AN ACT TO PROVIDE FOR THE PROHIBITION, PREVENTION, DETECTION, RESPONSE AND PROSECUTION OF CYBERCRIME, TO BE KNOWN AS CYBERCRIME ACT 2021

REPUBLIC OF LIBERIA

Contents

ACRONYMS

CBL	Central Bank of Liberia
CNII	Critical National Information Infrastructure
ICT	Information and Communications Technology
LACC	Liberia Anti-Corruption Commission
LCERT	Liberia Cybersecurity Emergency Response Team
LIBTELCO	Liberia Telecommunication Corporation
LNCC	Liberia National Cybersecurity Center
LNP	Liberia National Police
LRA	Liberia Revenue Authority
LTA	Liberia Telecommunication Authority
MoJ	Ministry of Justice
MoPT	Minister of Post and Telecommunications
NDFL	National Digital Forensics Lab
NSA	National Security Advisor

AN ACT TO PROVIDE FOR THE PROHIBITION, PREVENTION, DETECTION, RESPONSE AND PROSECUTION OF CYBERCRIMES, 2021

It is enacted by the Senate and House of Representatives of the Republic of Liberia, in Legislature Assembled:

PART I OBJECTIVES AND DEFINITIONS

1. Objectives.

The objectives of this Act are to:

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

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

(3) Promote cybersecurity and the protection of computer systems and networks, electronic communications; data and computer programs, intellectual property and privacy rights.

2. Definitions.

In this Act, unless the context otherwise requires:

(1) "**Access**" in relation to computer data, means rendering that computer data, by whatever means, in a form that would enable a person, at the time when it is so rendered or subsequently, to take account of that computer data including altering or erasing the computer data, copying or moving it to any computer data storage medium other than in which it is held or to a different location in the computer data storage medium in which it is held, uses it or has it output from the

computer system in which it is held, whether by having it displayed or in any other manner. While "Acquire" on the other hand means to use, examine or capture data or any data output, copy data, or move data to:

(a) a different location in a computer system in which it is held;

(b) any other location; or

(c) divert data from its intended destination to any other destination.

(2) "**Computer program**" means a set of instructions that, when executed in a computer system, causes a computer system to perform functions.

(3) "**Unauthorized access**" - A person accesses computer data held in a computer system or computer data storage medium without authorization if:

(a) the person is not entitled to control access to the program or data in question; and

(b) the person does not have consent to access such program or data from a person who is entitled to give such consent.

(4) "**Unauthorized act**" - A person commits an act in relation to a computer system without authorization if:

(a) the person is not himself a person who has responsibility for the computer and is entitled to determine whether the act may be done; and

(b) does not have consent to the act from any such person.

(5) "**Authorized officer**" means duly authorized officers of any law enforcement agency involved in the prohibition, prevention, elimination or combating of computer crimes and cyber security threats.

(6) **"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.

(7) **"Computer data storage medium**" means any device, physical or virtual, containing or designed to contain, or enabling or designed to enable storage of data, whether available in a single or distributed form for use by a computer.

(8) "**Computer system**" means any device or a group of interconnected or related devices, one or more of which, pursuant to a computer program, performs automatic processing of data.

(9) "**Content data**" means any computer data that conveys essence, substance, information, meaning, purpose, intent, or intelligence, either singularly or when in a combined form, in either its unprocessed or processed form.

(10) **"Critical National Information Infrastructure (CNII)**" means any assets, systems and networks, whether physical or virtual that are so vital to the security , defense or international relations of Liberia; the provisions of service directly related to communications infrastructure, banking and financial services, public utilities, public transportation or public key infrastructure or the protection of public safety including systems related to essential emergency services such as police, civil defense and medical services.

(11) "**Cybersecurity**" means the protection and prevention of damage to, unauthorized use of, or exploitation of, and, if needed, the restoration of electronic information and communications systems and the information contained therein to ensure confidentiality, integrity, and availability.

(12) "**Cyberstalking**" means the crime of using a computer system to stalk, harass, or threaten another person.

(13) **"Damage"** means any impairment to a computer or the integrity or availability of computer data or computer system that:

(a) causes loss aggregating at least One in value, or such other amount as the National Security Adviser may, by notification in the Gazette prescribe, except that any loss incurred or accrued more than one

year after the date of the offence in question shall not be taken in to account;

(b) modifies or impairs, or potentially modifies or impairs the medical examination, diagnosis, treatment or care of one or more persons;

(c) causes or threatens physical injury or death to any person; or

(d) threatens public health or public safety;

(e) the use of the Internet or other electronic means to stalk or harass an individual, a group of individuals, or an organization. It may include false accusations, monitoring, making threats.

(14) "**Device**" means:

(a) physical or virtual device or article;

(b) any electronic or virtual tool that is not in physical form;

(c) any computer program or computer data held in electronic form; and

(d) automated, self-executing, adaptive or autonomous devices, computer programs or computer systems.

(15) "**Function"** includes logic, control, algorithm, deletion, storage, retrieval or communication to, from or within a computer system.

(16) "**Interception**" in relation to a function of a computer system means listening to or recording of computer data or otherwise acquiring the substance, meaning or purport of such.

(17) "**Intimate image**" means a visual depiction of a person made by any means that: (a) under circumstances that give rise to a reasonable expectation of privacy; and (b) in which the person is nude, is exposing his or her genital organs or anal region or, in the case of a female, her breasts.

(18) "**Law enforcement agencies**" - includes any agency for the time being responsible for implementation and enforcement of the provisions of this Act.

(19) "**Minister**" means the Attorney – General of the Republic and Honorable Minister of Justice.

(20) "**Person**" includes an individual, body corporate, organization or group of persons.

(21) "**President**" means the President and Commander–in-Chief of the Armed Forces of the Republic of Liberia.

(22) "**Service provider**" means:

(a) any public or private entity that provides to users of its service the ability to communicate by means of a computer system; and

(b) any other entity that processes or stores computer data on behalf of such communication service or users of such service.

(23) "**Sexually explicit conduct**" includes at least the following real or simulated acts:

(a) sexual intercourse, including genital-genital, oral-genital, analgenital 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.

(24) **"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.

(25) "**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.

(26) **"Transmission of computer data"** means any transfer of signs, signals, writing, images, sounds, data, or intelligence of any nature transmitted in whole or in part by a wire, radio, electromagnetic, photo electronic or photo optical system.

PART II: PROTECTION OF CRITICAL NATIONAL INFORMATION INFRASTRUCTURE

3. Designation of certain computer systems or networks as Critical National Information Infrastructure (CNII).

(1) The President may on the recommendation of the National Security Advisor, by Order published in the Official Gazette, designate certain computer systems, networks and information infrastructure vital to the national security of Liberia or the socio- economic, commercial and social wellbeing of its citizens, as constituting Critical National Information Infrastructure (CNII).

(2) The Presidential Order made under subsection (1) of this section may prescribe minimum standards, guidelines, rules or procedure in respect of:

(a) the protection or preservation of critical information infrastructure;

(b) the general management of critical information infrastructure;

(c) access to, transfer and control of data in any critical information infrastructure;

(d) infrastructural or procedural rules and requirements for securing the integrity and authenticity of data or information contained in any critical national information infrastructure;

(e) the storage or archiving of data or information regarding critical national information infrastructure;

(f) recovery plans in the event of disaster or loss of the critical national information infrastructure or any part thereof; and

(g) any other matter required for the adequate protection, management and control of data and other resources in any critical national information infrastructure.

4. Audit and Inspection of critical national information infrastructure

There shall be a Presidential Order which may require the audit and inspection of any Critical National Information Infrastructure, from time to time, to evaluate compliance with the provisions of this Act.

PART III OFFENCES AND PENALTIES

5. Offences against Critical National Information Infrastructure **(CNII)**

A person commits an offence punishable under this Act if he/she intentionally and without authorization:

(1) Accesses the whole or part of any critical national information infrastructure designated pursuant to section 4 of this Act;

(2) Does an act which causes the serious hindering of the functioning of any critical national information infrastructure by inputting, transmitting, damaging, deleting, deteriorating, altering or suppressing computer data, designated pursuant to section 4 of this Act by any means.

(3) Upon conviction by a court of competent jurisdiction, the offence committed under subsection (2) shall be liable to either imprisonment for a term of not less than three (3) years and/or a fine to be determined by

the court based on the nature of the damage, and the assessed value of the infrastructure.

(4) Where the offence committed under subsection (1) of this section results into serious bodily injury, the offender shall be liable on conviction to imprisonment for a term of not less than five (5) years and/or a fine to be determined by the court in consideration of the extent of bodily injury, the nature of the damage, and the assessed value of the infrastructure.

(5) Where the offence committed under subsection (1) of this section results in death, the offender shall be liable on conviction to a term of imprisonment for life.

6. Unlawful access to a computer system or infrastructure

(1) Any person who without authorization or exceeding authorization, intentionally accesses the whole or in part, a computer system or infrastructure, commits an offence under this Act, and is liable upon conviction to imprisonment for a term not less than two (2) years or a fine in an amount double the gain realized by the defendant; but if such crime has not resulted in gain for the defendant, only sentence of imprisonment without a fine may be imposed;

(2) Any person who intentionally possesses data, with the knowledge that such data was acquired unlawfully as contemplated in this section, is guilty of an offence and is liable upon conviction to imprisonment for a term not less than two (2) years or a fine in an amount double the gain realized by the defendant; but if such crime has not resulted in gain for the defendant, only sentence of imprisonment without a fine may be imposed; and,

(3) Any person who, with the intent to commit an offence under this section, uses any device to avoid detection or otherwise prevent identification with the act or omission, commits an offense and is liable upon conviction to imprisonment for a term of not less than 3 years or not more than five (5) years, a fine in an amount double the gain realized by the defendant; but if such crime has not resulted in gain for the defendant, only sentence of imprisonment without a fine may be imposed.

7. Unlawful interception of communications

Any person, who intentionally and without authorization or in excess of authorization, intercepts by technical means, transmissions of non-public computer data to, from or within a computer system, including electromagnetic emissions or signals from a computer system carrying such computer data, commits an offense and is liable upon conviction to imprisonment for a term of not less than two (2) years or not more than five (5) years, a fine in an amount double the gain realized by the defendant; but if such crime has not resulted in gain for the defendant, only sentence of imprisonment without a fine may be imposed.

8. Unauthorized modification of computer data

(1) Any person who does an unauthorized act which causes the damaging, deletion, deteriorating, alteration, or suppression of computer data commits an offence and is liable upon conviction to imprisonment for a term of not less than three (3) years or to a fine of an amount double the gain realized by the defendant; but if such crime has not resulted in

gain for the defendant, only sentence of imprisonment without a fine may be imposed.

(2) For the purpose of this section, an act in relation to computer data held in any computer system takes place where, by the operation of any function of the computer system concerned any:

(a) computer data held in it is altered or erased; or

(b) computer data is added to or removed from any data held in it.

9. System interference

(1) Any person who without authority or in excess of authority, intentionally does an act which causes the serious hindering of the functioning of a computer system by inputting, transmitting, damaging, deleting, deteriorating, altering or suppressing computer data commits an offence and is liable upon conviction to imprisonment for a term of not less than two (2) years or fine of an amount double the gain realized by the defendant; but if such crime has not resulted in gain for the defendant, only sentence of imprisonment without a fine may be imposed.

(2) For the purpose of this section, an act in relation to a computer system takes place where, by the operation of any function of the computer system concerned, any act occurs which impairs the normal operation of any computer system concerned.

10. Misuse of devices

(1) Any person who unlawfully produces, supplies, or procures for use, imports, exports, distributes, offers for sale or otherwise makes available:

(a) any device including a computer program, or designed or adapted primarily 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, computer system or network is capable of being accessed for the purpose of committing an offence under this Act, or

(c) any device designed primarily to overcome security measures in any computer, computer system or network with the intent that the devices be utilized for the purpose of committing an offence under this Act,

(2) Any person who with intent to commit an offence under this Act, has in his possession any device or computer program referred to in subsection (1) of this section, commits an offence and shall be liable upon conviction to imprisonment for a term of not less than two years or to a fine of an amount double the gain realized by the defendant; but if such crime has not resulted in gain for the defendant, only sentence of imprisonment without a fine may be imposed.

(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 upon conviction to imprisonment for a term of not less than two (2) years or to a fine of an amount double the gain realized by the defendant; but if such crime has not resulted in gain for the defendant, only sentence of imprisonment without a fine may be imposed.

(4) Where the offence under subsection (1) of this section results in substantial loss or damage, the offender shall be liable to imprisonment for a term of not less than five years or to a fine of an amount double the gain realized by the defendant or the damage caused.

(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 upon conviction to imprisonment for a term of not less than five (5) years or to a fine of an amount double the gain realized by the defendant; but if such crime has not resulted in gain for the defendant, only sentence of imprisonment without a fine may be imposed.

11. Computer related forgery

Any person who intentionally accesses any computer system and inputs, alters, deletes or suppresses any computer data resulting in inauthentic data with the intention that such inauthentic data will be considered or acted upon for legal purposes 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 upon conviction to imprisonment for a term of not less than three (3) years or to a fine of an amount double the gain realized by the defendant; but if such crime has not resulted in gain for the defendant, only sentence of imprisonment without a fine may be imposed.

12. Computer related fraud

(1) Any person who intentionally and without authority or in excess of authority causes any loss of property to another by altering, erasing, inputting or suppressing any computer data held in any computer system, or by any interference with the functioning of a computer system, for the purpose of conferring any economic benefits for himself or another person, commits an offence and is liable upon conviction to imprisonment for a term of not less than three (3) years or to a fine of an amount double the gain realized by the defendant; but if such crime has not resulted in gain for the defendant, only sentence of imprisonment without a fine may be imposed.

(2) Any person who with intent to defraud sends electronic message to a recipient, where such 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 upon conviction to imprisonment for a term of not less than three (3) years or to a fine of an amount double the gain realized by the defendant; but if such crime has not resulted in gain for the defendant, only sentence of imprisonment without a fine may be imposed.

13. Identity theft and impersonation

Any person who in the course of using a computer system:

(1) intentionally obtains or possesses another person's or entity's identity information with the intent to deceive or defraud, or

(2) fraudulently impersonates another entity or person, living or dead, with intent to:

(a) gain advantage for himself or another person;

(b) obtain any property or an interest in any property;

(c) cause disadvantage to the entity or person being impersonated or another person; or

(d) avoid arrest or prosecution or to obstruct, pervert or defeat the course of justice,

commits an offence and is liable upon conviction to imprisonment for a term of not less than three (3) years or a fine of an amount double the gain realized by the defendant; but if such crime has not resulted in gain for the defendant, only sentence of imprisonment without a fine may be imposed.

14. Child pornography and related offences

(1) Any person who intentionally uses any computer system in or for:

(a) producing child pornography for the purpose of its distribution;

(b) offering or making available child pornography;

(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 is liable upon trial and conviction:

i. in the case of paragraphs (a), (b) and (c) to imprisonment for a term of three years or a fine of an amount double the gain realized by the defendant; but if such crime has not resulted in gain for the defendant, only sentence of imprisonment without a fine may be imposed, and

ii. in the case of paragraphs (d) and (e) of this subsection, to imprisonment for a term of not less than three (3) years or a fine of an amount double the gain realized by the defendant; but if such crime has not resulted in gain for the defendant, only sentence of imprisonment without a fine may be imposed.

(2) Any person who, intentionally proposes, grooms or solicits, through computer system, to meet a child, followed by material acts leading to such a meeting for the purpose of:

(a) engaging in sexual activities with a child;

(b) engaging in sexual activities with a 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;

(c) recruiting, inducing, coercing, 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 is liable upon conviction:

i. in the case of paragraphs (a) and (b) to imprisonment for a term of not more than Ten (10) years or a fine of an amount double the gain realized by the defendant; but if such crime has not resulted in gain for the defendant, only sentence of imprisonment without a fine may be imposed; and

ii. in the case of paragraph (c) of this subsection, to imprisonment for a term of not less than five (5) years or a fine of an amount double the gain realized by the defendant; but if such crime has not resulted in gain for the defendant, only sentence of imprisonment without a fine shall be imposed.

(3) 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.

(4) For the purpose of this section, the term "child" or "minor" shall include a person below Eighteen (18) years of age.

15. Cyberstalking

(1) Any person who, through a computer system, transmits or causes the transmission of any computer data:

(a) with intent to bully, threaten or harass another person, where such communication places another person in fear of death, violence or personal bodily injury or to another person; or

(b) containing any threat to kidnap any person or any threat to injure the person of another, any demand or request for a ransom for the release of any kidnapped person, with intent to extort from any person, firm, association or corporation, any money or other thing of value;

commits an offence under this Act and is liable upon conviction to imprisonment for a term of not more than three (3) years or a fine of an amount double the gain realized by the defendant; but if such crime has not resulted in gain for the defendant, only sentence of imprisonment without a fine shall be imposed.

(2) A court sentencing or otherwise dealing with a person convicted of an offence under subsections (1) may (as well as sentencing him or dealing with him in any other way) make an order for the purpose of protecting the victim or victims of the offence, or any other person mentioned in the order, from further conduct which:

(a) amounts to harassment, or

(b) will cause a fear of violence, death or bodily injury; prohibit the defendant from doing anything described/specified in the order.

(3) A defendant who does anything which he is prohibited from doing by an order under this section, commits an offence under this section and shall be liable upon conviction to imprisonment for a term of not more than one (1) year or a fine of an amount double the gain realized by the defendant; but if such crime has not resulted in gain for the defendant, only sentence of imprisonment without a fine shall be imposed.

(4) The order made under subsection (2) of this section may have effect for a specified period or until further order and the defendant or any other person mentioned in the order may apply to the court, which made the order for it to be varied or discharged by a further order.

16. Cyberterrorism

(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 upon conviction to life imprisonment.

(2) For the purposes of this section, "terrorism" shall have the same meaning under the Act to amend Chapters 14 and 15 Subchapter (C), Title 26 of the Liberian Code of Laws Revised, known as the New Penal Law of 1976 making the crimes of armed robbery, terrorism and hijacking capital offences, approved July 22, 2008, as amended.

17. Racist and xenophobic offences

(1) Any person who:

(a) distributes or otherwise makes available, any racist and xenophobic material to the public through a computer system or network,

(b) threatens, through a computer system or network, with the commission of a criminal offence:

i. persons for the reason that they belong to a group, distinguished by race, color, descent, national or ethnic origin, as well as, religion, if used as a pretext for any of these factors, or

ii. a group of persons which is distinguished by any of these characteristics;

(c) insults publicly, through a computer system or network:

i. persons for the reason that they belong to a group distinguished by race, color, descent or national or ethnic origin, as well as religion, if used as a pretext for any of these factors; or

ii. a group of persons which is distinguished by any of these characteristics; or

iii. distributes or otherwise makes available, through a computer system to the public, material which denies, approves or justifies acts constituting genocide or crimes against humanity, as defined under the Rome Statute of the International Criminal Court, 1998; commits an offence and shall be liable upon conviction to imprisonment for a term of not less than five (5) years or to a fine of an amount double the gain realized by the defendant; but if such crime has not resulted in gain for the defendant, only sentence of imprisonment without a fine shall be imposed.

(2) For the purpose of subsection (1) of this section, the term "racist and xenophobic material" means any written or printed material, any image

or any other representation of ideas or theories, which advocates, promotes or incites hatred, discrimination or violence, against any individual or group of individuals, based on race, color, descent or national or ethnic origin, as well as religion if used as a pretext for any of these factors.

18. Distribution of data message(s) that incites damage to property or violence

(1) Any person who makes available, transmits or distributes, by means of a computer system, a data message to a specific person, group of persons or the general public with the intention to incite:

(a) the causing of any damage to any property belonging to; or

(b) violence against, a person or a group of persons:

commits an offence and shall be liable upon conviction to imprisonment for a term of not more than one (1) year or to a fine of an amount double the gain realized by the defendant; but if such crime has not resulted in gain for the defendant, only sentence of imprisonment without a fine may be imposed.

19. Distribution of harmful data message(s)

(1) Any person, who unlawfully and intentionally makes available, transmits or distributes, by means of a computer system, a data message that is harmful, is guilty of an offence.

(2) For purposes of subsection (1), a data message is considered harmful when:

(a) it threatens a person with:

i. damage to any property belonging to, or violence against, that person; or

ii. damage to any property belonging to, or violence against, any member of the family or household of the person or any other person in a close relationship with the person;

(b) it threatens a group of persons with damage to any property belonging to, or violence against, the group of persons or any identified person forming part of the group of persons or who is associated with the group of persons;

(c) it intimidates, encourages or harasses a person to harm himself or herself or any other person; or

(d) it is inherently false in nature and it is aimed at causing mental, psychological, physical or economic harm to a specific person or a group of persons, and a reasonable person in possession of the same information and with regard to all the circumstances would regard the data message as harmful.

(3) Individuals, under this section, shall be liable upon conviction to imprisonment for a term of not more than three (3) years or to a fine of an amount double the gain realized by the defendant; but if such crime has not resulted in gain for the defendant, only sentence of imprisonment without a fine shall be imposed.

20. Distribution of data message(s) of intimate image without **consent**

Any person, who unlawfully, intentionally makes available, transmits or distributes, by means of a computer system, an intimate image of an identifiable person knowing that the person depicted in the intimate image did not give his or her consent to the making available, broadcasting or distribution of the data message, is guilty of an offence and shall be liable upon conviction to imprisonment for a term of not more than three (3) years or to a fine of an amount double the gain realized by the defendant; but if such crime has not resulted in gain for the defendant, only sentence of imprisonment without a fine may be imposed.

21. Order to protect complainants pending finalization of criminal proceedings

(1) A complainant who lays a charge with the Liberia National Police (LNP) that an offence contemplated in sections 18, 19 or 20 has allegedly been committed against them, may on an *ex parte* basis in the prescribed form and manner, make an application to a court of competent jurisdiction pending the finalization of the criminal proceedings to:

(a) prohibit any person(s) from further making available, broadcasting or distributing the data message contemplated in sections 18, 19 or 20 which relates to the charge; or

(b) order an electronic communications service provider or person in control of a computer system to remove or disable access to the data message in question.

(2) The court may, as soon as is reasonably possible, consider an application submitted to it in terms of subsection (1) and may, for that purpose, consider any additional evidence it deems fit, including oral evidence or evidence by affidavit, which must form part of the record of proceedings.

(3) If the court is satisfied that there is prima facie evidence that the data message in question constitutes an offence as contemplated in sections 18, 19 or 20 , the court shall issue the order referred to in subsection (1), in the prescribed form.

(4) The order must be served on the person referred to in subsection (1) (a) or electronic communications service provider or person referred to in subsection (1) (b) in the prescribed form and manner: Provided that, if the court is satisfied that the order cannot be served in the prescribed form and manner, the court may make an order allowing service to be effected in the manner as specified by law.

(5) An order referred to in subsection (1) is of force and effect from the time it is issued by the court and the existence thereof has been brought to the attention of the person referred to in subsection (1) (a) or electronic communications service provider or person referred to in subsection (1) (b).

(6) A person referred to in subsection (1) (a) or electronic communications service provider or person referred to in subsection (1) (b) may, within 10 days after the order has been served on him or her in terms of subsection (5), upon notice to the appropriate court of competent jurisdiction, in the prescribed form and manner, apply to the court for the setting aside or amendment of the order referred to in subsection (1).

(7) The court must as soon as is reasonably possible consider an application submitted to it in terms of subsection (6) and may for that purpose, consider such additional evidence as it deems fit, including oral evidence

or evidence by affidavit, which shall form part of the record of the proceedings.

(8) The court may, for purposes of subsections (2) and (7), in the prescribed manner cause to be subpoenaed any person as a witness at those proceedings or to provide any book, document or object, if the evidence of that person or book, document or object appears to the court essential to the just determination of the case.

(9) Any person or electronic communications service provider who fails to comply with an order referred to in subsection (4) will be held in contempt of court.

(10) Any person who is subpoenaed in terms of subsection (8) to attend proceedings and who fails to:

(a) attend or to remain in attendance;

(b) appear at the place and on the date and at the time to which the proceedings in question may be adjourned;

(c) remain in attendance at those proceedings as so adjourned; or

(d) produce any book, document or object specified in the subpoena, will be held in contempt.

(11) The provisions in respect of appeal and review as provided for according to Criminal Procedure Law, apply to proceedings in terms of this section.

22. Attempt, conspiracy, aiding and abetting

(1) Any person who attempts to commit any offence under this Act:

(a) does any act preparatory to; or

(b) in furtherance of the commission of an offence under this Act; or

(c) abets, aids or conspires to commit any offence under this Act,

commits an offence and is liable upon conviction to the punishment provided for the principal offence under this Act.

23. Corporate liability

(1) A body corporate that commits an offence under this Act shall be liable upon conviction to a fine of an amount double the gain realized and any person who at the time of the commission of the offence was a chief executive officer, director, secretary, manager or other similar officer of the body corporate or was purporting to act in any such capacity shall be liable upon conviction to imprisonment for a term of not less than two (2) years or a fine of an amount double the gain realized by the defendant; but if such crime has not resulted in gain for the defendant, only sentence of imprisonment without a fine shall be imposed.;

(2) Nothing contained in this section shall render any person liable to any punishment where he proves that the offence was committed without his knowledge and that he exercised all due diligence to prevent the commission of the offence.

PART IV PROCEDURAL LAW

24. Expedited preservation of stored computer data

(1) Any natural or legal person, including the service provider, shall at the order of Ministry of Justice or any law enforcement agency, preserve any computer data, including traffic data, subscriber information and communication content data, which is in its possession or control. The order shall indicate:

(a) data to be preserved;

(b) their origin and destination, if known; and

(c) the period of time over which data must be preserved.

(2) Any person who receives the order under subsection 1 of this section shall immediately preserve the data by protecting and maintaining its integrity and safeguarding the data against any possible loss or modification.

(3) Recipient of the order referred to in subsection 1 shall preserve data for a period specified in the order, up to a maximum of ninety (90) days, which can be subsequently renewed.

(4) Recipient of the order referred to in subsection 1 shall keep confidential all the facts pertaining to the order and its execution, during the whole period of its validity.

(5) Recipient of the order referred to in subsection 1 as well as anyone exercising any function under this Act shall take appropriate measures to safeguard the confidentiality of the preserved data and shall not disclose them to any third person, except pursuant to valid order issued on the basis of this Act or other applicable legislation.

25. Expedited preservation and partial disclosure of traffic data

Any service provider to whom the preservation order under section 26 has been served shall expeditiously disclose to the law enforcement agency which issued the order sufficient information about other service providers through which the communication was carried out, in order to identify all service providers involved in that communication.

26. Production order

(1) Where it is reasonably required for the purposes of a criminal investigation or proceedings, it shall be the duty of every natural or legal person in Liberia, including service provider, to submit, upon written and reasoned order of a Judge:

(a) specified computer data in that person's possession or control, which is stored in a computer system or a computer-data storage medium, or

(b) subscriber information relating to services in service provider's possession or control.

(2) Order specified in subsection 1 can be issued upon reasoned and written request of Ministry of Justice or any law enforcement agency.

(3) Any natural person who contravenes the provisions of subsection (1) of this section commits an offence and shall be liable upon conviction to imprisonment for a term not to exceed one (1) year or a fine to be determined by a court of competent jurisdiction based on the circumstances.

(4) Any legal person, including service provider, who contravenes the provisions of subsection (1) of this section, commits an offence and shall be liable upon conviction to a fine to be determined by a court of competent jurisdiction based on the circumstances.

(5) In addition to the punishment prescribed under subsection (3) of this section and subject to the provisions of section 20 of this Act, each director, manager or officer of the service provider shall be liable upon conviction to imprisonment for a term not to exceed one (1) year or a fine to be determined by a court of competent jurisdiction based on the circumstances.

27. Power to conduct search, seizure and arrest

(1) The Ministry of Justice (MoJ) may apply ex-parte to the court of competent jurisdiction for the issuance of a warrant for the purposes of search and arrest.

(2) The court may issue a warrant authorizing the Ministry to:

(a) enter and search any premises or place specified in the warrant;

(b) search any person or conveyance found on any premises or place empowered to enter and search under paragraph (a) of this subsection;

(c) stop, board and search any conveyance;

(d) seize, remove and detain anything, including computer or electronic device and relevant material found therein, which is, or contains or appears to the Ministry of Justice to be or to contain evidence of the commission of an offence under this Act; or

(e) use or cause to use a computer or any device to search any data contained in or available from 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; or

(h) arrest, search and detain any person whom the Ministry of Justice reasonably suspects of having committed or likely to commit an offence under this Act.

(3) The court shall not issue a warrant under subsection (2) of this section unless the court is satisfied that:

(a) the warrant is sought to prevent the commission of an offence under this Act; or

(b) the warrant is sought to prevent the interference with investigative process under this Act; or

(c) the warrant is required to find the perpetrator of a criminal offence, objects or evidence important for the criminal proceedings, when it is probable that these may be found in certain premises; or

(d) the person named in the warrant is preparing to commit an offence under this Act.

(4) Where a seizure of computer data is effected in the course of search or investigation under this Act, the law enforcement authorities shall have the competence 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.

(5) Where a seizure is effected in the course of search or investigation under this Act, a copy of the list of all the items, documents and other materials seized shall be made, duly endorsed and handed to the:

(a) person on whom the search is made; or

(b) owner of the premises, place or conveyance seized.

(6) Notwithstanding other provisions of this section, a woman shall only be searched by a woman.

(7) Nothing in this section shall be construed as derogating from the lawful right of any person in defense of his person or property.

(8) A duly authorized law enforcement officer acting under the instructions of the Minister, who uses such force as may be reasonably necessary for any purpose in accordance with this Act, shall not be liable in any criminal or civil proceedings, for having, by the use of reasonable force caused injury or death to any person, damage to, or loss of any property.

28. Powers to conduct investigation or search without warrant

(1) Where in a case of verifiable urgency an application to the court or to Judge in Chambers to obtain a warrant would cause delay and:

(a) a cybercrime or computer related offences is threatened, or

(b) there is the urgent need to prevent the commission of an offence provided under this Act, or

(c) there is grave danger that evidence reasonably required for the purposes of a criminal investigation or proceedings might be destroyed, the Ministry of Justice may, with the assistance of such other authorized officers as may be necessary and while search warrant is being sought for, initiate measure defined in Section 33 of this Act without court order.

(2) When it acts on the basis of subsection 1 of this section, the Ministry of Justice shall immediately inform the court of competent jurisdiction of its actions and shall request issuance of an order under Section 33 of this Act. The court is required to rule on the request within 24 hours. If the

court denies the request, all materials seized in the process shall be returned to its holder immediately.

29. Interception of electronic communications

(1) Where the criminal investigation or proceedings could not be carried out otherwise, a Judge may, upon the reasoned and written request of the Minister, order interception of communications against:

(a) the person for whom there are grounds for suspicion that he committed or has taken part in committing an offence punishable by imprisonment of not more than five (5) years, or

(b) against the person for whom there are grounds for suspicion that he delivers to the person in subsection (1)a above information and messages in relation to offences, or that the person in subsection (1)a uses their communication devices, or that they hide that person, or help him from being discovered by hiding the means by which the criminal offence was committed, traces of the criminal offences or objects resulting or acquired through the criminal offence.

(2) As an exception from subsection 1 of this section, when circumstances require that the delay in execution of interception would seriously compromise investigation or proceedings, the order from subsection 1 of this section may be issued by a written and reasoned order of the Minister himself. The Minister must deliver the order with a note on the time of issue and a statement of reasons to the Judge within eight (8) hours, and the Judge is required to rule on the legality of the order immediately. If the Judge accepts the order of the Minister, he shall proceed pursuant to subsection 1 of this section. If the Judge denies the order, Minister shall deliver all the material collected during the application of the measure to the Judge, after which the Judge shall ensure its immediate deletion.

(3) The order referred to in subsections 1 and 2 of this section shall state the available data on the person against whom the interception is to be applied, the facts justifying the necessity for interception of communications and the term for their duration.

(4) Interception of communications may last up to ninety (90) days. Upon the motion of the Minister the Judge shall, on account of important

reasons, prolong the duration of such measures for a term of another ninety (90) days.

(5) Service provider to whom the order from subsection 1 or 2 is delivered shall:

(a) through the application of technical means collect, record, permit or assist competent authorities with the collection or recording of content data associated of specified communications transmitted by means of a computer system; or

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

(6) As soon as the conditions referred to in subsection 1 of this section cease to exist, the Judge shall order interception to be discontinued.

(7) Any information unrelated to the investigation or proceeding which might be obtained on the basis of this section shall be deleted immediately.

(8) Upon the expiration of the order from this section, the Judge shall inform the person(s) against whom the interception was applied about the issuance of the order, its purpose and time frame.

30. Failure of service provider to perform certain duties

(1) In addition to other obligations under this Act, any service provider in Liberia shall, on the basis of valid order under this or other legislation, enable:

(a) the identification, tracking and tracing of proceeds of any offence or any property, equipment or device used in the commission of any offence; or

(b) the freezing, removal, erasure or cancellation of the services of the offender which enables the offender to either commit the offence or hide or preserve the proceeds of any offence or any property, equipment or device used in the commission of the offence.

(2) Any service provider who contravenes the provisions of subsection (1) of this section, commits an offence and shall be liable upon conviction to a

fine to be determined by a court of competent jurisdiction based on the circumstances.

(3) In addition to the punishment prescribed under subsection (2) of this section and subject to the provisions of section 20 of this Act, each director, manager or officer of the service provider shall be liable upon conviction to imprisonment for a term of not longer than one (1) year or a fine to be determined by a court of competent jurisdiction based on the totality of the circumstances.

31. Obstruction and refusal to release information

(1) Any person who:

(a) willfully obstructs any authorized law enforcement officer in the exercise of any powers conferred by this Act; or

(b) fails to comply with any lawful inquiry or requests made by an authorized law enforcement agency in accordance with the provisions of this Act, commits an offence.

(2) Unless other penalties under this Act apply, such person shall be liable upon conviction to imprisonment for a term of not more than one (1) year or to a fine of an amount double the gain realized by the defendant; but if such crime has not resulted in gain for the defendant, only sentence of imprisonment without a fine may be imposed.

32. Prosecution of offences

The Attorney-General of the Republic shall prosecute offences under this Act subject to the provisions of the Constitution of the Republic of Liberia, 1986.

33. **Order of forfeiture of assets**

(1) The Court of competent jurisdiction in imposing sentence on any person convicted of an offence under this Act, may order that the convicted person forfeits to the Government of the Republic of Liberia:

(a) any asset, money or property, whether tangible or intangible, constituting or traceable to proceeds of such offence; and

(b) any computer, equipment, software or electronic device and other technological device used or intended to be used to commit or to facilitate the commission of such offence.

(2) Where it is established that a convicted person has assets or properties in a foreign country, acquired as a result of such criminal activities listed in this Act, such assets or properties, shall subject to any Treaty or arrangement with such foreign country, be forfeited to the Government of Liberia.

(3) The office of the Attorney-General of the Republic shall ensure that the forfeited assets or properties are effectively transferred and vested in the Government of Liberia.

34. Order for payment of compensation or restitution

Without prejudice to section 33 of this Act, the Court in imposing sentence on any person convicted under this Act may make an Order requiring the convicted person to pay, in addition to any penalty imposed on him under this Act, monetary compensation to any person or entity for any damage, injury or loss caused to his computer, computer system or network, program or data or to recover any money lost or expended by such person or entity as a result of the offence being convicted for.

PART V ADMINISTRATION AND ENFORCEMENT

35. Establishment of the Liberia National Cybersecurity Center (LNCC) and the Liberia Cybersecurity Emergency Response Team (LCERT) as its technical group of experts

(1) There is established, the Liberia National Cybersecurity Center and the Liberia Cybersecurity Emergency Response Team (in this Act referred to as "LCERT"). The LNCC shall comprise of a representative each of the Ministries and Agencies listed in the Schedule to this Act.

(2) A representative appointed pursuant to subsection (1) of this section shall be an officer not below the Director level in the Civil Service Agency classification or its equivalent.

(3) The LCERT shall create an enabling environment for members to share knowledge, experience, intelligence and information on a regular basis and shall provide recommendations on issues relating to the prevention, protection and combating of cybercrimes; and the promotion of cybersecurity in Liberia.

(4) There is established a Board of the LNCC which shall comprise of a representative from each of the following Ministries and Agencies as indicated in the Schedule to this Act.

(5) A member of the LNCC Board shall cease to hold office if:

a) he ceases to hold the office on the basis of which he became a member of the LNCC Board; or

b) the President is satisfied that it is not in the public interest for the person to continue in office as a member of the LNCC Board.

(6) The meetings of the LNCC Board shall be presided over by the Chair of the Board.

(7) The LNCC Board shall meet quarterly each year and whenever the Minister of Post and Telecommunications as Chair convenes it.

36. **Funding**

The LNCC shall be funded through the following mechanisms:

(1) The LNCC shall submit its annual Budget to the Ministry of Posts and Telecommunications which shall form part of the Ministry's National Budget.

(2) Universal Access Fund; the universal fund Manager shall provide a budgetary support to the LNCC amounting to 10% of its (LNCC) annual budget.

(3) Donors/Partners; The Ministry of Post and Telecommunications shall engage donor partners to consider support to the LNCC operations.

(4) The Liberia Telecommunication Authority (LTA) shall provide a budgetary support to the LNCC amounting to 5% of its (LNCC) annual budget.

(5) The Liberia Telecommunication Corporation (LIBTELCO) shall provide a budgetary support to the LNCC amounting to 5% of its (LNCC) annual budget.

37. Co-ordination and enforcement

(1) The Minister of Post and Telecommunications (MoPT) shall have direct responsibility for the Liberia National Cybersecurity Center and shall chair its board in coordination with the Minister of Justice, being the cocoordinating body for all security and enforcement agencies serving as Co-Chair under this Act and shall:

(a) provide support to all relevant security, intelligence, law enforcement agencies and military services and the general business community to prevent and combat cybercrimes in Liberia;

(b) ensure the effective formulation and implementation of a comprehensive cybersecurity strategy for Liberia;

(c) 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 Liberia; and

(d) 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 Minister of Justice and Attorney General of the Republic (in this Act referred to as "Minister") shall be the Co-Minister for the effective implementation and administration of this Act; and shall strengthen and enhance the existing legal framework to ensure:

(a) conformity of Liberia's cybercrime and cybersecurity laws and policies with international standards and the African Union Conventions on Cybersecurity;

(b) maintaining international co-operation required for preventing and combating cybercrimes and promoting cybersecurity; and

(c) effective prosecution of cybercrimes and cybersecurity matters.

(3) All agencies of the Government of Liberia and legal entities serving as service providers shall develop requisite institutional capacity for the effective implementation of all provisions of this Act and shall in collaboration with the Liberia National Cybersecurity Center, initiate, develop and organize training programs nationally or internationally for officers charged with the responsibility for the prohibition, prevention, detection, investigation and prosecution of cybercrimes within Liberia.

38. Functions and powers of the LCERT

(1) The LCERT shall be responsible to:

(a) Identify – Develop the organizational capacity to identify, understand and manage cybersecurity risks to national computer infrastructure, assets, data, and capabilities;

(b) Protect – Develop and implement the appropriate safeguards to ensure protection of critical national infrastructure and ensure continued delivery of critical infrastructure services;

(c) Detect – Develop and implement the appropriate activities and protocols to detect and identify the occurrence of a cybersecurity event or threat;

(d) Respond – Develop and implement the appropriate activities and protocols to take responsive action regarding a detected cybersecurity event or threat;

(e) Recover – Develop and implement the appropriate activities and protocols to ensure implementation of plans for system resilience, recovery and restoration of any capabilities or services impaired due to a cybersecurity event.

(2) The LCERT shall also:

(a) create an enabling environment for the sharing amongst members of knowledge, experience, intelligence and information on a regular basis and shall provide recommendations on issues relating to the prevention and combating of cybercrimes and the promotion of cyber security in Liberia;

(b) formulate and provide general policy guidelines for the implementation of the provisions of this Act;

(c) advise on measures to prevent and combat computer related offences, cybercrimes, threats to national cyberspace and other cyber security related issues.

(3) The LNCC is authorized through its technical group (LCERT) to address all types of computer security incidents, or threats of such incidents within Liberia, and which require cross-organizational coordination.

(4) The level of support given by LCERT to computer security incidents will vary depending on the type and severity of the incident or issue, the type of constituent, the size of the user community affected, and LCERT's resources at the time. Special attention will be given to issues affecting critical national information infrastructure.

PART VI JURISDICTION AND INTERNATIONAL CO-OPERATION

39. Jurisdiction

(1) The Court of competent jurisdiction located in any part of Liberia, regardless of the location where the offence is committed, shall have jurisdiction to try offences under this Act committed:

(a) in Liberia; or

(b) on a ship or aircraft registered in Liberia; or

(c) by a Liberian outside Liberia if the person's conduct would also constitute an offence under a law of the country where the offence was committed; or

(d) outside Liberia, where:

i. the victim of the offence is a citizen or resident of Liberia; or

ii. the alleged offender is in Liberia and not extradited to any other country for prosecution.

40. Extradition

Offences under this Act shall be extraditable offences under the Extradition Treaties signed by the Republic of Liberia.

41. Request for mutual assistance

(1) The Minister or designated competent authority 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 Liberia and the requested or requesting country.

(3) The Minister or prosecuting attorney 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 apprehension of an offender or investigation of any offence under this Act.

42. Evidence pursuant to a request

(1) Any evidence gathered, pursuant to a request under this Act, in any proceedings in the court of any foreign State may, if authenticated, is prima facie admissible in any proceedings to which this Act applies.

(2) For the purpose of subsection (1) of this section, a document is authenticated if it is:

(a) certified by a Judge or Magistrate or Notary Public of the foreign State; and

(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.

43. Form of request

(1) A request under this Act shall be in writing, dated and signed by or on behalf of the person making the request.

(2) A request may be transmitted by facsimile or by any other electronic device or means; and Shall:

(a) confirm either that an investigation or prosecution is being conducted in respect of a suspected offence related to computer crimes and cybersecurity or that a person has been convicted of an offence related to cybercrimes and cybersecurity;

(b) state the grounds on which any person is being investigated or prosecuted for an offence related to computer crimes and cybersecurity or details of the conviction of the person; give sufficient particulars of the identity of the person;

(c) give sufficient particulars to identify any financial institution or designated non – financial institution or other persons believed to have information, documents or materials which may be of assistance to the investigation or prosecution;

(d) specify the manner in which and to whom any information, document or material obtained pursuant to the request is to be produced;

(e) state whether:

i. a forfeiture Order is required, or ii. the property

may be made the subject of such an Order.

(f) contain such other information as may assist in the execution of the request.

(3) A request shall not be invalidated for the purposes of this Act or any legal proceedings by failure to comply with the provision of subsection (2) of this section where the Attorney-General of the Republic is satisfied that there is sufficient compliance to enable him execute the request.

(4) Where the Attorney-General of the Republic considers it appropriate because an international arrangement so requires or it is in the public interest, he shall order that the whole or any part of any property forfeited under this Act or the value thereof, be returned or remitted to the requesting State.

44. Expedited Preservation of computer data

(1) Liberia may undertake expeditious preservation of data stored in a computer system or network, referring to crimes described under this Act or any other enactment, on the basis of request from foreign State to preserve and / or disclose certain computer 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 computer data to be retained and its relation to the offence;

(d) all the available information to identify the person responsible for the 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 and upon a court order, the Minister or other law enforcement agency, including contact point designated under Section 45, shall proceed pursuant to sections 26 of this Act.

(4) A request for expedited preservation of computer 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 data shall be denied.

45. Designation of contact point

(1) In order to provide immediate assistance for the purpose of international cooperation under this Act, the Minister of Post and Telecommunications and Chair of the LNCC in consultation the Co-Chair (Attorney General of Liberia) shall designate and maintain a contact point that shall be available twenty-four hours a day and seven days a week by or through a permanently designated phone number and email.

(2) This contact point can be contacted by other contact points in accordance with agreements, treaties or conventions to which Liberia 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 data 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 providing 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 this subsection, with a view to its expedited implementation.

PART VII MISCELLANEOUS

46. Directives of a general character

The President may issue to any agency responsible for implementing or enforcing any provisions of this Act, any directive of a general character or relating to particular matter with regard to the exercise by that agency of its functions and it shall be the duty of that agency to comply with the directive.

47. Regulations

(1) The Minister may make orders, rules, guidelines or regulations as are necessary for the efficient implementation of the provisions of this Act.

(2) Orders, rules, guidelines or regulations made under subsection (1) of this section may provide for the:

a) method of custody of video and other electronic recordings of suspects apprehended under this Act;

b) method of compliance with directives issued by relevant international institutions cybersecurity and cybercrimes;

c) procedure for freezing, unfreezing and providing access to frozen funds or other assets;

d) procedure for attachments, forfeiture and disposal of assets,

e) mutual legal assistance,

f) procedure for the prosecution of all cybercrime cases in line with national and international human rights standards; and

g) any other matter the Minister may consider necessary or expedient for the purpose of the implementation of this Act.

48. Short title

This Act may be cited as the **Cybercrime Act, 2021**.

SCHEDULE

MEMBERS OF THE LIBERIA NATIONAL CYBERSECURITY CENTER (LNCC)

Liberia National Cybersecurity Center Board.

(1) The LNCC shall comprise of a representative each of the following Ministries, Departments and Agencies:

(a) The Minister of Post and Telecommunications shall serve as Chair of the Board;

(b) Ministry of Justice shall Co-Chair the Board and shall in keeping with Section 37 Subsection 2, the Ministry of Justice will implement this Act and coordinate the activities of the Liberia National Police and the Bureau of Immigration & Naturalization and all other law enforcement agencies in search and seizure activities;

(c) Ministry of Foreign Affairs: the Ministry of Foreign Affairs will provide support in the matters of international cooperation, intellectual property concerns and extradition requests;

(d) Ministry of National Defense: the Ministry of Defense will provide support regarding issues of national defense;

(e) Liberia Telecommunications Authority (LTA): the Liberia Telecommunications Authority will provide regulatory support;

(f) Central Bank of Liberia (CBL): the Central Bank of Liberia will provide support regarding financial transactions and ;

(g) National Security Advisor: in keeping with Section 28 Subsection 1, the National Security Advisor shall be the co-coordinating body for all security and enforcement agencies under this Act;

(h) National Security Agency (NSA): the National Security Agency shall provide support regarding issues of national security;

(i) Liberia Anti-Corruption Commission (LACC): the Liberia AntiCorruption Commission shall provide support regarding issues of corruption; and,

(j) Liberia Revenue Authority (LRA): the Liberia Revenue Authority shall provide support regarding issues of customs and tax fraud;

(k) The office of the National Security Advisor to the President of the Republic of Liberia;

(l) The Ministry of Finance and Development Planning will provide support regarding the financial sector;

(m) Liberia Chamber of Commerce; shall serve as support directly

i. from the business/private sector

1) The Board shall also comprise of a representative of any other Ministry, Agency or Institution which the Minister may by notice published in the Official Gazette add to the list under paragraph 1 of this Schedule.

EXPLANATORY MEMORANDUM

(This Memorandum does not form part of the above Act but is intended to explain its purport)

The Act seeks to provide an effective, unified and comprehensive legal, regulatory and institutional framework for the prohibition, prevention, detection, prosecution and punishment of cybercrimes in Liberia; ensure the protection of critical national information infrastructure; and promote cybersecurity and the protection of computer systems and networks, electronic communications; data and computer programs, intellectual property and privacy rights.