striking down its provisions and thereby reopen the previously existing lacuna in our criminal laws do have some justification or merit. However, there is no doubt that so soon after its enactment, the Cybercrimes Act is already in desperate need of a significant overhaul to ensure that it achieves the objectives for which it was passed and also does not unwittingly and unconstitutionally place citizens at the unfortunate risk of the luck of a criminal draw.

MOFESOMO TAYO-OYETIBO[26]

[26]Mofesomo Tayo-Oyetibo is the Managing Counsel of the law firm of Twelve Legal and an experienced Commercial Law, Dispute Resolution and Technology, Media and Telecommunications (TMT) lawyer. Email: mofe@twelvelegal.com