*International Journal of Business & Law Research 12(4):32-47, Oct-Dec, 2024*

© SEAHI PUBLICATIONS, 2024 www.seahipublications.org ISSN: 2360-8986

DOI:10.5281/zenodo.13998804

# Corporate Liability for Cybercrimes under Nigerian Law: An Appraisal

**Oyepho, Akeuseph., LL.B. LL.M (RSU), BL (Abuja), Ph.D Research Candidate (RSU), Managing Solicitor, Oyepho, Oyepho & Co. No. 10a Deacon Iheke Street, Mgbuoba, Off NTA Road, Port Harcourt, Rivers State.**
**08035761997, oyepho.akuseph@ust.edu.ng, akeusephoyepho@gmail.com**

**ABSTRACT**
Corporate criminal liability is the legal responsibility of a corporation to criminal action; in Nigeria the focus in determining corporate liability is hinged on the doctrine of *alter ego,* which is the adopted approach to determining actual intention and corporate *mens rea*. Corporate liability for cybercrimes is the legal responsibility of companies for the commission of computer related crimes. This paper examines the corporate liability for cybercrimes under Nigerian Laws. The fundamental objectives of this paper are – to determine corporate liability for cybercrimes under Nigeria laws; to ascertain the normative and institutional framework on corporate liability for cybercrimes in Nigeria; to establish how *actus reus* and *mens rea* as basic ingredients of cybercrimes could be established for the purpose of corporate liability, and to appraise corporate liability for cybercrimes under Nigerian Laws. The doctrinal research methodology is adopted. It is the findings of this paper that the cybercrimes (Prohibition, Prevention Etc) Act 2015, the National Identity Management Act 2007, National Information Technology Development Agency Act 2007, Nigerian Communication Commission Act 2003, Money Laundering (Prevention and Prohibition) Act 2022, Copyrights Act 2022 and Administration of Criminal Justice Act 2015 have provisions related and connected with liability of Corporate bodies for Cybercrimes; it also finds that the doctrines or the principles of *alter ego* and *Superior Respondeat* which emanated from the United Kingdom and the United States of America respectively for the purpose of establishing corporate liability for cybercrimes are entrenched under Nigerian laws; the guilty act and the guilty mind of the directing minds of the corporation, is attributable to that of the corporation, and the corporation as well as the Director, Manager, Secretary and other officers acting in that capacity maybe jointly or severally proceeded against and punished accordingly. It is further discovered that under Nigerian laws, the highest punishment for commission of cybercrime by a corporation or company is winding up of the company and forfeiture of its assets to the Federal Government. It is concluded that Nigeria has enviable laws on corporate liability for cybercrimes. It is recommended that corporate bodies should be made to know their liabilities for cybercrimes. Cross-border corporate cybercrimes pose jurisdictional challenges, accordingly, it is advisable to strengthen international partnership to address cross-border corporate cybercrimes.
**Keywords:** Corporation, Liability, Cybercrimes, Nigerian Laws, Cyberspace, Crimes

## 1.0 INTRODUCTION

In the past, it was unimaginable that a corporation could be held liable; the argument generally advanced was that a corporation as an artificial person, has no physical existence and could therefore not be subjected to the prescribed penalties attached to offences. However, there were also those who felt that a corporation has all the attributes of a natural person and therefore capable of receiving all punishments attached to all offences including physical punishment. In Nigeria, it is clear that corporation though lack the natural attributes of natural persons, can be liable in the same extent as

natural persons.[1] In many ways this recognition had to surmount the difficulty in ascribing a guilty mind to a company without converting it to a natural person.

Corporate criminal liability refers to the legal responsibility of a corporation to criminal action. Corporations are entities that only exist through their employees. In Nigeria, the focus in determining corporate criminal liability is hinged on the doctrine of *alter ego* which is the adopted approach to determining actual intentions and corporate *mens rea.*[2] While the doctrine of *alter ego* is relied upon in United Kingdom and Nigeria, the doctrine of *Respondent Superior* is relied upon in the United States in determining the corporate *mens rea and actus reus.* In *New York Central and Hudson River Railroad and Company v United State*,[3] the US Supreme Court absorbed the difficulty of ascribing human characteristics such as "state of mind" to artificial person and came up with ingenious dependence on the doctrine of *Respondent Superior* to isolate those that represent the company and ascribe their actions to the company itself; this invariably relied on human acts to determine culpability of companies. In the UK, in the case of *Leonard's Carrying Company v Asiatic Petroleum Company Limited*[4] the court set a similar parameter to look beyond the abstract qualities of the company and review the activities of its "directing minds" who are influential enough to be referred to as its '*alter ego'*.[5] The principles of corporate criminal liability was fully established in common law in 1944 in the case of *Director of public prosecution v Kent and Sussex Contractors Limited*,[6] where the court agreed that a 'corporation can only have knowledge and form an intention through its human agents'.[7] The court further stated that 'circumstances may be such that the knowledge and intention of the agent must be imputed to the body corporate'[8] as if the corporation acts itself. In *RVICR Haulage Limited*,[9] another English Court agreed with the position but made an added observation that the company may not be liable for some offences that actually require physical actions such as rape and battery. It is instructive to note that corporate criminal liability started with non-feasance offences.

In Nigeria, in the case of *Orji Uzor Kalu v FRN*,[10] the Court of Appeal made the conclusion when called upon to determine corporate criminal liability by stating that the Appellant, who is the first accused in the case at the Federal High Court is the *alter ego* of the Second Accused, Stok Nigeria Limited and remained its directing mind even while he was the governor of a state. The same position was arrived at by another panel of the Court of Appeal in *Romrig Nigeria Limited v FRN*,[11] where it held that an accused person, a Director of Romrig Nigeria Limited was its *alter ego* and his absence at a key meeting with the prosecutor implies that the company was not part of the agreed outcomes at the plea bargain meeting. Also, in the case of *Abacha v Attorney General of the Federation,*[12] the Supreme Court stated loudly that a accompany can be prosecuted for crime as if it is a natural person.

It is established that in Nigeria, a company can be charged with conspiracy either with other companies or natural persons.[13] In *Federal Republic of Nigeria v Awe Odessa, All States Trust Bank Plc. and Others;*[14] the court convicted all the accused persons, including the company under section 3 of the Money Laundary Decree of 1995 for conspiracy and opening a bank account in All States Trust Bank for Ebenezer Retnan Ventures (one of the corporation accused in the case) without verifying the identity and address of Ebenezer Retnan Ventures. The unverified account was used to launder several sum of money to various banks in the United Kingdom. All States Trust Bank Plc. was convicted and sentenced to a fine of ₦2,000,000.00 (two Million Naira). The court also ordered the company to be wound up and its assets forfeited to the Federal Government of Nigeria. This is a clear instance of

[1] M Suleh-Yusuf, 'Criminal Liability of Corporate Persons in Nigeria' (2017)(3)(4) *International Journal of Law* 32 – 38.
[2] *Ibid.*
[3] (1909)21 UD 481.
[4] (1915) AC 705.
[5] *Ibid.*
[6] (1944) KB 146.
[7] *Ibid.*
[8] *Ibid.*
[9] (1944) KB 551
[10] (2012) SC 215.
[11] (2018)15 NWLR (pt. 1642)284 at 306 paras. A – B; 316 para A).
[12] (2014)18 NWLR (pt. 1438)21.
[13] Suleh-Yusuf (n[1]).
[14] FHC/KD/143/04.

how a company can be charged for conspiring with natural persons to commit an offence under money laundering legislations.

Nigerian Laws such as the Cybercrimes (Prohibition Prevention Etc) Act,[15] National Information Technology Development Agency Act,[16] National Identity Management Commission Act,[17] the Nigeria Copyright Act,[18] Nigerian Communication Commission Act[19] and the Money Laundering Act[20] have provisions on corporate liability for cybercrimes.

Cybercrimes are those crimes that are committed via the use of computers and Information Communication Technologies such as Computer Fraud, Phishing, Cyber Stalking, Identity Theft, Unlawful Access to Computers, Operation of Unregistered Cybercafé, System Interference, Intercepting Electronic Messages, E-mails, Electronic Money Transfers, Cyber Terrorism, Child Pornography, Computer Related Forgery, Willful Misdirection of Electronic Messages, Unlawful Interception of Computer Data, Theft of Electronic Devices, Unauthorized Modification of Computer Systems, Network Data And System Interference, Fraudulent Issuance of Electronic Instructions, Attempt, Conspiracy Aiding and Abating, Breach of Confidentiality, Importation and Fabrication of E-Tools and so on.

The Cyberspace or the Online Space is a place where individuals, corporations, governments and international institutions conduct their civil, political economic, social and cultural activities just as they do offline. Consequently, the Cyberspace or Cyber World hosts both law-abiding Cyber-Citizens or Netizens and recalcitrant Cybercitizens. Those who use the cyberspace to commit crimes are called Cyber criminals. They could be natural or artificial persons. This work will appraise the liability of artificial persons for cybercrimes under Nigerian laws.

## 2.0 Conceptual Framework

This segment will provide definitions and descriptions of terms, concepts and phrases that are relevant or closely connected to the topic of this work. They include Corporate Liability, Corporate Crimes, Cybercrimes, Cyberspace, Corporate Criminality, Information Technology, Computer System and the Internet.

### a) Corporate Liability

The Black's Law Dictionary[21] defines corporate liability as the 'liability incurred by a company as a result of certain acts of its members or officers'. An incorporated company is a legal entity and can be liable for both civil wrongs and criminal offences; however, there are offences such as rape, that a company is incapable of committing even through its controlling minds or officers.

### b) Corporate Crimes

Corporate crimes are crimes committed by corporation representatives acting on its behalf; examples include price-fixing and consumer fraud.[22] Although, a corporation as an entity cannot commit a crime other than through its representatives, it can be named as a criminal defendant.[23] Other names for corporate crimes are corporate offences, organizational crimes, and organizational offences. Corporates crimes or organizational crimes consist of offline and online crimes committed by corporations through its controlling minds, *alter ego* or *Respondent Superior*.

### c) Cybercrimes

Cybercrimes are crimes committed through the use of computers, Computer networks and associated technologies; crimes committed in the cyberspace are called cybercrimes. The Black's law Dictionary defines the term 'Cybercrime' as 'a crime involving the use of computer such as sabotage or stealing of electronically stored data'.[24] It is the use of computer and computer related tools as instruments to

[15] Cybercrimes (Prohibition, Prevention Etc) Act, 2015, ss. 6(4), 21(3), 25(2)(a), (29(1),(2) & (3), 32(12) & (13), 37, 38, 39, & 40.
[16] National Information Technology Development Agency Act 2007, ss. 16 & 17.
[17] National Identity Management Commission Act 2007, s. 28(3), & 29(b).
[18] Nigeria Copyrights Act 2022, ss. 46, 54, 55 & 56.
[19] Nigerian Communication Commission Act 2003, s. 139.
[20] Nigeria Money Laundering Act 2022, ss. 18, 19, & 20.
[21] B A Garner, (ed) *Black's Law Dictionary* (11th Edn New York USA: Thomson Reuters 2019)1098.
[22] *Ibid*, 467.
[23] *Ibid.*
[24] *Ibid*, 446.

further illegal ends, such as committing fraud, trafficking in child pornography, intellectual property theft, stealing identity or violating privacy. It is synonymous with cyber theft which is defined in the Black's Law Dictionary as 'the act of using an online computer service, such as one on the internet to steal someone else's property or interfere with someone else's use and enjoyment of property.[25]

**d) Cyberspace**

It is a fictional space used to describe the phenomenon of electronic signals transmitting through infrastructure of Information and Communication Technologies.[26] It is a worldwide virtual space, different from real space with sub-communities unevenly distributed using a technical environment-first of all, the internet, in which citizens and organizations utilize information and communication technology for their social and commercial interactions. Cyberspace has four components: a physical components (switches, routers, servers, cables, telecommunication towers, computers hardware and so on); a software components (logical networks); information and data components (information and data system collects, stores and relies upon to function) and cyber-human component (human beings and their interactions with hardware, software, data and information)[27]

**e) Corporate Criminality**

The phrase corporate criminality has been defined as the state, quality or condition of a corporation having incurred criminal responsibility.[28] The principle that incorporated body is a legal entity capable of incurring criminal responsibility.[29]

**f) Information Technology**

Information Technology (IT) is the use of computer, storage, networking and other physical devices, infrastructure and processes to create, process, store and exchange all forms of electronic data;[30] the commercial use of IT encompasses both computer technology and communications.[31] The Harvard Business Review coined the term Information Technology to make a distinction between purpose built machines designed to perform a limited scope of functions and general computing machines that could be programmed for various tasks.[32]

**g) Computer System**

The Council of Europe Convention (Budapest Convention) on Cybercrimes 2001, defines the term "computer system" in its Article 1(a) to mean 'any device or group of interconnected or related devices one or more of which pursuant to a program performs automatic processing of data.[33] similarly, the African Union Convention on Cybersecurity and Personal Data Protection 2014, in its Article 1 defines the phrase 'Computer System' to include an electronic, magnetic, optical, electrochemical or other high speed data processing devices of interconnected or related devices performing logical arithmetic or storage functions and include any data storage facility directly related to or operating in conjunction with such devices.[34]

---

[25] *Ibid.*
[26] B A Berkers, 'Human Rights Obligation of the Territorial State in Cyberspace of Areas outside its effective control (2019)(52)(2), Israel Law Review 21.
[27] N Tsagouries, 'The Legal Status of Cyberspace' in Nicholas K Tsagouries and Russal Buchan' (eds) *Research Handbook on International Law and Cyberspace* (Edward Elger 2015)15.
[28] Garner (n[21]), 428.
[29] *Ibid,*
[30] R Castagno and S J Bigelow, 'What is Information Technology: Definition and Example' <https://www.techtarget.com/searchdatercenter/definition/IT> accessed 2nd September, 2024.
[31] *Ibid.*
[32] *Ibid.*
[33] Budapest Convention 2001, art 1(a).
[34] African Union Convention on Cybersecurity and Personal Data Protection 2014, art 1.

**h) Internet**

The Internet is a vast network that connect computers all over the world. Through the internet, people can share information and communicate from anywhere with an internet connection.[35] The internet consists of technologies developed by different individuals and organizations. The internet works through a series of networks that connect devices around the world through telephones. Users are provided access to the internet by service providers.

## 3.0 Legal Framework on Corporate Liability for Cybercrimes in Nigeria

In Nigeria, there are legislations having provisions on Corporate liability for cybercrimes. They include but not limited to – the Cybercrimes (Prohibition, Prevention Etc) Act, 2015, National Information Technology Development Agency Act 2007, National Identity Management Commission Act 2007, Copyright Act 2022, Nigerian Communication Commission Act 2003 and the Money Laundering Act 2022. These legislations having provisions on corporate liability for cybercrimes will be X-rayed below.

**a) Cybercrimes (Prohibition, Prevention Etc) Act 2015**

The Act[36] is the principal law in Nigeria which criminalizes certain misbehaviours in Nigeria's cyberspace; the Act apart from criminalizing conducts by individuals and prescribing punishments for offenders, it also has provisions on corporate liability for cybercrimes.

Section 6 of the Act criminalizes unlawful access to a computer.[37] By Section 6(4), 'Any person or organization who knowingly and intentionally trafficks in any password or similar information through which a computer maybe accessed without lawful authority, if such trafficking effects public, private and or individual interest within or outside the Federation of Nigeria, commits an offence and shall be liable on conviction to a fine of not more than ₦7,000,000 or imprisonment for a term not more than three (3) years or both fine and imprisonment'.[38] From the above provision, an offence is committed by an organization which knowingly and intentionally trafficks in any password or similar information through which a computer is accessed without authority. Any organization that commits the offence of trafficking in password or similar information through which a computer is accessed without authorization, will on conviction be liable to a fine of ₦7,000,000.00.

By section 29(1) 'Any … organization who being a computer based service provider and/or vendor does any act with intent to defraud and by virtue of his position as a service provider, forges, illegally used security codes of the consumer with the intend to gain financial and/or material advantage or with intent to provide less value for money in his or its services to the consumer shall if a corporate organization be guilty of an offence and is liable to a fine of ₦5,000,000.00 and forfeiture of further equivalent of the monetary value of the loss sustained by the consumer.[39] The above offence deals with breach of confidentiality by service providers. Also, Section 29(2)(a) provides that 'where an offence under this Act which has been committed by a body corporate is proved to have been committed on the instigation or with the connivance of, or attributable to any neglect on the part of a director, manager, secretary or other similar officer purporting to act in any such capacity, he as well as the body corporate, where practicable, shall be deemed to be equity of the offence and shall be liable to be proceeded against and punished accordingly?[40] Furthermore, the Act in its Section 29(2)(b) stated that 'where a body corporate is convicted of an offence under this Act, the court may order that the body corporate be there upon and without any further assurances, but for such order, be would up and all its assets and properties forfeited to the Federal Government'[41]

The Act places a duty on all finance institutions in Nigeria to 'verify the identity of its customer carrying out electronic financial transactions by requiring the customer to present documents bearing their names, address and other relevant information before issuance of ATM Cards. Debit Cards and

[35] Britannica, 'Internet Description, History, Uses, and Facts' <https://www.britannic.com> accessed 2nd September, 2024.
[36] Cybercrimes Act (n15).
[37] *Ibid*, s. 6(1).
[38] *Ibid*, s. 6(4).
[39] *Ibid*, s. 29(1).
[40] *Ibid*, s. 29(2)(a).
[41] *Ibid*, s. 29(2)(2).

other related devices'.[42] In Section 37(1)(b), Financial Institutions are enjoined to apply the principle of know your customer in documentation of customers proceeding execution of customers electronic transfer, payment, debit and issuance order.[43] Section 37(2) is the punitive section for any official or organization who fails to obtain proper identity of customers before executing customer electronic instructions in whatever way; it states that any organization that fails in this duty commits an offence and shall be liable on conviction to a fine of ₦5,000,000.00.[44]

Similarly, by Section 37(3), 'Any Financial Institution that makes an authorized debit on a customer's account shall upon written notification by the custom, provide clear legal authorization for such debit to the customer or reverse such debit within 72 hours; any financial institution that fails to reverse such debit within 72 hours, shall be guilty of an offence and liable on conviction to restitution of the debit and fine of ₦5,000,000.00[45]

Still on corporate liability for cybercrimes under the cybercrimes, sections 39 and 40 deal with the duties of service providers to keep all traffic data and subscribers information as may be prescribed by relevant authority responsible for the regulation of communication services in Nigeria for a period of two years;[46] A service provider shall at the request of the relevant authority referred to in subsection (1) of Section 38 or any law enforcement Agency –

a) Preserve, hold or retain any traffic data, subscriber information non-content information, and content data; or
b) Release any information required to keep under subsection (1) of Section 38[47]

Service provider is defined by the Act in its Section 58 to mean 'any public or private entity that provides to users of its services the ability to communicate by means of a computer system, electronic communication devices, mobile network; and any other entity that processes or stores computer data on behalf of such communication service or users of such service.[48] The Act also defines traffic to mean, to sell, transfer, distribute, dispense or otherwise dispose of property or to buy, receive, possess, obtain control of, or use property with the intent to sell, transfer distribute, dispense, or otherwise dispose of such property;[49] and traffic data to mean 'any computer data relating to a communication by means of a computer system or network, generated by a computer system that formed a part in the chain of communication, indicating the communications origin, destination, route, time, date, size, duration, or type of underlying services',[50] by Section 38(3), a law enforcement agency, may, through its authorized officer, request for the release of any information in respect of subsection 2(b) of this section provided to comply.[51] Any data retained, processed or retrieved by the service provider at the request of any law enforcement agency, shall not be utilized except for legitimate purposes provided under this Act, any other legislations regulation or by order of a court of competent jurisdiction.[52]

Where there are reasonable grounds to suspect that the content of any electronic communication is reasonably required for purposes of criminal investigation or proceedings, a judge may on the basis of information on oath.

a) order a service provider, through the application of technical means to intercept, collect, record, permit or assist competent authorities with the collection or recording of content data/or traffic data associated with specified communications transmitted by means of computer system; or traffic data associated with specified communications transmitted by

[42] *Ibid*, s. 37(1)(a).
[43] *Ibid*, s. 37(1)(b).
[44] *Ibid*, s. 37(2).
[45] *Ibid*, s. 37(3).
[46] *Ibid*, s. 38(1)
[47] *Ibid*, s. 38(2)(a) – (b)
[48] *Ibid*, s.58
[49] *Ibid*
[50] *Ibid*
[51] *Ibid*, s. 38(3)
[52] *Ibid*, s. 38(4)

means of computer system; or authorize a law enforcement officer to collect or record such data through application of technical means.[53]

b) authorize a law enforcement officer to collect or record such data through application of technical means.

It is the duty of all service providers in Nigeria to comply with all the provisions of this Act, and disclose information requested by a law enforcement agency or otherwise render assistance however in any inquiry or proceeding under this Act.[54] Also, a service provider shall at the request of a law enforcement Agency in Nigeria or at its own initiative, provide assistance towards: -

a) the identification, apprehension and prosecution of offenders;[55]
b) the identification, tracking and tracing of proceeds of any offence or any property, equipment or device used in the commission of any offence[56] or
c) the freezing, removal, erasure or cancellation of service of the offender which enables the offender to either commit the offence, hide or preserve the proceeds of any offence or any property, equipment or device used in the commission of the offence.[57]

By Section 40(4), 'any service provider who contravenes the provisions of subsections (1) and (2) of this section (as stated above), commits an offence and shall be liable on conviction to a fine of not more than ₦10,000,000.00.[58] In addition to the above prescribed punishment, each director, manager or officer of the service provider shall be liable on conviction to imprisonment for a term of not more than 3 years or a fine of not more than ₦7,000,000.00 or both such fine and imprisonment.[59]

**b) National information Technology Development Act 2007**

The Act[60] mandate is to create a framework for planning, research, development, standardization, application, coordination, monitoring, evaluation and regulation of information technology practices, activities and systems in Nigeria. The Act establishes the National Information Technology Development Fund in its Section 12(1).[61] It shall be paid and credited into the National Information Technology Development Fund:

a) A levy of one percent of the profit before tax of companies and enterprises with an annual turnover of ₦100,000,000.00 and above such paid by the companies shall be tax deductible;
b) Grant-in-and assistance from bilateral and multilateral agencies;
c) All other sums accruing to the fund by way of gifts, endowments, bequest or other voluntary contribution by persons or organization, provided the terms and conditions attached to such gifts, endowments, bequest, or contribution will not jeopardize the function of the agency.
d) Such monies as may be appropriated for the fund by the National Assembly;
e) All other monies or assets that may, from time to time accrue to the fund.[62]

It is the duty of the Federal Inland Revenue Service to collect levy and pay into the fund. The Federal Inland Revenue Service is obligated by the Act that during the process of carrying out its duty of assessing company for either company or income tax or petroleum tax for an accounting period of the company, also assess such company for the levy.[63] The levy of one percent of the profit before tax of companies and enterprises imposed to be paid into the fund shall be due and payable within 60 days after the Federal Inland Revenue Service has served notice of the assessment on a company.[64] Where a levy due is not paid within the time specified, the Federal Inland Revenue Service shall serve on the company, a demand note for the unpaid plus sum which is equal to 2 percent of the levy.[65] It is provided in Section 16(5) of the Act, that:

[53] *Ibid*, s. 39(a) & (b)
[54] *Ibid*, s. 40(1)
[55] *Ibid*, s. 40(2)(a)
[56] *Ibid*, s. 40(2)(b)
[57] *Ibid*, s. 40(2)(c)
[58] *Ibid*, s. 40(3)
[59] *Ibid*, s. 40(4)
[60] National Information Technology Development (n[16])
[61] *Ibid*, s. 12(1)
[62] *Ibid*, s. 12(2)(a) – (e)
[63] *Ibid*, s. 15(2)
[64] *Ibid*, s. 15(3)
[65] *Ibid*, s. 15(4)

Any company, agency or organization that fails within two months after a demand note, to pay the levy or import duty imposed under Section 11 of the Act, commits an offence and is liable on conviction to a fine of not less than ₦1,000,000.00 and the Chief Executive Officer of the Company, Agency or Organization shall be liable to be prosecuted and punished for the offence in like manner as if he had himself committed the offence, unless he proves that the act or omission constituting the offence took place without his knowledge, consent or connivance.[66]

It is instructive to note that the institution of proceedings or imposition of a penalty does not relieve a company or organization from liability to pay the Federal Inland Revenue service such levy or levies that may become due under the Act.[67] Except as otherwise provided under the Act, a corporate body who violates or fails to comply with the provisions stated above, commits an offence. Where a body corporate fails to make payment within two months after a demand note for unpaid levy plus such sum which is equal to 2 percent of this levy has been served on the body corporate, the body corporate commits an offence under this Act.[68]

Section 17(3), provides that: where an offence under this Act is committed by a body corporate or firm …

a) Every Chief Executive Officer of the body corporate or any officer acting in that capacity or on his behalf; and
b) … commits an offence, unless he proves that the act or omission constituting the offence took place without his knowledge, consent or connivance.[69]

By Section 18(1), anybody corporate who commits an offence under this Act (NITDAA) where no specific penalty is provided, is liable on conviction:

a) For a first offence, to a fine of ₦200,000.00 or imprisonment for a term of one year or to both such fine and imprisonment; and
b) For a second and subsequent offence, to a fine of ₦500,000.00 or to imprisonment for a term of 3 years or to both such fine and imprisonment.[70]

It is important to point out here that because the NITDAA 2007, is an act that provides legal framework for the development and regulation of information communication technologies in Nigeria, it is submitted that crimes committed by both natural and artificial persons could be loosely regarded as cybercrimes.

**c) National Identity Management Commission Act 2007**

The Act[71] provides for the establishment of a National Identity database and the National Identity Management Commission charged with the responsibilities for management of the National Database, the registration of individuals and issuance of general multi-purpose identity cards and so on. It has provisions concerning corporate cyber offences or cybercrimes. Though the word, cybercrime or corporate cybercrimes is not mentioned in the Act, Sections 28(1) & (3), and 29(b) create offences which are cyber-oriented. Section 28(1) criminalizes unauthorized access on data or information contained in the database; and where the offence is committed by a body corporate and is proved to have been committed with the connivance of or attributable to any negligent on the part of a director, manager, secretary or other similar officer of the body corporate or any other person purporting to act in any such capacity, such person as well as the body corporate shall be deemed guilty of that offence and shall each be liable on conviction, to imprisonment for ten (10 years and the body corporate to a fine of ₦10,000,000.00.[72]

[66] *Ibid*, s. 16(5)
[67] *Ibid*, s. 16(6)
[68] *Ibid*, s. 17(2)
[69] *Ibid*, s. 17(3)(a) – (b)
[70] *Ibid*, s. 18(1)(a) – (b)
[71] National Identity Management Act (n[17])
[72] *Ibid*, s. 28(3)

Similarly, by Section 29, any person (including artificial person) who carries out or permits the carrying out of any transaction specified in Section 27 (which include: purchase of insurance policies, application for, and issuance of passport; transactions specified under contributory health insurance scheme, transactions with social security implications etc.) without National Identification Number, commits an offence;[73] and shall where the offence is committed by a body corporate, be liable on conviction to a fine of not less than ₦1,000,000.00 and in addition, the Chief Executive or the manager or other similar officer of the body corporate, or any other person purporting to act in any such capacity shall be deemed guilty of the offence and shall be liable on conviction to a fine of ₦1,000,000.00 each.[74] It is pertinent to add that where the offence created by Section 29 of the NIMCA 2007, is committed online by the body corporate, it metamorphoses into a cybercrime punishable under Section 29(b) of the Act as stated above.

**d) Copyright Act 2022**

The Act repeals the Copyright Act, Cap C28 Laws of the Federation of Nigeria, 2024 and enact the Copyright Act 2022 to provide for the regulation, protection and administration of copyright and related matters. The Act in its Sections 44 to 47[75] and 54 to 62[76] create copyright offences and provisions related to online content respectively.

By Section 44, 'Any person who –

(a) makes or causes to be made for sale, hire or for the purposes of trade or business any infringing copy of work in which a copyright subsists;

(b) imports or causes to be imported into Nigeria, other than for private or domestic use, a copy of any work which, if it had been made in Nigeria, would be an infringing copy; or

(c) has in his possession, any plate, master tape, machine, equipment, device or contrivance for the purposes of making nay infringing copy of any such work; commits an offence and is liable on conviction to a fine of at least ₦10,000 for every copy dealt in contravention of this section or imprisonment for a term of at least five years or both.[77] Similarly, any person who – (a) sells, lets for hire or for the purpose of trade or business, exposes or offers for sale any infringing copy of a work; (b) distributes for the purposes of trade or business any infringing copy of a work, (c) has in his possession other than for his private or domestic use, any infringing copy of a work; (d) has in his possession, sells, lets for hire or distributes for the purpose of trade or business or exposes or offers for sale or hire any copy of a work which if it had been made in Nigeria would be an infringing copy, commits an offence and is liable on conviction to a fine of at least ₦10,000 for every copy dealt with in contravention of this Section or imprisonment for a term of at least three years or both.[78] By Section 44(4), any person who, without the consent of owner, distributes to the public for commercial purposes, by way of rental, lease, hire loan or similar arrangement, copies of work in which copyright subsists, commit an offence under the Act and is liable on conviction to a fine of at least ₦1,000 for every copy dealt with or imprisonment for a term of at least three years or both.[79]

A person who without the consent of the owner of a work in which copyright subsists, communicates to the public or makes the work available to the public by wire or wireless means in such a way that members of the public are able to access the work from a place and at a time individually chosen by them for commercial purposes, commits an offence under the Act and is liable on conviction to a fine of at least ₦1,000,000.00 or imprisonment for a term of at least five years or both;[80] also, a person who without the consent of the owner of a copyright does any of the acts listed in Section 13(a) – (e) (concerning the copyright in a broadcast which shall be the exclusive right to do and authorize the doing of any of the following acts – rebroadcasting the broadcast; communication to the public of the broadcast; making the broadcast available to the public by wire or wireless means in such a way that

[73] *Ibid*, s. 29(a)
[74] *Ibid*, s. 29(b)
[75] Copyright Act (n[18]), Ss 44 – 47
[76] *Ibid*, Ss 54 – 62
[77] *Ibid*, s. 44(1)(a) – (c)
[78] *Ibid*, s. 44(2)(a) – (d)
[79] *Ibid*, s. 44(4)
[80] *Ibid*, s. 44(7)

members of the public are able to access the work from a place and a time independently chosen by them; fixation of the broadcast; reproduction of fixation of the broadcast) of the Act, in respect of broadcast, commits an offence under the Act and is liable on conviction to a fine of at least ₦1,000,000.00 or imprisonment for a term of at least five years.[81]

The offences stated above may be committed by natural or artificial persons. They could also be committed offline or online. If any of the offences as contained under Section 44 of the Act is committed online, then, the offence so committed assumes the nature and form of a cybercrime. The offence created under Section 44(7) clearly is a cyber-offence or a cybercrime, however all the other offences created under Section 44 comes within the definition of cybercrimes or cyber-offences if committed in cyberspace or through the use of computer or information community technologies and devices.

Where any of the offences as contained in Section 44 is committed by a body corporate, the body corporation and its principal officers are deemed to have committed the offence and maybe liable to be proceeding against and punished accordingly, provided that nothing contained in this subsection shall render any person liable to any punishment if he proves that the offence was committed without his knowledge or that he exercised all due diligence to prevent the commission of the offence.[82] By Section 46 (2) of the Act, where an offence has been committed by a body corporate and it is proved that the offence was committed with the consent or connivance of any director, manager, secretary or other officer of the body corporate such director, manager, secretary or other officers shall be deemed to have committed that office and shall be proceeded against and punished accordingly.[83]

It is instructive to note that for the purposes of section 46 of the Act, a body corporate includes a firm or association of persons,[84] and 'directors' in relation to a form includes a partner in a firm.[85]

Where a body corporate is convicted of an offence under section 55 of the Act the court may order that the asset and properties be fortified unless the body corporate proves to the satisfaction of the court that such assets were not proceeds of the offence for which the body corporate was convicted.[86]

Notwithstanding, the provisions of any law to the contrary, it is permissible for both criminal and civil actions to be taken simultaneously in respect of the same infringement under the Act.[87]

As expressed above, a part from the offence provided for in section 44 (7) of the Act, which is clearly embedded with elements or characteristic of cybercrime, it is axiomatic that if a body corporate commits any other offence under section 44 of the Act through the instrumentality of a computer, computer related devices or information communication technologies or via cyberspace, that offence or crime is a cybercrime or cyber offence and the body corporate and its principal officers are collectively or individually liable for the commission of the copyright offence in cyberspace or online just as they do offline.

**(e) Nigerian Communication Commission Act 2003.**

The Act did not mention the word 'cybercrimes but it primarily deals with issues related and connected with communication technologies that falls within the ambit of what permeates in cyberspace. Accordingly, the Act could be referred to as a cyber-legislation. Crimes committed in cyberspace are called cybercrimes. The Act made provisions for corporate criminal liability in its section 39.[88]

The section has it that 'if a body corporate commits an offence under this Act or its subsidiary legislation, a person who at the time of the commission of the offence was a director, chief executive, manager, secretary or other similar office of the body corporate or was purporting to act in any such capacity was in any manner or to any extent responsible for the management of any of the affairs of the body corporate or was assisting in such management – (a) maybe charged severally or jointly in

[81] *Ibid*, s. 44(8)
[82] *Ibid*, s. 46(1)
[83] *Ibid*, s. 46(2)
[84] *Ibid*, s. 46(3)(a)
[85] *Ibid*, s. 46(3)(b)
[86] *Ibid*, s. 46(4)
[87] *Ibid*, s. 47
[88] Nigerian Communication Commission Act (n[19])

the some proceedings with the body corporate;[89] and (b) if the body corporate is found guilty of the offence, shall be deemed to be guilty of that of offence unless, having regard to the nature of his functions in that capacity and to all circumstances, he proves:

(i) That the offence was committed without his knowledge, consent or connivance, and
(ii) That he had taken all reasonable cautions and exercised due diligence to prevent the commission of the offence.[90]

It is pertinent to State that most of the offences or crimes created by the Act touches on cyber related misbehaviours and could be loosely called cybercrimes. These crimes or offences may be committed by natural or artificial persons, and maybe proceeded against and punished accordingly.

**(f) Money Laundering (prevention and prohibition) Act, 2022.**

The Money Laundering (prevention and prohibition) Act provides a comprehensive legal framework for preventing and prohibiting money laundering in Nigeria; it establishes the Special Control Unit under the Economic and Financial Crimes Commission. The Act establishment the Special Control Unit Against Money Laundering (the SUML) saddled with the responsibility for effective implementation of the provisions of the Act about designated non-financial business and professions.[91] Sections 18, 19 and 20 carry offences created by the Act. By Section 18 (2) '… a body corporate, in or outside Nigeria, who directly or indirectly – (a) conceals or disguises the origin of, (b) converts or transfers, (c) removes from the jurisdiction, or (d) acquires, uses, retains or takes possession or control of any fund or property, intentionally, knowingly or reasonably ought to have known that such fund or property is, or forms part of the proceeds of unlawful act, comments on offence of money laundering under the Act.[92]

A body corporate who contravenes the provisions of Section 18 (2) as stated above, is liable on conviction to imprisonment for a term of not less than four years but not more than fourteen years or a fine not less than five times the value of the proceeds of the crime or both.[93] By Section 18(5), where the body corporate persists in the commission of the offence for which it was convicted in first instance, the regulators may withdraw or revoke the certificate or license of the body corporate. If a body corporate does the acts designated as offences under section 18 (2) of the Act as stated above, through the instrumentality of a computer or computer related technology or ICTs, such as using internet enabled devices to transfer proceeds of unlawful acts from Nigeria to other countries, knowing same to be proceeds of unlawful acts, with the intention to remove from the jurisdiction in order to conceal the illegal act it could be adjudged to have committed a cybercrime, punishable under the Act.

A combined reading of Sections 18 (2) (b) & (d) of the Act gives credence to this conclusion as the word 'transfer' as used in Section 18 (2) (b) covers transfer of proceeds of unlawful act such as funds or other valuables offline and online. When a corporate body intentionally, knowingly, or reasonably ought to have known that a particular fund or property forms part of the proceeds of an unlawful act and transfer same via the use of computer, computer related devices, powered by the internet or ICT or even acquires, uses, retain, take possession, or take control of the fund or property via the use of computer, computer related devices powered by the internet or ICTs; or conceals, disguises the origin of, converts or removes from the jurisdiction funds or property which forms proceeds of unlawful act via computer, computer related devices powered by the internet or ICTs, commits a Money Laundering that is cybercrime in nature punishable under the Money Laundering Act 2022.

It is pertinent to state that most of the Money Laundering offences are committed through the use of components of cyberspace, that is, via computers, logical networks, computer data and information and so on.

[89] *Ibid*, s. 139
[90] *Ibid*, s. 39 (b)
[91] Money Laundering Act (n[20]), Ss. 1 & 17
[92] *Ibid*, s. 18(2)(a) – (d)
[93] *Ibid*, s. 18(4)

**(g) Administration of Criminal Justice Act 2015.**

The Act provides for the Administration of Criminal Justice System, which promotes management of criminal justice institutions, speedy dispensation of justice, protection of the society from crimes and protections of the rights and interest of the suspect, the defendant and the victim in Nigeria. Sections 477 to 484 have provisions related and connected with the trial of body corporate or corporation in Nigeria. A corporation by Section 477 (1) means anybody corporate, incorporated in Nigeria or elsewhere.[94] A representative for the purposes of part 47 dealing with trial of corporation, means '… a person duly appointed by the corporation to represent it for the purpose of doing any act or thing which representative of the corporation is authorized to do, but a person so appointed shall not, by virtue only of being so appointed, be qualified to act on behalf of the corporation before any court for any other purpose.[95] Regarding the trial of corporation, 'a representative need not be appointed under seal of the corporation, and a statement in writing purporting to be signed by a managing director of a corporation or by any person (by whatever name called) having, or being one of the persons having, the management of affairs of the corporation, to the effect that the person named in the statement has been appointed as the representative of the corporation for the purposes of trial of corporation, is admissible without further proof or *prima facie* evidence that the person has been so appointed.[96]

Where a charge is preferred against a corporation or information framed and filed against a corporation, it may via its representative in writing enter a plea of guilty or not guilty or any plea which may be entered under the Act and it either the corporation does not appear by a representative or though it does so appear fails to enter a plea, it is the duty of the court to enter a plea of not guilty and proceed with the trial as though the corporation had duly entered a plea of not guilty.[97] A corporation may be charged jointly and tried with an individual for any offence.[98]

## 4.0 Determining of *mens rea* and *Actus reus* for corporate criminal liability in Nigeria

In Nigeria, the courts have often made reference to the common law term of *mens rea* and *actus reus* in determining corporate criminal liability. In *Pinnacle Communications Ltd v FRN & Ors*,[99] the question for determination was, whether a corporate body is capable of forming the necessary *mens rea* for consummation of an offence? The court held that '… the argument that, the appellant is a corporate body, and therefore not capable of forming the necessary *mens rea* for consummation of the offence is not supported by law, because natural persons run the appellant as a company, those persons are the *alter ego* of the appellant (the corporate body Pinnacle Communication Ltd), and therefore their state of mind is that of the appellant *ipso facto*.[100]

In *Abeke v State*,[101] it was held that *mens rea* means a guilty mind, is a necessary precondition for attributing criminal acts to either a natural person or a fictional personality. Similarly, in *AG Eastern Region v Amalgamated press of Nigeria Ltd*,[102] the preliminary objection raised by the defendant on the ground that an offence could not be committed by a company in the absence of *mens rea* was overruled by the court, which relied on the attribution principle to determine the liability of the company based on the intents and acts of its officers and directors. However, the court also stated that certain offences cannot be attributed to the company and cited offences of personal violence or with offences for which the only punishment is imprisonment.

Accordingly, the intent or mental state (*mens rea)* and the acts (*actu reus)* of a corporate body for the purposes of criminal liability is established by proving the intent or mental state and acts of its *alter ego* or directing minds or its *respondent superior* and attributing same to the corporate body. The

[94] Administration of Criminal Justice Act 2015, s. 477(1)
[95] *Ibid*, s. 477(2)
[96] *Ibid*, s. 477(3)
[97] *Ibid*, s. 478
[98] *Ibid*, s. 484(2)
[99] (2020) LPELR – 51883 (CA)
[100] *Ibid, Saadu Ayinla alananiu & 2 Ors* CA/IL/C89/2019 (unreported); *Alhaji Mohammed Abacha & Anr V AGF & 4 Ors* (2014) NWLR (pt 1438)31
[101] (2007)3 S.C (pt 11)105
[102] (1961)1 ALL NLR 199

principal officers of the corporate body, that is, the directors, secretary and managers, are the directing minds, *alter ego* and *respondeat superior* of the company or corporation.

## 5.0 Appraisal of Corporate Liability for Cybercrimes under Nigerian Law

The Cybercrimes Act, National Information Development Agency Act, National Identity Management Act, Nigerian Communication Commission Act, Money Laundering Act and Administration of Criminal Justice Act have provisions related and connected with corporate liability for cybercrimes and procedures for the trial of corporate bodies. It is a basic principle of criminal law that a crime (including cybercrime) consists of both a mental and physical element. In *Yelli v State*,[103] on elements of an offence, the Supreme Court held that "it is a fundamental principle of criminal law that a crime consists of both a mental and 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 latin for 'guilty mind', developed in England around 1600, when judges began to hold that an act alone could not create criminal liability unless it is accompanied by a guilty state of mind; the degree of *mens rea* required for particular crime varied then; in order words, *mens rea* is a criminal intention or knowledge that an act is wrong, and today most of the crimes (including cybercrimes) are defined by statutes that generally contains a word or phrase indicating the *mens rea* requirement; thus a typical statute may require that a person act knowingly, purposely or recklessly".[104]

Also, the Supreme Court in an answer to the question 'what are the essential elements of an offence, stated in *Babatola v State*[105] per Chukwudifu Akunne Oputa, of blessed memory, that, '… in common law offences, there are always present two essential elements – (a) a guilty conduct and (b) a mind of fault; it was the great St. Augustine who once remarked that "*ream linguam non facit nisi mens rea",* ... from there the legalists got the now popular latin maxim *actus non facit reum nisi mens sit rea"*;- no man should according to this maxim be convicted of a crime unless his physical conduct (the guilty act) is accompanied with a guilty mental element – a mind at fault, a *mens rea*; the intent and act must both concur to constitute the crime"[106]

Under the cybercrimes (Prohibition, Prevention Etc) Act 2015, particularly Sections 6, 29, 37, 38, 39, and 40 that provide for corporate liability for cybercrimes, the *actus reus and the mens rea* are fundamental ingredients or elements of the various corporate cybercrimes. The act of commission of the offence and the mental state of the offender are necessary ingredients of the offences. Under Section 6(1) & (4), the act that constitutes the offence is unlawful access to a computer. The words "knowingly and intentionally" require that before the offence created under Section 6(4), that is, trafficks in any password or similar information through which a computer may be accessed without authorization …' would be seen to have been committed, the organization or person which traffics in the password or information through which the computer was accessed without authorization must have done that intentionally and knowingly – which denotes the mental element of the offence.

The physical element therefore is the act of trafficking in the password or similar information by the organization (through its *alter ego* or *superior Respondeat)* through which a computer is accessed without authorization. The mental element is the knowledge and the intention by the offender that the password or similar information he traffics maybe used for illegal or unauthorized accessed to a computer. When the two elements of the offence of illegal trafficking in password is established, the person and/or organization would be held to have committed the offence and on conviction be liable to a fine of not more than ₦7,000,000.00 or imprisonment for a term of not more than 3 years or both.[107] In consonance with the above expressions, the Court of Appeal per Misitura Omodere Bolaji-Yusuf in *Onya v State*,[108] stated that 'The presumes that a man intends the natural and probable consequences of his acts and that the test to be applied to the circumstances is the objective test as

[103] (2022) LPELR – 57865 (SC)
[104] *Ibid*, 37 para A – F
[105] (1989) LPELR – 965 (SC)
[106] (1989) LPELR – 965 (SC)
[107] Cybercrimes Act (n…), s. 6(4)
[108] (2019) LPELR – 48500 (CA)

opposed to subjective test of what a reasonable man in the street would contemplate as a probable result of his act.[109]

Also, in *Bolanle Abeke v The State*,[110] the Supreme Court per Tobi JSC (as he then was) held that: 'I entirely agree with the appellant that to convict … the prosecution must prove that the accused had *mens rea* and *actus reus;* put in common simple parlance, *mensrea* means a guilty mind and *actus reus* means a guilty act'[111] In *Njoku & Ors v The State*[112] the Supreme Court per Onoghen JSC held that: 'it is elementary in criminal trial that before an accused person is asked to undergo any sort of sentence, there must be a finding by the trial court on the concurrence of the two main elements of any crime that is the *Actus Reus* and *MENSREA.* ACTUS REUS is taken to be the wrongful deed, that comprises the physical components of a crime and that generally must be coupled with MENS REA. MENS REA is the criminal intent or guilty mind of the accused';[113]

Similarly, under Section 29(1) & (2), for a body corporate to be convicted for breach of confidentiality, the director, manager, secretary or other similar officers of the body corporate or any other officers purporting to act in any such capacity, does so with intent, to defraud, or by his position forges, illegally used security codes of the consumer with intent to gain any financial and material advantage or with intent to provide less value for money of its services to the customer is guilty of an offence and liable to a fine of ₦5,000,000 and for forfeiting of equivalent of the monetary value of loss sustained by the customer;[114] it is explicit from the Section that a guilty act and a guilty mind are elements of the offence. By subsection (2) of Section 29 where the offence committed by the body corporate is committed on the "instigation" or with the "connivance" of or "attributable to any neglect" on the part of a director, manager, secretary … the body corporate as well as the officer(s) shall be taken to be guilty of the offence…'.[115] The words "intent" "connivance", "instigation" and so on as used in the section denote the requirement of a guilty mind as a fundamental ingredient of the offence and the prosecution is duty bound to prove that. Similarly, the doctrine of '*alter ego*' which originated from the United Kingdom and that of '*superior respondeat'* which originated from the United States of America, which doctrines imply that for the purpose of establishing or determining corporate criminal liability, the guilty act and the guilty mind of the principal officers or the directing minds of the body corporate is attributed to the body corporate; simply put, the guilty mind and the guilty act of the director, manager and secretary of the body corporate is taken to be that of the body corporate, for the purposes of holding the body corporate criminally liable, are well enshrined in section 29(2)(a); it is stated in Section 29(2)(b) of the Act, that, 'where a body corporate is convicted for an offence under the Act, the court may order that the body corporate be wound up and all its assets and properties forfeited to the Federal Government.[116]

Under the National Information Technology Development Agency Act 2007, 'Any company or organization that fails within two months after a demand note to pay the levy (created under section 12 of the Act, that is, one percent of the profit before tax of companies … with annual turnover of ₦1,000,000.00 and above) or the import duty imposed under Section 11 of the Act commits an offence and is liable on conviction to a fine of not less than ₦1,000,000.000 and the Chief Executive Officer of the company, shall be liable to be prosecuted and punished for the offence in like manner as if he had himself committed the offence, unless he proves that the act or omission constituting the offence took place without his "knowledge", 'consent' or "connivance".[117] Here again, the use of the words "knowledge", "consent" or "connivance" in the section denotes that for the Chief Executive Officer to bear responsibility of the offence of failure by the company to pay the levy or impart duty imposed under sections 12 and 11, respectively, two months after a demand note issued to it by the Federal Inland Revenue Service as mandated under section 16(1) of the Act, the prosecution must

[109] *Ibid*, 24 – 27 paras C - C
[110] (2007) LPELR – 31 (SC) at 18B – F); *Egwu v State* (2019) LPELR – 48499 (CA), 24 – 28 paras D – A
[111] *Ibid*
[112] LPELR – 20608 (SC) 21 – 22(F – C)
[113] *Ibid*
[114] Cybercrimes Act (n ), s. 29(2)
[115] *Ibid, s. 29(2)(b)*
[116] National Information Development (n[16]), s. 16(5)
[117] National Identity Management (n[17]), s. 28(1) & (3)

establish that the failure to pay the levy or import duty was done with the knowledge, consent or connivance of the Chief Executive Officer. Accordingly, a guilty act (failure to pay levy or import duty) and a guilty (mind knowledge, consent or connivance not to pay the levy or import duty) which are the *actus reus* and the *mens rea* of the offence. The *alter ego* and *superior respondent* doctrines are statutorily transplanted in Section 17(3) of the Act, where the Chief Executive of the body corporate or any officer acting in that capacity or on his behalf bears criminal liability of the body corporate except he proves lack of knowledge, or lack of consent or lack of connivance in the commission of the offence.

Under the National Identity Management Commission Act 2007, particularly in Section 28(1) and (3), a combined reading of the two subsections in relation to corporate criminal liability would have it that, where a body corporate without lawful authorization, accesses data or information contained in the National database and is proved to have been committed with the "connivance of" or "attributable to any neglect" on the part of a director, manager, secretary or other similar officer of the body corporate such officer or person as well as the body corporate shall be deemed guilty of that offence and shall each be liable on conviction to imprisonment for 10 years and the body corporate to a fine of ₦10,000,000.00.[118]

The offence of unauthorized accessed of data or information in the National database of the NIMC by a person or body corporate is clearly a cybercrime, which offence is similar to the offence created in Section 6 of the Cybercrimes (Prohibition, Prevention Etc) Act 2015. In both Acts, a guilty act (unauthorized access to a computer for fraudulent purposes and obtained data) and a guilty mind (knowledge or intention, or connivance of commission of the guilty act) are ingredients of the offence. In the NIMCA, the director, manager, secretary or other similar officers of the body corporate who connived in the commission of the offence of unauthorized access in the National database of NIMC, such person as well as the body corporate shall be deemed guilty of the offence and shall each be liable on conviction for 10 years imprisonment and the body corporate to a fine of ₦10,000,000.00. Of course, the *alter ego* doctrine is incorporated under Sections 28(3) of the NIMCA 2007.[119]

Under the Nigerian Communication Commission Act, 2003, if a body corporate commits an offence under the Act, or its subsidiary legislation, a person who at the time of commission of the offence was a director, chief executive officer, manager, secretary or other similar officers of the body corporate or was purporting to act in any such capacity or in any manner or to any extent responsible for the management of any of the affairs of the body corporate or was assisting in such management – (a) maybe charged severally or jointly in the same proceedings with the body corporate; and if the body corporate is found guilty of the offence, shall be deemed to be guilty of that offence unless he proves that the offence was committed without his "knowledge" "consent" or "connivance";[120] and that he has taken all reasonable precautions and exercised due diligence to prevent the commission of the offence. Again, the physical and the mental elements of a crime that is, the *actus reus* and the mens rea are the basic ingredients to establish corporate criminal liability for cybercrime and the *alter ego* doctrine incorporated in Section 139(a) & (b) of the NCCA 2003.

## 6.0 CONCLUSION

The Cybercrimes (Prohibition, Prevention) Act 2015, in its Sections 6, 29, 37, 38, 39 and 40 contained provisions dealing with corporate liability for cybercrimes, wherein, the *alter ego* and the *superior respondeat* doctrines or principles is incorporated. Offences ranging from unauthorized access to a computer, trafficking in password through which a computer maybe accessed without lawful authorization, breach of confidentiality by service providers, a financial institutions failure to verify the identity of its customers carrying out electronic financial transaction by requiring the customers to present documents bearing their names, addresses and other relevant information before issuance of ATM Cards, Credit Cards, Debit Cards and other related electronic devices; unauthorized debit on a customer's account by a financial institution, failure by a financial institution to keep traffic data and subscriber information for a period of two (2) years and so on, with penalties on conviction

[118] *Ibid*
[119] Nigerian Communication Commission Act (n..), s. 139(a)
[120] *Ibid*, 139(b)

ranging from fines, terms of imprisonment for its principal officers who are found culpable, to winding up and forfeiture of assets and properties of the body corporate. The acts of the *alter ego* of the company or body corporate are deemed to be the acts of the body corporate as well as the director, manager, secretary or other similar officers of the body corporate. A guilty act and a guilty mind is required to be established to sustain a conviction against a body corporate for liability for cybercrimes under the cybercrimes Act 2015.

Also, under the NITDA Act 2007, NIMC Act 2007, Copyright Act 2022 and the NCC Act 2003, particularly in their Sections 16(5), 28(3), … and 139(a) & (b) respectfully, corporate liability for crimes committed by it via its officers is enshrined. In all the Acts aforestated, the criminal acts of its employees are attributed to the body corporate for the purpose of liability. Or the criminal acts of employees of the body corporate are deemed to be committed by the body corporate. In most instances, the body corporate and the officers are jointly or severally liable.

For example, under Section 28(3) of the NIMC Act 2007, where a body corporate without lawful authorization accesses data or information in the Database of National Identity Management Commission established under Section 14 of the Act, and is proved to have been committed with the connivance of a director, manager, secretary or other similar officer of the body corporate, such person as well as the body corporate shall be deemed guilty of that offence and shall be liable on conviction to imprisonment for 10 years and the body corporate to a fine of ₦10,000,000.00. Undoubtly, Section 28(8) of the NIMC Act creates a cybercrime, which is similar to the crime or offence created in Section 6 of the cybercrimes Act dealing with unauthorized access to a computer. The penalties for corporate liability for cyber-offences or cyber related crimes under the NITDA Act 2007, NIMC Act 2007, Copyright Act 2022 and NCC Act 2003 range from payments of fine and terms of imprisonments.

It is instructive to note that the highest punishment for corporate liability for cybercrimes under Nigerian Laws on conviction is wound up of the body corporate; in my humble view, which is equivalent to death penalty handed down for natural person for commission of murder and so on. To this end, Nigerian laws have enviable provisions for corporate liability for cybercrimes.

## 7.0 RECOMMENDATION

This paper recommends as follows:

1) Corporate bodies should be made to know their liability for cybercrimes as many corporate bodies are unaware of their liability for cybercrimes.
2) Law enforcement and judicial officials require training and retraining on cybercrimes, particularly on corporate cybercrimes.
3) Cross-border corporate cybercrimes pose jurisdictional challenges, accordingly, it is advisable to strengthen international partnership to address cross-border corporate cybercrimes.
4) Corporate bodies in Nigeria should adopt and implement robust cybersecurity measures and initiatives.