Nigeria

Cybercrime legislation

Domestic equivalent to the provisions of the Budapest Convention

Table of contents

Version 23.03.2020

[reference to the provisions of the Budapest Convention]

This profile has been prepared by the Cybercrime Programme Office (C-PROC) of the Council of Europe in view of sharing information on cybercrime legislation and assessing the current state of implementation of the Budapest Convention on Cybercrime under national legislation. It does not necessarily reflect official positions of the State covered or of the Council of Europe.

www.coe.int/cybercrime

COUNCIL OF EUROPE

CONSEIL DE L'EUROPE

State:	
Signature of the Budapest Convention:	
Ratification/accession:	

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
Chapter I – Use of terms	
Article 1 – "Computer system", "computer data", "service provider", "traffic data": For the purposes of this Convention: a "computer system" means any device or a group of interconnected or related devices, one or more of which, pursuant to a program, performs automatic processing of data; b "computer data" means any representation of facts, information or concepts in a form suitable for processing in a computer system, including a program suitable to cause a computer system to perform a function; c "service provider" means: i any public or private entity that provides to users of its service the ability to communicate by means of a computer system, and ii any other entity that processes or stores computer data on behalf of such communication service or users of such service; d "traffic data" means any computer data relating to a communication by means of a computer system, generated by a computer system that formed a part in the chain of communication, indicating the communication's origin, destination, route, time, date, size, duration, or type of underlying service	**Cybercrimes Act 2015 Section 58** In this Act – "access" means gaining entry into, instructing or communicating with the logical, arithmetical, or memory function resources of a computer system or network; "Access Device" means and includes: Electronic cards such as: (a) Debit Cards; (b) Credit Cards; (c) Charge cards; (d) Loyalty Cards; (e) Magnetic Stripe based cards; (f) Smart Chip Based cards; (g) EMV Cards; (h) Passwords; (i) Personal identification number (PIN), (i) Electronic plate,

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	(ii) Electronic serial number, (iii) Code number, (iv) Mobile identification number, (v) Any account number or other telecommunications service, equipment, or instrument identifier, or other means of account access including telephones, PDAs, etc., (vi) Automatic Teller Machines, (vii) Point of Sales Terminals, (viii) Other vending machines; "ATM" means Automated Teller Machine. "authorized access" - A person has authorized access to any program or data held in a computer if — (a) the person is entitled to control access to the program or data in question; or (b) the person has consent to access such program or data from a person who is charged with granting such consent; "Authorised Manufacturer" means a financial institution which or any other person who is authorised under any written law to produce a card; "authorized officer or authorized persons" means a member of any law enforcement Agency or a person mandated by it, involved in the prohibition, prevention, elimination or combating of computer crimes and cyber security threats; "Bank Card" means any instrument, token, device, or card whether known as a

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	bank service card, banking card, cheque guarantee card, or debit card or by any other similar name, issued with or without a fee by an issuer for the use of the cardholder in obtaining goods, services, or anything else of value or for the use in automated banking device to obtain money or any of the services offered through the device; "Card" means a bank card, credit card, or payment card; "Cardholder" means the person named on the face of a bank card, credit card or payment card to whom or for whose benefit such a card is issued by an issuer; "Card-Making Equipment" means any equipment, machine, plate, mechanism, impression, or any other device designed, used, or capable of being used to produce a card, a counterfeit card, or any aspect or component of a card; "Computer" means an electronic, magnetic, optical, electrochemical or other high speed data processing device performing logical, arithmetic, or storage functions and includes any data storage facility. All communication devices that can directly interface with a computer through communication protocols shall form part of this definition. This definition excludes the following; portable hand-held calculator typewriters and typesetters or other similar devices; "computer data" include every information including information required by the computer to be able to operate, run programs, store programs and store information that the computer user needs such as text files or other files that are associated with the program the computer user is running. "computer program" or "program" means a set of instructions written to perform or execute a specified task with a computer; "computer system" refers to any device or group of interconnected or related devices, one or more of which, pursuant to a program, performs automated or interactive processing of data. It covers any type of device with data processing capabilities including, but not limited to, computers and mobile phones. The device consisting of hardware and software may include input, output and storage components which may stand alone or be connected in a network or other similar devices. It also includes computer data storage devices or media;

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	"Consumer" means every person or organization who enters into computer based purchase, lease transfer, maintenance and consultancy service agreements with a computer service provider and the customer and agent of the consumer. Consumers will also include bank account holders who carry financial cards; "content data" means the actual information or message sent across during a communication session "Counterfeit Card" means a bank card, credit card or a payment card which is fictitious, altered, or forged and includes any facsimile or false representation, deception, or component of such a card, or any such card which is stolen, obtained as part of a scheme to defraud, or otherwise unlawfully obtained, and which may or may not be embossed with account information or an issuer's information; ''Countering Violent Extremism (CVE) Program" includes any intervention designed to counter the persistence of violent radicalization to reduce the incidence of violent activities, change the behaviour of violent extremists, and counter the negative extreme groups while promoting core national values; also any program that seeks to identify the underlying causes of radicalization (social, cultural, religious and economic) and develop strategies that provide solutions and also introduce measures to change the attitudes and perceptions of potential recruits, including providing vocational training of prisoners and means of sustainable livelihood and reintegration of reformed extremists to their families and communities''; "Credit" includes a cash loan, or any other financial information; "Credit Card" means any instrument, token, device, or card, whether known as a charge card or by any other similar name, issued with or without a fee by an issuer for the use of the cardholder in obtaining goods, services, or anything else of value on credit from a creditor or for use in an automated banking device to obtain money or any of the services offered through the device; "Creditor" means a person or company that agrees or is authorised by an issuer

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	to supply goods, services, or anything else of value and to accept payment by use of a bank card, credit card, payment card for the supply of such goods, services or anything else of value to the cardholder; "Critical infrastructure" means, 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; "Counterfeit access device" means counterfeit, fictitious, altered, or forged, or an identifiable component of an access device or a counterfeit access device; "cyberstalking" a course of conduct directed at a specific person that would cause a reasonable person to feel fear; "cybersquatting" The acquisition of a domain name over the internet in bad faith to profit, mislead, destroy reputation, and deprive others from registering the same, if such a domain name is: (i) Similar, identical, or confusingly similar to an existing trademark registered with the appropriate government agency at the time of the domain name registration: (ii) Identical or in any way similar with the name of a person other than the registrant, in case of a personal name; and (iii) Acquired without right or with intellectual property interests in it. "damage" means any impairment to a computer or the integrity or availability of data, program, system or information that — (i) causes financial loss; or (ii) modifies or impairs or potentially modifies or impairs the medical examination, diagnosis, treatment or care of one or more persons; or (iii) causes or threatens physical injury or death to any person; or

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	(iv) threatens public health or public safety; "data" means representations of information or of concepts that are being prepared or have been prepared in a form suitable for use in a computer; "database" means digitally organized collection of data for one or more purposes which allows easy access, management and update of data; "device" means any object or equipment that has been designed to do a particular job or whose mechanical or electrical workings are controlled or monitored by a microprocessor ; "electronic communication" includes communications in electronic format, instant messages, short message service (SMS), e-mail, video, voice mails, multimedia message service (MMS), Fax, and pager; "electronic device" means a device which accomplishes its purpose electronically. This includes ,computer systems, telecommunication devices, smart phones, access cards, credit cards, debit cards, loyalty cards etc; "electronic record" means a record generated, communicated, received or stored by electronic, magnetic, optical or other means in an information system or for transmission from one information system to another; "Electronic transfer of fund" means any transfer of funds which is initiated by a person by way of instruction, authorisation or order to a bank to debit or credit an account maintained with that bank through electronic means and includes point of sales transfers, automated teller machine transactions, direct deposits or withdrawal of funds, transfer initiated by telephone, internet and card payment; "Expired Card" means a card which is no longer valid because the term shown of it has expired; "Financial Institution" includes any individual, body, association or group of persons, whether corporate or unincorporated which carries on the business of

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	investment and securities, a discount house, finance company and money brokerage whose principal object includes factoring project financing equipment leasing, debt administration, fund management, private ledger services, investment management, local purchase order financing, export finance, project consultancy, financial consultancy, pension fund management, insurance institutions, debt factorization and conversion firms, dealer, clearing and settlement companies, legal practitioners, hotels, casinos, bureau de change, supermarkets and such other businesses as the Central Bank or appropriate regulatory authorities may, from time to time, designate"; "Financial Transaction" means, (a) a transaction which in any way involves movement of funds by wire or other electronic means; (b) involves one or more monetary instruments; (c) involves the transfer of title to any real or personal property; "function" includes logic, control, arithmetic, deletion, storage, retrieval and communication or telecommunication to, from or within a computer; "Identity Theft" means, the stealing of somebody else personal information to obtain goods and services through electronic based transactions; "Infrastructure Terminal" includes terminals shall include GSM Phones that can be used to access bank or any other sensitive information, Point of sales terminals (POS) and all other Card Acceptor Devices that are in use now or may be introduced in the future; "Interception" in relation to a function of a computer system or communications network, includes listening to or recording of communication data of a computer or acquiring the substance, meaning or purport of such and any acts capable of blocking or preventing any of these functions; "Issuer" includes a financial institution which or any other entity who is authorised by the Central Bank to issue a payment card; "law enforcement agencies" includes any agency for the time being responsible for implementation and enforcement of the provisions of this Act;

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	"Minister" means the Attorney-General of the Federation; "Modification" means deletion, deterioration, alteration, restriction or suppression of data within computer systems or networks, including data transfer from a computer system by any means. "network" means a collection of hardware components and computers interconnected by communications channels that allow sharing of resources and information; "payment Card" means any instrument, token, device, or card, or known by any other similar name, and encoded with a stated money value and issued with or without a fee by an issuer for use of the cardholder in obtaining goods, services, or anything else of value, except money; "person" includes an individual, body corporate, organisation or group of persons; "President" means the President, Commander-in-Chief of the Armed Forces of the Federal Republic of Nigeria; "Phishing" means the criminal and fraudulent process of attempting to acquire sensitive information such as usernames, passwords and credit card details, by masquerading as a trustworthy entity in an electronic communication through e-mails or instant messaging either in form of an email from what appears from your bank asking a user to change his or her password or reveal his or her identity so that such information can later be used to defraud the user; "Purchasing Forged Electronic" Means of Credit/Debit Transfer Instruments Such as Credit Card, Debit Card, Smart Card, ATM or Other Related Electronic Payment System Devices; "Receives" or "Receiving" means acquiring possession, title or control or accepting a card as security for credit; "Revoked Card" means a card which is no longer valid because permission to use it has been suspended or terminated by the issuer, whether on its own or on

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	the request of the cardholder; "Service provider" means - (i) 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 networks; and (ii) any other entity that processes or stores computer data on behalf of such communication service or users of such service; "Sexually explicit conduct" includes at least the following real or simulated acts - (a) sexual intercourse, including genital-genital, oral-genital, anal-genital or oral-anal, between children, or between an adult and a child, of the same or opposite sex; (b) bestiality; (c) masturbation; (d) sadistic or masochistic abuse in a sexual context; or (e) lascivious exhibition of the genitals or the pubic area of a child. It is not relevant whether the conduct depicted is real or simulated; "Spamming" is an abuse of electronic messaging systems to indiscriminately send unsolicited bulk messages to individuals and corporate organizations; "Traffic" means 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; and "traffic data" - means 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 communication's origin,

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	destination, route, time, date, size, duration, or type of underlying service.
Chapter II – Measures to be taken at the national level	
Section 1 – Substantive criminal law	
Title 1 – Offences against the confidentiality, integrity and availability of computer data and systems	
Article 2 – Illegal access Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, the access to the whole or any part of a computer system without right. A Party may require that the offence be committed by infringing security measures, with the intent of obtaining computer data or other dishonest intent, or in relation to a computer system that is connected to another computer system.	**Cybercrimes Act 2015 Section 6** **Unlawful access to a computer** (1) Any person, who without authorization, intentionally accesses in whole or in part, a computer system or network for fraudulent purposes and obtain data that are vital to national security, commits an offence and shall be liable on conviction to imprisonment for a term of not more than 5 years or to a fine of not more than ₦5,000,000.00 or to both fine and imprisonment. (2) Where the offence provided in subsection (1) of this section is committed with the intent of obtaining computer data, securing access to any program, commercial or industrial secrets or classified information, the punishment shall be imprisonment for a term of not more than 7 years or a fine of not more than ₦7,000,000.00 or to both such fine and imprisonment. (3) Any person who, with the intent to commit an offence under this section, uses any device to avoid detection or otherwise prevent identification or attribution with the act or omission, commits an offence and shall be liable on conviction to imprisonment for a term of not more than 7 years or to a fine of not more than ₦7,000,000.00 or to both such fine and imprisonment. (4) Any person or organisation who knowingly and intentionally trafficks in any password or similar information through which a computer may be accessed without lawful authority, if such trafficking affects 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 ₦7,000,000.00 or imprisonment for a term of not more than 3 years or both such fine and imprisonment.

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	Cybercrimes Act 2015 Section 18 **Cyber terrorism** (1) Any person that accesses or causes to be accessed any computer or computer system or network for purposes of terrorism, commits an offence and is liable on conviction to life imprisonment. (2) For the purpose of this section, "terrorism" shall have the same meaning under the Terrorism (Prevention) Act, 2011, as amended.
Article 3 – Illegal interception Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, the interception without right, made by technical means, of non-public transmissions of computer data to, from or within a computer system, including electromagnetic emissions from a computer system carrying such computer data. A Party may require that the offence be committed with dishonest intent, or in relation to a computer system that is connected to another computer system.	**Cybercrimes Act 2015 Section 9** **Intercepting Electronic Messages, Emails Electronic Money Transfer** Any person who unlawfully destroys or aborts any electronic mails or processes through which money and or valuable information is being conveyed is guilty of an offence and is liable to imprisonment for 7 years in the first instance and upon second conviction shall be liable to 14 years imprisonment. **Cybercrimes Act 2015 Section 11** **Wilful misdirection of Electronic Messages** Any person who misdirects electronic messages with either the intention to fraudulently obtain financial gain as a result of such act or with the intention of obstructing the process in order to cause delay or speeding the messages with a view to cause an omission or commission that may defeat the essence of such messages is guilty of an offence and is liable to imprisonment for Three Years or a fine of ₦1,000,000.00 or both. **Cybercrimes Act 2015 Section 12** **Unlawful interceptions** (1) Any person, who intentionally and without authorization, intercepts by technical means, non-public transmissions of computer data, content, or traffic data, including electromagnetic emissions or signals from a computer, computer system or network carrying or emitting signals, to or from a computer, computer system or connected system or network; commits an offence and

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	shall be liable on conviction to imprisonment for a term of not more than 2 years or to a fine of not more than N5,000,000.00 or to both such fine and imprisonment.
Article 4 – Data interference 1 Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, the damaging, deletion, deterioration, alteration or suppression of computer data without right. 2 A Party may reserve the right to require that the conduct described in paragraph 1 result in serious harm.	**Cybercrimes Act 2015 Section 16** **Unauthorized modification of computer systems, network data and System interference** (1) Any person who with intent and without lawful authority directly or indirectly modifies or causes modification of any data held in any computer system or network, commits an offence and shall be liable on conviction to imprisonment for a term of not more than 3 years or to a fine of not more than ₦7,000,000.00 or to both such fine and imprisonment. (2) For the purpose of this section, a modification of any data held in any computer system or network includes modifications that take place whereby the operation of any function of the computer system or network concerned, or any - (a) program or data held in it is altered or erased; (b) program or data is added to or removed from any program or data held in it; (c) program or data is suppressed to prevent or terminate the availability of the data or function to its authorized users; or (d) act occurs which impairs the normal operation of any computer, computer system or network concerned. (3) Any person who without lawful authority, intentionally does an act which causes directly or indirectly the serious hindering of the functioning of a computer system by inputting, transmitting, damaging, deleting, deteriorating, altering or suppressing computer data or any other form of interference with the computer system, which prevents the computer system or any part thereof, from functioning in accordance with its intended purpose, commits an offence and shall be liable on conviction to imprisonment for a term of not more than 2

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	years or to a fine of not more than N5,000,000.00 or to both such fine and imprisonment.
Article 5 – System interference Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, the serious hindering without right of the functioning of a computer system by inputting, transmitting, damaging, deleting, deteriorating, altering or suppressing computer data	**Cybercrimes Act 2015 Section 8** **System Interference** Any person who without lawful authority, intentionally or for fraudulent purposes does an act which causes directly or indirectly the serious hindering of the functioning of a computer system by inputting, transmitting, damaging, deleting, deteriorating, altering or suppressing computer data or any other form of interference with the computer system, which prevents the computer system or any part thereof, from functioning in accordance with its intended purpose, commits an offence and shall be liable on conviction to imprisonment for a term of not more than 2 years or to a fine of not more than N5,000,000.00 or to both fine and imprisonment. **Cybercrimes Act 2015 Section 10** **Tampering with Critical Infrastructure** From the commencement of this Act, any person being employed by or under a Local Government of Nigeria, private organization or financial institution with respect to working with any critical infrastructure, electronic mails commits any act which he is not authorized to do by virtue of his contract of service or intentionally permits, tampering with such computer, is guilty of an offence and is liable to a fine of N2,000,000.00 or imprisonment for 3 years. **Cybercrimes Act 2015 Section 16** **Unauthorized modification of computer systems, network data and System interference**

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	(1) Any person who with intent and without lawful authority directly or indirectly modifies or causes modification of any data held in any computer system or network, commits an offence and shall be liable on conviction to imprisonment for a term of not more than 3 years or to a fine of not more than N7,000,000.00 or to both such fine and imprisonment. (2) For the purpose of this section, a modification of any data held in any computer system or network includes modifications that take place whereby the operation of any function of the computer system or network concerned, or any - (a) program or data held in it is altered or erased; (b) program or data is added to or removed from any program or data held in it; (c) program or data is suppressed to prevent or terminate the availability of the data or function to its authorized users; or (d) act occurs which impairs the normal operation of any computer, computer system or network concerned. (3) Any person who without lawful authority, intentionally does an act which causes directly or indirectly the serious hindering of the functioning of a computer system by inputting, transmitting, damaging, deleting, deteriorating, altering or suppressing computer data or any other form of interference with the computer system, which prevents the computer system or any part thereof, from functioning in accordance with its intended purpose, commits an offence and shall be liable on conviction to imprisonment for a term of not more than 2 years or to a fine of not more than N5,000,000.00 or to both such fine and imprisonment. **Cybercrimes Act 2015 Section 32** **Phishing, Spamming, Spreading of Computer Virus**

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	(1) Any person who knowingly or intentionally engages in computer phishing shall be liable upon conviction to 3 years imprisonment or a fine of N1, 000,000.00 or both. (2) Any person who engages in spamming with intent to disrupt the operations of a computer be it public or private or financial institutions shall be guilty of an offence and liable upon conviction to 3 years imprisonment or a fine of N1, 000,000.00 or both. (3) Any person who engages in malicious or deliberate spread of viruses or any malware thereby causing damage to critical information in public, private or financial institution's computers shall be guilty of an offence is liable upon conviction to 3 years imprisonment or a fine of ₦1,000,000.00 or both.
Article 6 – Misuse of devices 1 Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally and without right: a the production, sale, procurement for use, import, distribution or otherwise making available of: i a device, including a computer program, designed or adapted primarily for the purpose of committing any of the offences established in accordance with the above Articles 2 through 5; ii a computer password, access code, or similar data by which the whole or any part of a computer system is capable of being accessed, with intent that it be used for the purpose of committing any of the offences established in Articles 2 through 5; and b the possession of an item referred to in paragraphs a.i or ii above, with intent that it be used for the purpose of committing any of the offences established in Articles 2 through 5. A Party may require by law that a number of such items be possessed before criminal liability attaches. 2 This article shall not be interpreted as imposing criminal liability where the production, sale, procurement for use, import, distribution or otherwise making available or possession referred to in paragraph 1 of this article is not for the purpose of committing an offence established in accordance with	**Cybercrimes Act 2015 Section 28** **Importation and fabrication of E-Tools** (1) Any person who unlawfully produces, supplies, adapts, manipulates or procures for use, imports, exports, distributes, offers for sale or otherwise makes available - (a) any device, including a computer program or a component designed or adapted for the purpose of committing an offence under this Act; (b) a computer password, access code or similar data by which the whole or any part of a computer system or network is capable of being accessed for the purpose of committing an offence under this Act; or (c) any device, including a computer program designed to overcome security measures in any computer system or network with the intent that the devices be utilized for the purpose of violating any provision of this Act: commits an offence and 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 to both. (2) Any person who with intent to commit an offence under this Act, has in his

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
Articles 2 through 5 of this Convention, such as for the authorised testing or protection of a computer system. 3 Each Party may reserve the right not to apply paragraph 1 of this article, provided that the reservation does not concern the sale, distribution or otherwise making available of the items referred to in paragraph 1 a.ii of this article.	possession any device or program referred to in subsection (1) of this section, commits an offence and shall be liable on conviction to imprisonment for a term of not more than 2 years or to a fine of not more than ₦5,000,000.00 or to both such fine and imprisonment. (3) Any person who, knowingly and without authority, discloses any password, access code or any other means of gaining access to any program or data held in any computer or network for any unlawful purpose or gain, commits an offence and shall be liable on conviction to imprisonment for a term of not more than 2 years or to a fine of not more than ₦5,000,000.00 or to both fine and imprisonment. (4) Where the offence under subsection (1) of this section results in loss or damage, the offender shall be liable to imprisonment for a term of not more than 5 years or to a fine of not more than ₦10,000,000.00 or to both such fine and imprisonment. (5) Any person who with intent to commit any offence under this Act uses any automated means or device or any computer program or software to retrieve, collect and store password, access code or any means of gaining access to any program, data or database held in any computer, commits an offence and shall be liable on conviction to imprisonment for a term of not more than 5 years or to a fine of not more than ₦10,000,000.00 or to both such fine and imprisonment. (6) Any persons who without lawful authority and or appropriate license where required, with fraudulent intent, imports, transports or installs within the Federation of Nigeria any tool, implement, item used or designed to be used in making, forging, altering, or counterfeiting any electronic device, commits an offence and shall be liable on conviction to imprisonment for a term of not more than 7 Years or a fine of not more than ₦5,000,000.00 or to both such fine and imprisonment.
Title 2 – Computer-related offences	
Article 7 – Computer-related forgery	***Cybercrimes Act 2015 Section 13***

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally and without right, the input, alteration, deletion, or suppression of computer data, resulting in inauthentic data with the intent that it be considered or acted upon for legal purposes as if it were authentic, regardless whether or not the data is directly readable and intelligible. A Party may require an intent to defraud, or similar dishonest intent, before criminal liability attaches.	**Computer Related Forgery** A person who knowingly accesses any computer or network and inputs, alters, deletes or suppresses any data resulting in inauthentic data with the intention that such inauthentic data will be considered or acted upon as if it were authentic or genuine, regardless of whether or not such data is directly readable or intelligible, commits an offence and is liable on conviction to imprisonment for a term of not less than 3 years or to a fine of not less than ₦7,000,000.00 or both.
Article 8 – Computer-related fraud Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally and without right, the causing of a loss of property to another person by: a any input, alteration, deletion or suppression of computer data; b any interference with the functioning of a computer system, with fraudulent or dishonest intent of procuring, without right, an economic benefit for oneself or for another person.	**Cybercrimes Act 2015 Section 11** **Wilful misdirection of Electronic Messages** Any person who misdirects electronic messages with either the intention to fraudulently obtain financial gain as a result of such act or with the intention of obstructing the process in order to cause delay or speeding the messages with a view to cause an omission or commission that may defeat the essence of such messages is guilty of an offence and is liable to imprisonment for Three Years or a fine of ₦1,000,000.00 or both. **Cybercrimes Act 2015 Section 14** **Computer related fraud** (1) Any person who knowingly and without authority or in excess of authority causes any loss of property to another by altering, erasing, inputting or suppressing any data held in any computer, whether or not for the purpose of conferring any economic benefits on himself or another person, commits an offence and is liable on conviction to imprisonment for a term of not less than 3 years or to a fine of not less than ₦7,000,000.00 or both fine and imprisonment. (2) Any person who with intent to defraud sends electronic message materially misrepresents any fact or set of facts upon which reliance the recipient or another person is caused to suffer any damage or loss, commits an offence and shall be liable on conviction to imprisonment for a term of not less than 5 years and to a fine of not less than ₦10,000,000.00 or to both fine and imprisonment.

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	(3) Any person who with intent to defraud, franks electronic messages, instructions, super scribes any electronic message and or instruction, commits an offence and shall be liable on conviction to imprisonment for a term of not more than 3 years or to a fine of not more than N5,000,000.00 or to both such fine and imprisonment (4) Any person employed in the public or private sector, who with intent to defraud, manipulates a computer or other electronic payment devices with the intent to short pay or overpay or actually short pays or overpays any employee of the public or private sector, commits an offence and shall be liable on conviction to imprisonment for a term of not more than 7 Years and shall forfeit the proprietary interest in the stolen money or property to the bank, financial institution or the customer. (a) Any person employed by or under the authority of any bank or other financial institutions who with intent to defraud, directly or indirectly, diverts electronic mails, commits an offence and shall be liable on conviction to imprisonment for a term of not more than 5 Years or a fine of not more than ₦7,000,000.00 or to both fine and imprisonment. (b) Any person who commits an offence under subsection (4) above, which results in material and/or financial loss to the bank, financial institution and/or customers shall in addition to 7 years imprisonment be liable to refund the stolen money or forfeit any property to which it has been converted to the bank, financial institution or the customer. (5) Any employee of a financial institution found to have connived with another person or group of persons to perpetrate fraud using computer system(s) or network, commits an offence and shall be liable on conviction to imprisonment for a term of not more than 7 years and shall in addition, refund the stolen money or forfeit any property to which it has been converted to the bank, financial institution or the customer. (a) Any person who steals a financial institutions or Public Infrastructure Terminal commits an offence and shall be liable on conviction to imprisonment

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	for a term of 3 years or a fine of ₦1,000,000.00 or to both fine and imprisonment. (b) Any person who steals an Automated Teller Machine (ATM) commits an offence and shall be liable on conviction to imprisonment for a term of not more than 7 years or a fine of not more than ₦10,000,000.00 or to both fine and imprisonment. All proceeds of such theft shall be forfeited to the lawful owners of the ATM. (c) Any person who attempts to steal an ATM, commits an offence and shall be liable on conviction to imprisonment for a term of not more than 1 year or a fine of not more than ₦1,000,000.00 or both fine and imprisonment. **Additional fraud provisions** **Cybercrimes Act 2015 Section 7.2** **Registration of Cybercafé** (2) Any person, who perpetrates electronic fraud or online fraud using a cybercafé, shall be guilty of an offence and shall be sentenced to Three Years imprisonment or a fine of One Million Naira or both. **Cybercrimes Act 2015 Section 9** **Intercepting Electronic Messages, Emails Electronic Money Transfers** Any person who unlawfully destroys or aborts any electronic mails or processes through which money and or valuable information is being conveyed is guilty of an offence and is liable to imprisonment for 7 years in the first instance and upon second conviction shall be liable to 14 years imprisonment. **Cybercrimes Act 2015 Section 20** **Fraudulent issuance of E-Instructions** **Cybercrimes Act 2015 Section 22**

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	Any person being authorized by any financial institution and charged with the responsibility of using computer or other electronic devices for financial transactions such as posting of debit and credit, issuance of electronic instructions as they relate to sending of electronic debit and credit messages or charged with the duty of confirmation of electronic fund transfer, unlawfully with the intent to defraud issues false electronic or verbal messages is guilty of an offence and is liable to imprisonment for 7 years. **Cybercrimes Act 2015 Section 33** **Electronic cards related fraud** (1) Any person who with intent to defraud, uses any access device including credit, debit, charge, loyalty and other types of financial cards, to obtain cash, credit, goods or service commits an offence and shall be liable on conviction to imprisonment for a term of not more than 7 Years or a fine of not more than ₦5,000,000.00 or to both such fine and imprisonment and shall further be liable to payment in monetary terms the value of loss sustained by the owner of the credit card. (2) Any person who uses: (a) a counterfeit access device; (b) an unauthorized access device; (c) an access device issued to another person; resulting in a loss or gain commits an offence and shall be liable on conviction to imprisonment for a term of not more than 7 years or a fine of not more than ₦5,000,000.00 and forfeiture of the advantage or value derived from his act. (3) Any person who steals an electronic card commits an offence and shall be liable on conviction to imprisonment for a term of not more than 3 years or to a fine of not more than ₦1,000,000.00. He shall further be liable to repayment in monetary terms the value of loss sustained by the cardholder or forfeiture of the

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	assets or goods acquired with the funds from the account of the cardholder. (4) Any person who receives a card that he knows or ought to know to have been lost, mislaid, or delivered under a mistake as to the identity or address of the cardholder and who retains possession with the intent to use, sell, or to traffic it to a person other than the issuer or the cardholder commits an offence and shall be liable on conviction to not more than 3 years imprisonment or to a fine of not more than ₦1,000,000.00 and shall further be liable to payment in monetary terms the value of loss sustained by the cardholder. (5) Any person who, with intent to defraud the issuer, a creditor, or any other person, obtains control over a card as security for a debt commits an offence and shall be liable on conviction to imprisonment for a term of not more than 3 years or to a fine of not more than N3,000,000.00 or to such both fine and imprisonment and shall further be liable to payment in monetary terms the value of loss sustained by the card holder or forfeiture of the assets or goods acquired with the funds from the account of the cardholder. (6) Any person, other than the cardholder or a person authorized by him, who, with the intend to defraud the issuer or a creditor, signs a card commits an offence and shall be liable on conviction to imprisonment for a term of not more than 3 years or a fine of not more than ₦1,000,000.00. (7) Any person who, with intent to defraud an issuer or a creditor, uses, for the purpose of obtaining money, goods, services, or anything else of value, a card obtained or retained fraudulently or a card which he knows is forged or expired, or who obtains money, goods, services, or anything else of value by representing, without the consent or authorization of the cardholder, that he is the holder of a specified card, or by representing that he is the holder of a card and such card has been validly issued, commits an offence and shall be liable on conviction to imprisonment for a term of not more than 3 years and a fine of not more than ₦1,000,000.00. (8)

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	(a) Any creditor who, with intent to defraud the issuer or the cardholder, furnishes goods, services, or anything else of value upon presentation of a card which he knows is obtained or retained fraudulently or illegally or a card which he knows is forged, expired, or revoked commits an offence and shall be liable on conviction to imprisonment for a term of not more than 3 years or a fine of not more than ₦1,000,000.00 or to both such fine and imprisonment. (b) Any Creditor who, with intent to defraud the issuer, or the cardholder, fails to furnish goods, services, or anything of value which he represents in writing to the issuer or the cardholder that he has furnished commits an offence and shall be liable on conviction to imprisonment for a term of not more than 3 years or a fine of not more than ₦1,000,000.00 or to both such fine and imprisonment. (c) Any person who is authorized by a creditor to furnish goods, services, or anything else of value upon presentation of a card or a card account number by a cardholder, or any agent or employee of such person, who, with intent to defraud the issuer, or the cardholder, presents to the issuer or the cardholder, for payment, a card transaction record of sale, which sale was not made by such person or his agent or employee, commits an offence and shall be liable on summary conviction to a fine of not more than ₦500,000 and to imprisonment for 3 years. (d) Any person who, without the creditor's authorization, employs, solicits or otherwise causes a person who is authorized by the creditor to furnish goods, services or anything else of value upon presentation of a card account number by the cardholder, or employs, solicits or otherwise causes an agent or employee of such authorized person, to remit to the creditor a card transaction record of a sale that was not made by such authorized person or his agent or employee commits an offence and shall be liable on conviction to imprisonment for a term of not more than 3 years or to a fine of not more than ₦1,000,000.00 or to both such fine and imprisonment. (9) Any person who with intent to defraud, possesses counterfeit cards, invoices, vouchers, sales drafts, or other representations or manifestations of counterfeit cards, or card account numbers of another person, commits an

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	offence and shall be liable on conviction to imprisonment for a term of not more than 5 years or to a fine of not more than ₦3,000,000.00 or to both such fine and imprisonment. (10) Any person who receives, possesses, transfers, buys, sells, controls, or has custody of any card-making equipment with intent that such equipment be used in the manufacture of counterfeit cards commits an offence and shall be liable on conviction to imprisonment for a term of not more than 5 years or to a fine of not more than ₦7,000,000.00 or to both such fine and imprisonment. (11) Any person who, with intent to defraud another person, falsely alters any invoice for money, goods, services, or anything else of value obtained by use of a card after that invoice has been signed by the cardholder or a person authorized by him, commits an offence and shall be liable on conviction to imprisonment for a term of not more than 3 years or to a fine of not more than ₦5,000,000.00 or to both such fine and imprisonment. (12) Any institution that makes available, lends, donates, or sells any list or portion of a list of cardholders and their addresses and account numbers to any person without the prior written permission of the cardholder(s), commits an offence and shall be liable on conviction to a fine of ₦10,000,000.00. (13) An institution may make available to the Central Bank of Nigeria or a licensed credit bureau, which seeks to determine only the cardholder's rating, any list or portion of a list of any cardholder and their addresses without the permission of the cardholder, but must within 7 working days, give notice in writing of the disclosure to the cardholder. Such institution which fails to comply with the requirement to notify the cardholder, commits an offence and shall be liable on conviction to a fine of not more than ₦1,000,000.00. **Cybercrimes Act 2015 Section 34** **Cybercrimes Act 2015 Section 35** **Dealing in Card of Another**

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	Any person, other than the issuer, who receives and retains possession of two or more cards issued in the name or names of different cardholders, which cards he knows were taken or retained under circumstances which constitute a card theft commits an offence and is liable on summary conviction to 3 years imprisonment or to a fine of one ₦1,000,000.00and shall further be liable to repayment in monetary terms the value of loss sustained by the cardholder or forfeiture of the assets or goods acquired with the funds from the account of the cardholder. **Cybercrimes Act 2015 Section 36** **Use of Fraudulent Device or Attached E-mails and Websites** (1) Any person who with intent to defraud uses any device or attachment, e-mails or fraudulent website to obtain information or details of a cardholder commits an offence and upon conviction is liable to imprisonment for a period of 3 years or to a fine of ₦1,000,000.00 or both. (2) Any person who fraudulently re-direct funds transfer instructions during transmissions over any authorized communications path or device and re-directs funds transferred electronically with an authorized account commits any offence and upon conviction is liable to imprisonment for a period of 3years or to a fine of ₦1,000,000.00 and shall further be liable to payment in monetary terms the value of loss sustained by the cardholder or forfeiture of the assets or goods acquired with the funds from the account of the cardholder.
Title 3 – Content-related offences	
Article 9 – Offences related to child pornography 1 Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally and without right, the following conduct: a producing child pornography for the purpose of its distribution through a computer system; b offering or making available child pornography through a computer system; c distributing or transmitting child pornography through a	**Cybercrimes Act 2015 Section 23** **Child pornography and related offences** (1) Any person who intentionally uses any computer system or network in or for- (a) producing child pornography; (b) offering or making available child pornography;

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
computer system; d procuring child pornography through a computer system for oneself or for another person; e possessing child pornography in a computer system or on a computer-data storage medium. 2 For the purpose of paragraph 1 above, the term "child pornography" shall include pornographic material that visually depicts: a a minor engaged in sexually explicit conduct; b a person appearing to be a minor engaged in sexually explicit conduct; c realistic images representing a minor engaged in sexually explicit conduct 3 For the purpose of paragraph 2 above, the term "minor" shall include all persons under 18 years of age. A Party may, however, require a lower age-limit, which shall be not less than 16 years. 4 Each Party may reserve the right not to apply, in whole or in part, paragraphs 1, sub-paragraphs d. and e, and 2, sub-paragraphs b. and c.	(c) distributing or transmitting child pornography; (d) procuring child pornography for oneself or for another person; (e) possessing child pornography in a computer system or on a computer-data storage medium: commits an offence under this Act and shall be liable on conviction – (i) in the case of paragraphs (a), (b) and (c) to imprisonment for a term of 10 years or a fine of not more than ₦20,000,000.00 or to both fine and imprisonment; and (ii) in the case of paragraphs (d) and (e) of this subsection, to imprisonment for a term of not more than 5 years or a fine of not more than ₦10,000,000.00 or to both such fine and imprisonment. (2) Any person who knowingly makes or sends other pornographic images to another computer by way of unsolicited distribution shall be guilty of an offence and upon conviction shall be sentenced to One year imprisonment or a fine of Two Hundred and Fifty Thousand Naira or both. (3) Any person who, intentionally proposes, grooms or solicits, through any computer system or network, to meet a child for the purpose of: (a) engaging in sexual activities with the child; (b) engaging in sexual activities with the child where – (i) use is made of coercion, inducement, force or threats; (ii) abuse is made of a recognized position of trust, authority or influence over the child, including within the family; or (iii) abuse is made of a particularly vulnerable situation of the child, mental or physical disability or a situation of dependence;

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	(c) recruiting, inducing, coercing, exposing, or causing a child to participate in pornographic performances or profiting from or otherwise exploiting a child for such purposes; commits an offence under this Act and shall be liable on conviction - (i) in the case of paragraphs (a) to imprisonment for a term of not more than 10 years and a fine of not more than ₦15,000,000.00; and (ii) in the case of paragraphs (b) and (c) of this subsection, to imprisonment for a term of not more than 15 years and a fine of not more than ₦25,000,000. (4) For the purpose of subsection (1) above, the term "child pornography" shall include pornographic material that visually depicts - (a) a minor engaged in sexually explicit conduct; (b) a person appearing to be a minor engaged in sexually explicit conduct; and (c) realistic images representing a minor engaged in sexually explicit conduct. (5) For the purpose of this section, the term "child" or "minor" means a person below 18 years of age.
Title 4 – Offences related to infringements of copyright and related rights	
Article 10 – Offences related to infringements of copyright and related rights 1 Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law the infringement of copyright, as defined under the law of that Party, pursuant to the obligations it has undertaken under the Paris Act of 24 July 1971 revising the Bern Convention for the Protection of Literary and Artistic Works, the Agreement on Trade-Related Aspects of Intellectual Property Rights and the WIPO Copyright Treaty, with the exception of any moral rights conferred by such conventions, where such acts are committed wilfully, on a commercial scale and by means of a computer system.	**Copyright Act 1990 Section 25** A performer's right is infringed by a person who, without the performer's consent or authorisation in writing, does any of the following, that is - (a) makes a recording of the whole or substantial part of a live performance: Provided that where the consent sought is to make a recording of the work for

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
2 Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law the infringement of related rights, as defined under the law of that Party, pursuant to the obligations it has undertaken under the International Convention for the Protection of Performers, Producers of Phonograms and Broadcasting Organisations (Rome Convention), the Agreement on Trade-Related Aspects of Intellectual Property Rights and the WIPO Performances and Phonograms Treaty, with the exception of any moral rights conferred by such conventions, where such acts are committed wilfully, on a commercial scale and by means of a computer system. 3 A Party may reserve the right not to impose criminal liability under paragraphs 1 and 2 of this article in limited circumstances, provided that other effective remedies are available and that such reservation does not derogate from the Party's international obligations set forth in the international instruments referred to in paragraphs 1 and 2 of this article.	research, private or domestic use, such consent shall not be reasonably refused; (b) broadcasts live, or includes live in a cable programme, the whole or a substantial part of the live performance; (c) performs in public the whole or a substantial part of the live performance; (d) shows or plays in public the whole or a substantial part of the live performance for commercial purposes; (e) broadcast, or includes in a cable programme, a substantial part of the performance by means of recording which is, and which that person knows or has reason to believe was made without the performer's consent; (f) imports into the country otherwise than for his private or domestic use, a recording of a performer's work which is an infringing recording; or (g) in the course of trade or business, sells or lets for hire, offers, distributes or displays for sale or hire a recording of a performer's work which is an infringing recording. **Copyright Act 1990 Section 27** Notwithstanding the provisions of section 25 of this Act, a person who does any of the acts set out in the said section 25 shall, unless he proves to the satisfaction of the court that he did not know that this conduct was an infringement of the performer's right, be liable on conviction - (a) in the case of an individual, to a fine not exceeding N10,000; (b) in the case of a body corporate, to a fine of N50,000; (c) in all other cases, to a fine of N100 for each copy dealt with in contravention or to imprisonment for twelve months or to both such fine and imprisonment.

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	(2) A court before which an offence under this section is tried shall order that the recording or any other part thereof be delivered to the performer.
Title 5 – Ancillary liability and sanctions	
Article 11 – Attempt and aiding or abetting 1 Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, aiding or abetting the commission of any of the offences established in accordance with Articles 2 through 10 of the present Convention with intent that such offence be committed. 2 Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, an attempt to commit any of the offences established in accordance with Articles 3 through 5, 7, 8, and 9.1.a and c. of this Convention. 3 Each Party may reserve the right not to apply, in whole or in part, paragraph 2 of this article.	**Cybercrimes Act 2015 Section 27** **Attempt, conspiracy, aiding and abetting** (1) Any person who – (a) attempts to commit any offence under this Act; or (b) aids, abets, conspires, counsels or procures another person(s) to commit any offence under this Act: commits an offence and shall be liable on conviction to the punishment provided for the principal offence under this Act. (2) Any employee of a financial institution found to have connived with another person or group of persons to perpetrate fraud using computer system(s) or network, commits an offence and shall be liable on conviction to imprisonment for a term of not more than 7 years and shall in addition, refund the stolen money or forfeit any property to which it has been converted to the bank, financial institution or the customer.
Article 12 – Corporate liability 1 Each Party shall adopt such legislative and other measures as may be necessary to ensure that legal persons can be held liable for a criminal offence established in accordance with this Convention, committed for their benefit by any natural person, acting either individually or as part of an organ of the legal person, who has a leading position within it, based on: a a power of representation of the legal person; b an authority to take decisions on behalf of the legal person; c an authority to exercise control within the legal person. 2 In addition to the cases already provided for in paragraph 1 of this article, each Party shall take the measures necessary to ensure that a legal person can be held liable where the lack of supervision or control by a natural	**Corporate criminal liability is foreseen in Federal and State laws and also reflected in a number of provisions of the Cybercrime Act 2015 (e.g. Sections 37 to 40).**

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
person referred to in paragraph 1 has made possible the commission of a criminal offence established in accordance with this Convention for the benefit of that legal person by a natural person acting under its authority. 3 Subject to the legal principles of the Party, the liability of a legal person may be criminal, civil or administrative. 4 Such liability shall be without prejudice to the criminal liability of the natural persons who have committed the offence.	
Article 13 – Sanctions and measures 1 Each Party shall adopt such legislative and other measures as may be necessary to ensure that the criminal offences established in accordance with Articles 2 through 11 are punishable by effective, proportionate and dissuasive sanctions, which include deprivation of liberty. 2 Each Party shall ensure that legal persons held liable in accordance with Article 12 shall be subject to effective, proportionate and dissuasive criminal or non-criminal sanctions or measures, including monetary sanctions.	
Section 2 – Procedural law	
Article 14 – Scope of procedural provisions 1 Each Party shall adopt such legislative and other measures as may be necessary to establish the powers and procedures provided for in this section for the purpose of specific criminal investigations or proceedings. 2 Except as specifically provided otherwise in Article 21, each Party shall apply the powers and procedures referred to in paragraph 1 of this article to: a the criminal offences established in accordance with Articles 2 through 11 of this Convention; b other criminal offences committed by means of a computer system; and c the collection of evidence in electronic form of a criminal offence. 3 a Each Party may reserve the right to apply the measures referred to in Article 20 only to offences or categories of offences specified in the reservation, provided that the range of such offences or categories of offences is not more restricted than the range of offences to which it applies	**Evidence Act 2011 Section 84** **Admissibility of Statements in Documents Produced by Computers** (1) In any proceeding a statement contained in a document produced by a computer shall be admissible as evidence of any fact stated in it of which direct oral evidence would be admissible, if it is shown that the conditions in subsection (2) of this section are satisfied in relation to the statement and computer in question (2) The conditions referred to in subsection (1) of this section are – (a) that the document containing the statement was produced by the computer during a period over which the computer was used regularly to store or process information for the purposes of any activities regularly carried on over that period, whether for profit or not by anybody, whether corporate or not, or by any individual,

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
the measures referred to in Article 21. Each Party shall consider restricting such a reservation to enable the broadest application of the measure referred to in Article 20. b Where a Party, due to limitations in its legislation in force at the time of the adoption of the present Convention, is not able to apply the measures referred to in Articles 20 and 21 to communications being transmitted within a computer system of a service provider, which system: i is being operated for the benefit of a closed group of users, and ii does not employ public communications networks and is not connected with another computer system, whether public or private, that Party may reserve the right not to apply these measures to such communications. Each Party shall consider restricting such a reservation to enable the broadest application of the measures referred to in Articles 20 and 21	(b) that over that period there was regularly supplied to the computer in the ordinary course of those activities information of the kind contained in the statement or of the kind from which the information so contained is derived, (c) that throughout the material part of that period the computer was operating properly or, if not, that in any respect in which it was not operating properly or was out of operation during that part of that period was not such as to affect the production of the document or the accuracy of its contents, and (d) that the information contained in the statement reproduces or is derived from information supplied to the computer in the ordinary course of those activities. (3) Where over a period the functioning of storing or processing information for the purposes of any activities regularly carried on over that period as mentioned in subsection (2) (a) of this section was regularly performed by computers, whether – (a) by a combination of computers operating over that period; (b) by different computers operating in succession over that period; (c) by different combinations of computers operating in succession over that period; or (d) in any other manner involving the successive operation over that period, in whatever order, of one or more computers and one or more combinations of computers, all the computers used for that purpose during that period shall be treated for the purposes of this section as constituting a single computer; and reference in this section to a computer shall be construed accordingly. (4) In any proceeding where is desired to give a statement in evidence by virtue of this section, a certificate – (a) identifying the document containing the statement and describing the

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	manner in which it was produced, (b) giving such particulars of any device involved in the production of that document as may be appropriate for the purpose of showing that the document was produced by a computer, (c) dealing with any of the matters to which the conditions mentioned in subsection (2) above relate, and purporting to be signed by a person occupying a responsible position in relation to the operation of the relevant device or the management of the relevant activities, as the case may be, shall be evidence of the matter stated in the certificate; and for the purpose of this subsection it shall be sufficient for a matter to be stated to the best of the knowledge and belief of the person stating it. (5) For the purposes of this section – (a) information shall be taken to be supplied to a computer if it is supplied to it in any appropriate form and whether it is supplied directly or (with or without human intervention) by means of any appropriate equipment; (b) where, in the course of activities carried on by any individual or body, information is supplied with a view to its being stored or processed for the purpose of those activities by a computer operated otherwise than in the course of those activities, that information, if duly supplied to that computer, shall be taken to be supplied to it in the course of those activities; (c) a document shall be taken to have been produced by a computer whether it was produced by it directly or (with or without human intervention) by means of any appropriate equipment. **Evidence Act, 2011 Section 258** (1) In this Act "bank" or "banker" means a bank licensed under the Banks and Other Financial Institutions Act Cap B3LFN, 2004 and includes anybody authorised under an enactment to carry on banking nosiness;

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	"banker's book" (and related expressions) includes ledger, day books, account books and all other books used in banking business; "banking business" has the meaning assigned to it in the Banks and Other Financial Institutions Act 1991; "the Constitution" means the Constitution of the Federal Republic of Nigeria 1999; "copy of a document" includes – (a) in the case of a document falling within paragraph (b) but not (c) of the definition of "document" in this subsection, a transcript of the sounds or other data embodied in it; (b) in the case of a document falling within paragraph (b) but not (c) of that definition, a reproduction or still reproduction of the image or images embodied in it whether enlarged or not; (c) in the case of a document falling within both those paragraphs, such a transcript together with such a still reproduction; and (d) in the case of a document not falling within the said paragraph (c) of which a visual image is embodied in a document falling within that paragraph, a reproduction of that image, whether enlarged or not, and any reference to a copy of the material part of a document shall be construed accordingly; "computer" means any device for storing and processing information, and any reference to information being derived from other information is a reference to its being derived from it by calculation, comparison or any other process; "court" includes all judges and magistrates and, except arbitrators, all persons legally authorised to take evidence; "custom" means a rule which, in a particular district, has, from long usage, obtained the force of law;

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	"document" includes (a) books, maps, plans, graphs, drawings, photographs, and also includes any matter expressed or described upon any substance by means of letters, figures or marks or by more than one of these means, intended to be used or which may be used for the purpose of recording that matter; (b) any disc, tape, sound track or other device in which sounds or other data (not being visual images) are embodied so as to be capable (with or without the aid of some other equipment) of being reproduced from it, and (c) any film, negative, tape or other device in which one or more visual images are embodied so as to be capable (with or without the aid of some other equipment) of being reproduced from it; and (d) any device by means of which information is recorded, stored or retrievable including computer output; "fact" includes (a) anything, state of things, or relation of things, capable of being perceived by the senses, and (b) any mental condition of which any person is conscious; "fact in issue" includes any fact from which either by itself or in connection with other facts the existence, non-existence, nature or extent of any right, liability or disability asserted or denied in any suit or proceeding necessarily follows; "film" includes a microfilm; "financial institution" has the meaning assigned to "other financial institution" by the Banks and Other Financial Institutions Act 1991; "person interested" means any person likely to be personally affected by the outcome of a proceeding;

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	"Public Service of the Federation or of a State" has the meaning assigned thereto in the Constitution, and "public officer" shall be construed accordingly; "real evidence" means anything other than testimony admissible hearsay or a document the contents of which are offered as evidence of a fact at a trial, which is examined by the court as a means of proof of such fact; "statement" includes any representation of fact whether made in words or otherwise; and "wife" and "husband" mean respectively the wife and husband of a marriage validly contracted under the Marriage Act, or under Islamic Law or a Customary law applicable in Nigeria, and includes any marriage recognised as valid under the Marriage Act (2) In this Act, any reference to a section or other provision of the Criminal Code Act or the Criminal Procedure Act shall, as case may be, be construed as including a reference to the corresponding section or provision of the Criminal Code Law or Penal Code Law or the Criminal Procedure Code Law of a State or in respects of the Federal Capital Territory, Abuja, the Penal Code Act or the Criminal Procedure Code Act, whichever may be appropriate. **Cybercrimes Act 2015 Section 41** **Co-ordination and enforcement** (1) The office of the National Security Adviser shall be the coordinating body for all security and enforcement agencies under this Act and shall; (a) provide support to all relevant security, intelligence, law enforcement agencies and military services to prevent and combat cybercrimes in Nigeria; (b) ensure formulation and effective implementation of a comprehensive cyber security strategy and a national cyber security policy for Nigeria; (c) establish and maintain a National Computer Emergency Response Team (CERT) Coordination Center responsible for managing cyber incidences in

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	Nigeria; (d) establish and maintain a National Computer Forensic Laboratory and coordinate utilization of the facility by all law enforcement, security and intelligence agencies; (e) build capacity for the effective discharge of the functions of all relevant security, intelligence, law enforcement and military services under this Act or any other law on cybercrime in Nigeria; (f) establish appropriate platforms for public private partnership (PPP); (g) coordinate Nigeria's involvement in international cyber security cooperation to ensure the integration of Nigeria into the global frameworks on cyber security; and (h) do such other acts or things that are necessary for the effective performance of the functions of the relevant security and enforcement agencies under this Act. (2) The Attorney-General of the Federation shall strengthen and enhance the existing legal framework to ensure – (a) conformity of Nigeria's cybercrime and cyber security laws and policies with regional and international standards; (b) maintenance of international co-operation required for preventing and combating cybercrimes and promoting cyber security; and (c) effective prosecution of cybercrimes and cyber security matters. (3) All law enforcement, security and intelligence agencies shall develop requisite institutional capacity for the effective implementation of the provisions of this Act and shall in collaboration with the Office of the National Security Adviser, initiate, develop or organize training programmers nationally or internationally for officers charged with the responsibility for the prohibition, prevention, detection, investigation and prosecution of cybercrimes.

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
Article 15 – Conditions and safeguards 1 Each Party shall ensure that the establishment, implementation and application of the powers and procedures provided for in this Section are subject to conditions and safeguards provided for under its domestic law, which shall provide for the adequate protection of human rights and liberties, including rights arising pursuant to obligations it has undertaken under the 1950 Council of Europe Convention for the Protection of Human Rights and Fundamental Freedoms, the 1966 United Nations International Covenant on Civil and Political Rights, and other applicable international human rights instruments, and which shall incorporate the principle of proportionality. 2 Such conditions and safeguards shall, as appropriate in view of the nature of the procedure or power concerned, *inter alia,* include judicial or other independent supervision, grounds justifying application, and limitation of the scope and the duration of such power or procedure. 3 To the extent that it is consistent with the public interest, in particular the sound administration of justice, each Party shall consider the impact of the powers and procedures in this section upon the rights, responsibilities and legitimate interests of third parties.	**Cybercrimes Act 2015 Section 45** **Power of arrest, search and seizure** (1) A law enforcement officer may apply ex-parte to a Judge in chambers for the issuance of a warrant for the purpose of obtaining electronic evidence in related crime investigation. (2) The Judge may issue a warrant authorizing a law enforcement officer to - (a) enter and search any premises or place if within those premises, place or conveyance – (i) an offence under this Act is being committed; or (ii) there is evidence of the commission of an offence under this Act; or (iii) there is an urgent need to prevent the commission of an offence under this Act (b) search any person or conveyance found on any premises or place which such authorized officers who are empowered to enter and search under paragraph (a) of this subsection; (c) stop, board and search any conveyance where there is evidence of the commission of an offence under this Act; (d) seize, remove and detain anything which is, or contains evidence of the commission of an offence under this Act; (e) use or cause to use a computer or any device to search any data contained in or available to any computer system or computer network; (f) use any technology to decode or decrypt any coded or encrypted data contained in a computer into readable text or comprehensible format; (g) require any person having charge of or otherwise concerned with the

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	operation of any computer or electronic device in connection with an offence under this Act to produce such computer or electronic device. (3) The court shall issue a warrant under subsection (2) of this section where it is satisfied that – (a) the warrant is sought to prevent the commission of an offence under this Act or to prevent the interference with investigative process under this Act; or (b) the warrant is for the purpose of investigating cybercrime, cyber security breach, computer related offences or obtaining electronic evidence; or (c) there are reasonable grounds for believing that the person or material on the premises or conveyance may be relevant to the cybercrime or computer related offences under investigation; or (d) the person named in the warrant is preparing to commit an offence under this Act.
Article 16 – Expedited preservation of stored computer data 1 Each Party shall adopt such legislative and other measures as may be necessary to enable its competent authorities to order or similarly obtain the expeditious preservation of specified computer data, including traffic data, that has been stored by means of a computer system, in particular where there are grounds to believe that the computer data is particularly vulnerable to loss or modification. 2 Where a Party gives effect to paragraph 1 above by means of an order to a person to preserve specified stored computer data in the person's possession or control, the Party shall adopt such legislative and other measures as may be necessary to oblige that person to preserve and maintain the integrity of that computer data for a period of time as long as necessary, up to a maximum of ninety days, to enable the competent authorities to seek its disclosure. A Party may provide for such an order to be subsequently renewed. 3 Each Party shall adopt such legislative and other measures as may be	**Cybercrimes Act 2015 Section 38** **Records retention and protection of data** (1) A service provider shall keep all traffic data and subscriber information as may be prescribed by the relevant authority for the time being, responsible for the regulation of communication services in Nigeria, for a period of 2 years. (2) A service provider shall, at the request of the relevant authority referred to in subsection (1) of this section 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 be kept under subsection (1) of this section. (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 and

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
necessary to oblige the custodian or other person who is to preserve the computer data to keep confidential the undertaking of such procedures for the period of time provided for by its domestic law. 4 The powers and procedures referred to in this article shall be subject to Articles 14 and 15.	it shall be the duty of the service provider to comply. (4) Any data retained, processed or retrieved by the service provider at the request of any law enforcement agency under this Act shall not be utilized except for legitimate purposes as may be provided for under this Act, any other legislation, regulation or by an order of a court of competent jurisdiction. (5) 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) Subject to the provisions of this Act, any person who contravenes any of the provisions of this section commits an offence and shall be liable on conviction to imprisonment for a term of not more than 3 years or a fine of not more than N7,000,000.00 or to both fine and imprisonment.
Article 17 – Expedited preservation and partial disclosure of traffic data 1 Each Party shall adopt, in respect of traffic data that is to be preserved under Article 16, such legislative and other measures as may be necessary to: a ensure that such expeditious preservation of traffic data is available regardless of whether one or more service providers were involved in the transmission of that communication; and b ensure the expeditious disclosure to the Party's competent authority, or a person designated by that authority, of a sufficient amount of traffic data to enable the Party to identify the service providers and the path through which the communication was transmitted. 2 The powers and procedures referred to in this article shall be subject to Articles 14 and 15.	
Article 18 – Production order 1 Each Party shall adopt such legislative and other measures as may be necessary to empower its competent authorities to order: a a person in its territory to submit specified computer data in that	**Cybercrimes Act 2015 Section 38** **Records retention and protection of data**

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
person's possession or control, which is stored in a computer system or a computer-data storage medium; and b a service provider offering its services in the territory of the Party to submit subscriber information relating to such services in that service provider's possession or control. 2 The powers and procedures referred to in this article shall be subject to Articles 14 and 15. 3 For the purpose of this article, the term "subscriber information" means any information contained in the form of computer data or any other form that is held by a service provider, relating to subscribers of its services other than traffic or content data and by which can be established: a the type of communication service used, the technical provisions taken thereto and the period of service; b the subscriber's identity, postal or geographic address, telephone and other access number, billing and payment information, available on the basis of the service agreement or arrangement; c any other information on the site of the installation of communication equipment, available on the basis of the service agreement or arrangement.	(1) A service provider shall keep all traffic data and subscriber information as may be prescribed by the relevant authority for the time being, responsible for the regulation of communication services in Nigeria, for a period of 2 years. (2) A service provider shall, at the request of the relevant authority referred to in subsection (1) of this section 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 be kept under subsection (1) of this section. (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 and it shall be the duty of the service provider to comply. (4) Any data retained, processed or retrieved by the service provider at the request of any law enforcement agency under this Act shall not be utilized except for legitimate purposes as may be provided for under this Act, any other legislation, regulation or by an order of a court of competent jurisdiction. (5) 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) Subject to the provisions of this Act, any person who contravenes any of the provisions of this section commits an offence and 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 to both fine and imprisonment.
Article 19 – Search and seizure of stored computer data 1 Each Party shall adopt such legislative and other measures as may be necessary to empower its competent authorities to search or similarly access: a a computer system or part of it and computer data stored	**Cybercrimes Act 2015 Section 45** **Power of arrest, search and seizure** (1) A law enforcement officer may apply ex-parte to a Judge in chambers for the issuance of a warrant for the purpose of obtaining electronic evidence in related

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
therein; and b a computer-data storage medium in which computer data may be stored in its territory. 2 Each Party shall adopt such legislative and other measures as may be necessary to ensure that where its authorities search or similarly access a specific computer system or part of it, pursuant to paragraph 1.a, and have grounds to believe that the data sought is stored in another computer system or part of it in its territory, and such data is lawfully accessible from or available to the initial system, the authorities shall be able to expeditiously extend the search or similar accessing to the other system. 3 Each Party shall adopt such legislative and other measures as may be necessary to empower its competent authorities to seize or similarly secure computer data accessed according to paragraphs 1 or 2. These measures shall include the power to: a seize or similarly secure a computer system or part of it or a computer-data storage medium; b make and retain a copy of those computer data; c maintain the integrity of the relevant stored computer data; d render inaccessible or remove those computer data in the accessed computer system. 4 Each Party shall adopt such legislative and other measures as may be necessary to empower its competent authorities to order any person who has knowledge about the functioning of the computer system or measures applied to protect the computer data therein to provide, as is reasonable, the necessary information, to enable the undertaking of the measures referred to in paragraphs 1 and 2. 5 The powers and procedures referred to in this article shall be subject to Articles 14 and 15.	crime investigation. (2) The Judge may issue a warrant authorizing a law enforcement officer to - (a) enter and search any premises or place if within those premises, place or conveyance – (i) an offence under this Act is being committed; or (ii) there is evidence of the commission of an offence under this Act; or (iii) there is an urgent need to prevent the commission of an offence under this Act (b) search any person or conveyance found on any premises or place which such authorized officers who are empowered to enter and search under paragraph (a) of this subsection; (c) stop, board and search any conveyance where there is evidence of the commission of an offence under this Act; (d) seize, remove and detain anything which is, or contains evidence of the commission of an offence under this Act; (e) use or cause to use a computer or any device to search any data contained in or available to any computer system or computer network; (f) use any technology to decode or decrypt any coded or encrypted data contained in a computer into readable text or comprehensible format; (g) require any person having charge of or otherwise concerned with the operation of any computer or electronic device in connection with an offence under this Act to produce such computer or electronic device. (3) The court shall issue a warrant under subsection (2) of this section where it

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	is satisfied that – (a) the warrant is sought to prevent the commission of an offence under this Act or to prevent the interference with investigative process under this Act; or (b) the warrant is for the purpose of investigating cybercrime, cyber security breach, computer related offences or obtaining electronic evidence; or (c) there are reasonable grounds for believing that the person or material on the premises or conveyance may be relevant to the cybercrime or computer related offences under investigation; or (d) the person named in the warrant is preparing to commit an offence under this Act.
Article 20 – Real-time collection of traffic data 1 Each Party shall adopt such legislative and other measures as may be necessary to empower its competent authorities to: a collect or record through the application of technical means on the territory of that Party, and b compel a service provider, within its existing technical capability: i to collect or record through the application of technical means on the territory of that Party; or ii to co-operate and assist the competent authorities in the collection or recording of, traffic data, in real-time, associated with specified communications in its territory transmitted by means of a computer system. 2 Where a Party, due to the established principles of its domestic legal system, cannot adopt the measures referred to in paragraph 1.a, it may instead adopt legislative and other measures as may be necessary to ensure the real-time collection or recording of traffic data associated with specified communications transmitted in its territory, through the application of technical means on that territory.	**Cybercrimes Act 2015 Section 39** **Interception of electronic communications** Where there are reasonable grounds to suspect that the content of any electronic communication is reasonably required for the purposes of a 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 and/or traffic data associated with specified communications transmitted by means of a computer system; or (b) authorize a law enforcement officer to collect or record such data through application of technical means.

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
3 Each Party shall adopt such legislative and other measures as may be necessary to oblige a service provider to keep confidential the fact of the execution of any power provided for in this article and any information relating to it. 4 The powers and procedures referred to in this article shall be subject to Articles 14 and 15.	
Article 21 – Interception of content data 1 Each Party shall adopt such legislative and other measures as may be necessary, in relation to a range of serious offences to be determined by domestic law, to empower its competent authorities to: a collect or record through the application of technical means on the territory of that Party, and b compel a service provider, within its existing technical capability: i to collect or record through the application of technical means on the territory of that Party, or ii to co-operate and assist the competent authorities in the collection or recording of, content data, in real-time, of specified communications in its territory transmitted by means of a computer system. 2 Where a Party, due to the established principles of its domestic legal system, cannot adopt the measures referred to in paragraph 1.a, it may instead adopt legislative and other measures as may be necessary to ensure the real-time collection or recording of content data on specified communications in its territory through the application of technical means on that territory. 3 Each Party shall adopt such legislative and other measures as may be necessary to oblige a service provider to keep confidential the fact of the execution of any power provided for in this article and any information relating to it. 4 The powers and procedures referred to in this article shall be subject to Articles 14 and 15.	**Cybercrimes Act 2015 Section 39** **Interception of electronic communications** Where there are reasonable grounds to suspect that the content of any electronic communication is reasonably required for the purposes of a 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 and/or traffic data associated with specified communications transmitted by means of a computer system; or (b) authorize a law enforcement officer to collect or record such data through application of technical means.
Section 3 – Jurisdiction	
Article 22 – Jurisdiction 1 Each Party shall adopt such legislative and other measures as may be necessary to establish jurisdiction over any offence established in	**Cybercrimes Act 2015 Section 50** **Jurisdiction**

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
accordance with Articles 2 through 11 of this Convention, when the offence is committed: a in its territory; or b on board a ship flying the flag of that Party; or c on board an aircraft registered under the laws of that Party; or d by one of its nationals, if the offence is punishable under criminal law where it was committed or if the offence is committed outside the territorial jurisdiction of any State. 2 Each Party may reserve the right not to apply or to apply only in specific cases or conditions the jurisdiction rules laid down in paragraphs 1.b through 1.d of this article or any part thereof. 3 Each Party shall adopt such measures as may be necessary to establish jurisdiction over the offences referred to in Article 24, paragraph 1, of this Convention, in cases where an alleged offender is present in its territory and it does not extradite him or her to another Party, solely on the basis of his or her nationality, after a request for extradition. 4 This Convention does not exclude any criminal jurisdiction exercised by a Party in accordance with its domestic law. When more than one Party claims jurisdiction over an alleged offence established in accordance with this Convention, the Parties involved shall, where appropriate, consult with a view to determining the most appropriate jurisdiction for prosecution.	(1) The Federal High Court located in any part of Nigeria regardless of the location where the offence is committed shall have jurisdiction to try offences under this Act, if committed – (a) in Nigeria; or (b) in a ship or aircraft registered in Nigeria; or (c) by a citizen or resident in Nigeria if the person's conduct would also constitute an offence under a law of the country where the offence was committed; or (d) outside Nigeria, where – (i) the victim of the offence is a citizen or resident of Nigeria; or (ii) the alleged offender is in Nigeria and not extradited to any other country for prosecution. (2) In the trial of any offence under this Act, the fact that an accused person is in possession of- (a) pecuniary resources or property for which he cannot satisfactorily account; or (b) which is disproportional to his known sources of income; or (c) that he had at or about the time of the alleged offence obtained an accretion to his pecuniary resources or property for which he cannot satisfactorily account: may, if proved, be taken into consideration by the Court as corroborating the testimony of witness in the trial. (3) The court shall ensure that all matters brought before it by the Commission against any person, body or authority shall be conducted with dispatch and given accelerated hearing.

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	(4) Subject to the provisions of the Constitution of the Federal Republic of Nigeria, an application for stay of proceedings in respect of any criminal matter brought under this Act shall not be entertained until judgment is delivered.
Chapter III – International co-operation	
Article 24 – Extradition 1 a This article applies to extradition between Parties for the criminal offences established in accordance with Articles 2 through 11 of this Convention, provided that they are punishable under the laws of both Parties concerned by deprivation of liberty for a maximum period of at least one year, or by a more severe penalty. b Where a different minimum penalty is to be applied under an arrangement agreed on the basis of uniform or reciprocal legislation or an extradition treaty, including the European Convention on Extradition (ETS No. 24), applicable between two or more parties, the minimum penalty provided for under such arrangement or treaty shall apply. 2 The criminal offences described in paragraph 1 of this article shall be deemed to be included as extraditable offences in any extradition treaty existing between or among the Parties. The Parties undertake to include such offences as extraditable offences in any extradition treaty to be concluded between or among them. 3 If a Party that makes extradition conditional on the existence of a treaty receives a request for extradition from another Party with which it does not have an extradition treaty, it may consider this Convention as the legal basis for extradition with respect to any criminal offence referred to in paragraph 1 of this article. 4 Parties that do not make extradition conditional on the existence of a treaty shall recognise the criminal offences referred to in paragraph 1 of this article as extraditable offences between themselves. 5 Extradition shall be subject to the conditions provided for by the law of the requested Party or by applicable extradition treaties, including the grounds on which the requested Party may refuse extradition. 6 If extradition for a criminal offence referred to in paragraph 1 of this article is refused solely on the basis of the nationality of the person sought, or because the requested Party deems that it has jurisdiction over the offence,	**Cybercrimes Act 2015 Section 52** **Request for mutual assistance** (1) The Attorney - General of the Federation may request or receive assistance from any agency or authority of a foreign State in the investigation or prosecution of offences under this Act; and may authorize or participate in any joint investigation or cooperation carried out for the purpose of detecting, preventing, responding and prosecuting any offence under this Act. (2) The joint investigation or cooperation referred to in sub-section (1) may be carried out whether or not any bilateral or multilateral agreements exist between Nigeria and the requested or requesting country. (3) The Attorney - General of the Federation may, without prior request, forward to a competent authority of a foreign State, information obtained in the course of investigation, if such information will assist in the investigation of an offence or in the apprehension of an offender under this Act.

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
the requested Party shall submit the case at the request of the requesting Party to its competent authorities for the purpose of prosecution and shall report the final outcome to the requesting Party in due course. Those authorities shall take their decision and conduct their investigations and proceedings in the same manner as for any other offence of a comparable nature under the law of that Party. 7 a Each Party shall, at the time of signature or when depositing its instrument of ratification, acceptance, approval or accession, communicate to the Secretary General of the Council of Europe the name and address of each authority responsible for making or receiving requests for extradition or provisional arrest in the absence of a treaty. b The Secretary General of the Council of Europe shall set up and keep updated a register of authorities so designated by the Parties. Each Party shall ensure	
Article 25 – General principles relating to mutual assistance 1 The Parties shall afford one another mutual assistance to the widest extent possible for the purpose of investigations or proceedings concerning criminal offences related to computer systems and data, or for the collection of evidence in electronic form of a criminal offence. 2 Each Party shall also adopt such legislative and other measures as may be necessary to carry out the obligations set forth in Articles 27 through 35. 3 Each Party may, in urgent circumstances, make requests for mutual assistance or communications related thereto by expedited means of communication, including fax or e-mail, to the extent that such means provide appropriate levels of security and authentication (including the use of encryption, where necessary), with formal confirmation to follow, where required by the requested Party. The requested Party shall accept and respond to the request by any such expedited means of communication. 4 Except as otherwise specifically provided in articles in this chapter, mutual assistance shall be subject to the conditions provided for by the law of the requested Party or by applicable mutual assistance treaties, including the grounds on which the requested Party may refuse co-operation. The	**Cybercrimes Act 2015 Section 52** **Request for mutual assistance** (1) The Attorney - General of the Federation may request or receive assistance from any agency or authority of a foreign State in the investigation or prosecution of offences under this Act; and may authorize or participate in any joint investigation or cooperation carried out for the purpose of detecting, preventing, responding and prosecuting any offence under this Act. (2) The joint investigation or cooperation referred to in sub-section (1) may be carried out whether or not any bilateral or multilateral agreements exist between Nigeria and the requested or requesting country. (3) The Attorney - General of the Federation may, without prior request, forward to a competent authority of a foreign State, information obtained in the course of investigation, if such information will assist in the investigation of an offence or in the apprehension of an offender under this Act. **Cybercrimes Act 2015 Section 53** **Evidence pursuant to a request**

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
requested Party shall not exercise the right to refuse mutual assistance in relation to the offences referred to in Articles 2 through 11 solely on the ground that the request concerns an offence which it considers a fiscal offence. 5 Where, in accordance with the provisions of this chapter, the requested Party is permitted to make mutual assistance conditional upon the existence of dual criminality, that condition shall be deemed fulfilled, irrespective of whether its laws place the offence within the same category of offence or denominate the offence by the same terminology as the requesting Party, if the conduct underlying the offence for which assistance is sought is a criminal offence under its laws.	(1) Any evidence gathered, pursuant to a request under this Act, in any investigation or proceedings in the court of any foreign State, if authenticated, shall be prima facie admissible in any proceedings to which this Act applies. (2) For the purpose of subsection (1) of this section, evidence is authenticated if it is – (a) certified by a Judge or Magistrate or Notary Public of the foreign State; or (b) sworn to under oath or affirmation of a witness or sealed with an official or public seal – (i) of a Ministry or Department of the Government of the foreign State; or (ii) in the case of a territory, protectorate or colony, of the person administering the Government of the foreign territory, protectorate or colony or a department of that territory, protectorate or colony.
Article 26 – Spontaneous information 1 A Party may, within the limits of its domestic law and without prior request, forward to another Party information obtained within the framework of its own investigations when it considers that the disclosure of such information might assist the receiving Party in initiating or carrying out investigations or proceedings concerning criminal offences established in accordance with this Convention or might lead to a request for co-operation by that Party under this chapter. 2 Prior to providing such information, the providing Party may request that it be kept confidential or only used subject to conditions. If the receiving Party cannot comply with such request, it shall notify the providing Party, which shall then determine whether the information should nevertheless be provided. If the receiving Party accepts the information subject to the conditions, it shall be bound by them.	**Cybercrimes Act 2015 Section 52** **Request for mutual assistance** (1) The Attorney - General of the Federation may request or receive assistance from any agency or authority of a foreign State in the investigation or prosecution of offences under this Act; and may authorize or participate in any joint investigation or cooperation carried out for the purpose of detecting, preventing, responding and prosecuting any offence under this Act. (2) The joint investigation or cooperation referred to in sub-section (1) may be carried out whether or not any bilateral or multilateral agreements exist between Nigeria and the requested or requesting country. (3) The Attorney - General of the Federation may, without prior request, forward to a competent authority of a foreign State, information obtained in the course of investigation, if such information will assist in the investigation of an offence or in the apprehension of an offender under this Act.

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
Article 27 – Procedures pertaining to mutual assistance requests in the absence of applicable international agreements 1 Where there is no mutual assistance treaty or arrangement on the basis of uniform or reciprocal legislation in force between the requesting and requested Parties, the provisions of paragraphs 2 through 9 of this article shall apply. The provisions of this article shall not apply where such treaty, arrangement or legislation exists, unless the Parties concerned agree to apply any or all of the remainder of this article in lieu thereof. 2 a Each Party shall designate a central authority or authorities responsible for sending and answering requests for mutual assistance, the execution of such requests or their transmission to the authorities competent for their execution. b The central authorities shall communicate directly with each other; c Each Party shall, at the time of signature or when depositing its instrument of ratification, acceptance, approval or accession, communicate to the Secretary General of the Council of Europe the names and addresses of the authorities designated in pursuance of this paragraph; d The Secretary General of the Council of Europe shall set up and keep updated a register of central authorities designated by the Parties. Each Party shall ensure that the details held on the register are correct at all times. 3 Mutual assistance requests under this article shall be executed in accordance with the procedures specified by the requesting Party, except where incompatible with the law of the requested Party. 4 The requested Party may, in addition to the grounds for refusal established in Article 25, paragraph 4, refuse assistance if: a the request concerns an offence which the requested Party considers a political offence or an offence connected with a political offence, or b it considers that execution of the request is likely to prejudice its sovereignty, security, *ordre public* or other essential interests. 5 The requested Party may postpone action on a request if such action would prejudice criminal investigations or proceedings conducted by its authorities. 6 Before refusing or postponing assistance, the requested Party shall, where appropriate after having consulted with the requesting Party, consider	**Cybercrimes Act 2015 Section 52** **Request for mutual assistance** (1) The Attorney - General of the Federation may request or receive assistance from any agency or authority of a foreign State in the investigation or prosecution of offences under this Act; and may authorize or participate in any joint investigation or cooperation carried out for the purpose of detecting, preventing, responding and prosecuting any offence under this Act. (2) The joint investigation or cooperation referred to in sub-section (1) may be carried out whether or not any bilateral or multilateral agreements exist between Nigeria and the requested or requesting country. (3) The Attorney - General of the Federation may, without prior request, forward to a competent authority of a foreign State, information obtained in the course of investigation, if such information will assist in the investigation of an offence or in the apprehension of an offender under this Act. **Cybercrimes Act 2015 Section 53** **Evidence pursuant to a request** (1) Any evidence gathered, pursuant to a request under this Act, in any investigation or proceedings in the court of any foreign State, if authenticated, shall be prima facie admissible in any proceedings to which this Act applies. (2) For the purpose of subsection (1) of this section, evidence is authenticated if it is – (a) certified by a Judge or Magistrate or Notary Public of the foreign State; or (b) sworn to under oath or affirmation of a witness or sealed with an official or public seal – (i) of a Ministry or Department of the Government of the foreign State; or

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
whether the request may be granted partially or subject to such conditions as it deems necessary. 7 The requested Party shall promptly inform the requesting Party of the outcome of the execution of a request for assistance. Reasons shall be given for any refusal or postponement of the request. The requested Party shall also inform the requesting Party of any reasons that render impossible the execution of the request or are likely to delay it significantly. 8 The requesting Party may request that the requested Party keep confidential the fact of any request made under this chapter as well as its subject, except to the extent necessary for its execution. If the requested Party cannot comply with the request for confidentiality, it shall promptly inform the requesting Party, which shall then determine whether the request should nevertheless be executed. 9 a In the event of urgency, requests for mutual assistance or communications related thereto may be sent directly by judicial authorities of the requesting Party to such authorities of the requested Party. In any such cases, a copy shall be sent at the same time to the central authority of the requested Party through the central authority of the requesting Party. b Any request or communication under this paragraph may be made through the International Criminal Police Organisation (Interpol). c Where a request is made pursuant to sub-paragraph a. of this article and the authority is not competent to deal with the request, it shall refer the request to the competent national authority and inform directly the requesting Party that it has done so. d Requests or communications made under this paragraph that do not involve coercive action may be directly transmitted by the competent authorities of the requesting Party to the competent authorities of the requested Party. e Each Party may, at the time of signature or when depositing its instrument of ratification, acceptance, approval or accession, inform the Secretary General of the Council of Europe that, for reasons of efficiency, requests made under this paragraph are to be addressed to its central authority.	(ii) in the case of a territory, protectorate or colony, of the person administering the Government of the foreign territory, protectorate or colony or a department of that territory, protectorate or colony.
Article 28 – Confidentiality and limitation on use 1 When there is no mutual assistance treaty or arrangement on the basis of uniform or reciprocal legislation in force between the requesting and the	

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
requested Parties, the provisions of this article shall apply. The provisions of this article shall not apply where such treaty, arrangement or legislation exists, unless the Parties concerned agree to apply any or all of the remainder of this article in lieu thereof. 2 The requested Party may make the supply of information or material in response to a request dependent on the condition that it is: a kept confidential where the request for mutual legal assistance could not be complied with in the absence of such condition, or b not used for investigations or proceedings other than those stated in the request. 3 If the requesting Party cannot comply with a condition referred to in paragraph 2, it shall promptly inform the other Party, which shall then determine whether the information should nevertheless be provided. When the requesting Party accepts the condition, it shall be bound by it. 4 Any Party that supplies information or material subject to a condition referred to in paragraph 2 may require the other Party to explain, in relation to that condition, the use made of such information or material.	
Article 29 – Expedited preservation of stored computer data 1 A Party may request another Party to order or otherwise obtain the expeditious preservation of data stored by means of a computer system, located within the territory of that other Party and in respect of which the requesting Party intends to submit a request for mutual assistance for the search or similar access, seizure or similar securing, or disclosure of the data. 2 A request for preservation made under paragraph 1 shall specify: a the authority seeking the preservation; b the offence that is the subject of a criminal investigation or proceedings and a brief summary of the related facts; c the stored computer data to be preserved and its relationship to the offence; d any available information identifying the custodian of the stored computer data or the location of the computer system; e the necessity of the preservation; and f that the Party intends to submit a request for mutual assistance for the search or similar access, seizure or similar securing, or disclosure of the stored computer data.	**Cybercrimes Act 2015 Section 55** **Expedited Preservation of computer data** (1) Nigeria may be requested to expedite the preservation of electronic device or data stored in a computer system, or network, referring to crimes described under this Act or any other enactment, pursuant to the submission of a request for assistance for search, seizure and disclosure of those data. (2) The request under subsection (1) of this section shall specify - (a) the authority requesting the preservation or disclosure; (b) the offence being investigated or prosecuted, as well as a brief statement of the facts relating thereto; (c) the electronic device or computer data to be retained and its relation to the offence; (d) all the available information to identify the person responsible for the

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
3 Upon receiving the request from another Party, the requested Party shall take all appropriate measures to preserve expeditiously the specified data in accordance with its domestic law. For the purposes of responding to a request, dual criminality shall not be required as a condition to providing such preservation. 4 A Party that requires dual criminality as a condition for responding to a request for mutual assistance for the search or similar access, seizure or similar securing, or disclosure of stored data may, in respect of offences other than those established in accordance with Articles 2 through 11 of this Convention, reserve the right to refuse the request for preservation under this article in cases where it has reasons to believe that at the time of disclosure the condition of dual criminality cannot be fulfilled. 5 In addition, a request for preservation may only be refused if: a the request concerns an offence which the requested Party considers a political offence or an offence connected with a political offence, or b the requested Party considers that execution of the request is likely to prejudice its sovereignty, security, *ordre public* or other essential interests. 6 Where the requested Party believes that preservation will not ensure the future availability of the data or will threaten the confidentiality of or otherwise prejudice the requesting Party's investigation, it shall promptly so inform the requesting Party, which shall then determine whether the request should nevertheless be executed. 4 Any preservation effected in response to the request referred to in paragraph 1 shall be for a period not less than sixty days, in order to enable the requesting Party to submit a request for the search or similar access, seizure or similar securing, or disclosure of the data. Following the receipt of such a request, the data shall continue to be preserved pending a decision on that request.	electronic device or data or the location of the computer system; (e) the necessity of the measure of preservation, and (f) the intention to submit a request for assistance for search, seizure and disclosure of the data. (3) In executing the demand of a foreign authority under the preceding sections, the Attorney - General of the Federation may order any person who has the control or availability of such data, including a service provider, to preserve them or turn them in for proper preservation by an appropriate authority or person. (4) Without prejudice to the provisions of subsection (3) of this section, the preservation may also be requested by any law enforcement agency, with responsibility for enforcing any provisions of this Act, pursuant to an order of court, which order may be obtained ex parte where there is urgency or danger in delay. (5) Where a court grants an order, pursuant to the provisions of subsection (4) of this section, such order shall indicate - (a) the nature of the evidence; (b) their origin and destination, if known; and (c) the period of time which shall not exceed 90 days over which data must be preserved. (6) In compliance with the preservation order, any person who has the control or availability of such data, including a service provider, shall immediately preserve the data for the specified period of time, protecting and maintaining its integrity. (7) A request for expedited preservation of electronic evidence or data may be refused if, there are reasonable grounds to believe that the execution of a request for legal assistance for subsequent search, seizure and release of such

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	data would be denied.
Article 30 – Expedited disclosure of preserved traffic data 1 Where, in the course of the execution of a request made pursuant to Article 29 to preserve traffic data concerning a specific communication, the requested Party discovers that a service provider in another State was involved in the transmission of the communication, the requested Party shall expeditiously disclose to the requesting Party a sufficient amount of traffic data to identify that service provider and the path through which the communication was transmitted. 2 Disclosure of traffic data under paragraph 1 may only be withheld if: a the request concerns an offence which the requested Party considers a political offence or an offence connected with a political offence; or b the requested Party considers that execution of the request is likely to prejudice its sovereignty, security, *ordre public* or other essential interests.	
Article 31 – Mutual assistance regarding accessing of stored computer data 1 A Party may request another Party to search or similarly access, seize or similarly secure, and disclose data stored by means of a computer system located within the territory of the requested Party, including data that has been preserved pursuant to Article 29. 2 The requested Party shall respond to the request through the application of international instruments, arrangements and laws referred to in Article 23, and in accordance with other relevant provisions of this chapter. 3 The request shall be responded to on an expedited basis where: a there are grounds to believe that relevant data is particularly vulnerable to loss or modification; or b the instruments, arrangements and laws referred to in paragraph 2 otherwise provide for expedited co-operation.	**Cybercrimes Act 2015 Section 52** **Request for mutual assistance** (1) The Attorney - General of the Federation may request or receive assistance from any agency or authority of a foreign State in the investigation or prosecution of offences under this Act; and may authorize or participate in any joint investigation or cooperation carried out for the purpose of detecting, preventing, responding and prosecuting any offence under this Act. (2) The joint investigation or cooperation referred to in sub-section (1) may be carried out whether or not any bilateral or multilateral agreements exist between Nigeria and the requested or requesting country. (3) The Attorney - General of the Federation may, without prior request, forward to a competent authority of a foreign State, information obtained in the course of investigation, if such information will assist in the investigation of an offence or in the apprehension of an offender under this Act. **Cybercrimes Act 2015 Section 53** **Evidence pursuant to a request**

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	(1) Any evidence gathered, pursuant to a request under this Act, in any investigation or proceedings in the court of any foreign State, if authenticated, shall be prima facie admissible in any proceedings to which this Act applies. (2) For the purpose of subsection (1) of this section, evidence is authenticated if it is – (a) certified by a Judge or Magistrate or Notary Public of the foreign State; or (b) sworn to under oath or affirmation of a witness or sealed with an official or public seal – (i) of a Ministry or Department of the Government of the foreign State; or (ii) in the case of a territory, protectorate or colony, of the person administering the Government of the foreign territory, protectorate or colony or a department of that territory, protectorate or colony.
Article 32 – Trans-border access to stored computer data with consent or where publicly available A Party may, without the authorisation of another Party: a access publicly available (open source) stored computer data, regardless of where the data is located geographically; or b access or receive, through a computer system in its territory, stored computer data located in another Party, if the Party obtains the lawful and voluntary consent of the person who has the lawful authority to disclose the data to the Party through that computer system.	
Article 33 – Mutual assistance in the real-time collection of traffic data 1 The Parties shall provide mutual assistance to each other in the real-time collection of traffic data associated with specified communications in their territory transmitted by means of a computer system. Subject to the provisions of paragraph 2, this assistance shall be governed by the conditions and procedures provided for under domestic law. 2 Each Party shall provide such assistance at least with respect to criminal offences for which real-time collection of traffic data would be available in a similar domestic case.	

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
Article 34 – Mutual assistance regarding the interception of content data The Parties shall provide mutual assistance to each other in the real-time collection or recording of content data of specified communications transmitted by means of a computer system to the extent permitted under their applicable treaties and domestic laws.	
Article 35 – 24/7 Network 1 Each Party shall designate a point of contact available on a twenty-four hour, seven-day-a-week basis, in order to ensure the provision of immediate assistance for the purpose of investigations or proceedings concerning criminal offences related to computer systems and data, or for the collection of evidence in electronic form of a criminal offence. Such assistance shall include facilitating, or, if permitted by its domestic law and practice, directly carrying out the following measures: a the provision of technical advice; b the preservation of data pursuant to Articles 29 and 30; c the collection of evidence, the provision of legal information, and locating of suspects. 2 a A Party's point of contact shall have the capacity to carry out communications with the point of contact of another Party on an expedited basis. b If the point of contact designated by a Party is not part of that Party's authority or authorities responsible for international mutual assistance or extradition, the point of contact shall ensure that it is able to co-ordinate with such authority or authorities on an expedited basis. 3 Each Party shall ensure that trained and equipped personnel are available, in order to facilitate the operation of the network.	**Cybercrimes Act 2015 Section 56** **Designation of contact point** (1) In order to provide immediate assistance for the purpose of international cooperation under this Act, the Office of the National Security Adviser shall designate and maintain a contact point that shall be available twenty-four hours a day and seven days a week. (2) This contact point can be reached by other contact points in accordance with agreements, treaties or conventions by which Nigeria is bound, or in pursuance of protocols of cooperation with international judicial or law enforcement agencies. (3) The immediate assistance to be provided by the contact point shall include – (a) technical advice to other points of contact; (b) expeditious preservation of evidence in cases of urgency or danger in delay; (c) collection of evidence for which it has the legal jurisdiction in cases of urgency or danger in delay; (d) detection of suspects and provision of legal information in cases of urgency or danger in delay; (e) the immediate transmission of requests concerning the measures referred to in paragraphs (b) and (d) of subsection (3) of this section, with a view to its expedited implementation.
Article 42 – Reservations	

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
By a written notification addressed to the Secretary General of the Council of Europe, any State may, at the time of signature or when depositing its instrument of ratification, acceptance, approval or accession, declare that it avails itself of the reservation(s) provided for in Article 4, paragraph 2, Article 6, paragraph 3, Article 9, paragraph 4, Article 10, paragraph 3, Article 11, paragraph 3, Article 14, paragraph 3, Article 22, paragraph 2, Article 29, paragraph 4, and Article 41, paragraph 1. No other reservation may be made.	

Back to the Table of Contents