

# ACT

## THE CYBER SECURITY AND CRIME ACT, 2021

### ARRANGEMENT OF SECTIONS

#### PART I—PRELIMINARY

##### Section

1. Interpretation.

#### PART II—ADMINISTRATION AND COORDINATION

2. Establishment of the National Computer Security Incidence Response Coordination Center.
3. Functions and Powers of the Center
4. Establishment of the National Cybersecurity Advisory Council.
5. Functions and Powers of the Council.
6. Establishment of National Cyber Security Fund.

#### PART III—CRITICAL NATIONAL INFORMATION INFRASTRUCTURE

7. Designation of Critical National Information Infrastructure.
8. Audit and Inspection of Critical National Information Infrastructure.

#### PART IV—POWERS AND PROCEDURES

9. Scope of Powers and Procedures.
10. Search and Seizure of Stored Computer data.
11. Record of and Access to Seized Data.
12. Production Order.
13. Expedited Preservation and Partial Disclosure of Traffic Data.

41. Computer fraud.
42. Identity theft and impersonation.
43. Electronic signature.
44. Cyber stalking and bullying.
45. Cyber Squatting.
46. Infringement of copyright and related rights.
47. Online child sexual abuse.
48. Online adult sexual abuse.
49. Attempting and Aiding or Abetting.
50. Registration of cyber cafes.
51. Cyber Terrorism.
52. Racist Xenophobic Offences.
53. Reporting cyber threats.
54. Breach of confidence by service provider.
55. Employees responsibility.
56. Corporate liability.
57. Acts by children.

PART VII–MISCELLANEOUS PROVISION.

58. Regulations.

DR. JULIUS MAADA BIO,  
*President.*



No.



2021

**The Cyber Security and Crime Act, 2021.**

Short title.

**Being an Act to provide for the effective, unified and comprehensive legal, regulatory and institutional framework for the prohibition, prevention, detection, prosecution and punishment of cybercrimes; prevention of the abusive use of computer systems; to provide for the establishment of structures to promote cybersecurity and capacity building; to provide for the timely and effective collection of electronic evidence for the purpose of investigation and prosecution of cybercrime; to provide for the protection of Critical National Information Infrastructure and the protection of computer systems and networks, electronic communications, data and computer programs, intellectual property and privacy rights to provide for facilitation of international cooperation in dealing with cybercrime matters and to provide for other related matters.**

[ ]

ENACTED by the President and Members of Parliament in this present Parliament assembled. Date of commencement.

"crime against humanity" includes any of the following acts committed as part of a widespread or systematic attack directed against any civilian population, with knowledge of the attack: murders, extermination, enslavement, deportation or forcible transfer of population, imprisonment, torture rape, sexual slavery, enforced prostitution, forced pregnancy, enforced sterilisation or any other form of sexual violence of comparable gravity, persecution against an identifiable group on political, racial, national, ethnic, cultural, religious or gender grounds, enforced disappearance of persons, the crime of apartheid, other inhumane acts of similar character intentionally causing great suffering or serious bodily or mental injury;

"Critical National Information Infrastructure" means computer systems that are necessary for the continuous delivery of essential services that Sierra Leone relies on, the loss or compromise of which will lead to a debilitating impact on-

- (a) the security, defence or international relations of Sierra Leone;
- (b) the existence or identity of a confidential source of information relating to the enforcement of the criminal law;
- (c) the provision of services directly related to communications, infrastructure, banking and financial services, public utilities, public transportation or public key infrastructure; or
- (d) the protection of public safety including system related to essential emergency services;

---

service (SMS), e-mail, video, voice mails, multimedia message service (MMS), Fax, and pager;

"enforcement officer" means an officer in a law enforcement agency trained in cyber security work designated or authorised to carryout functions including for the purposes of Part IV of this Act;

"extradite" means the legal obligation of states under public international law to handover persons who commit international crimes to a foreign state for indictment, prosecution or imprisonment.

"encrypted data" means data which has been transformed from its plain text version to an unintelligible format, regardless of the technique utilised for such transformation and irrespective of the medium in which such data occurs or can be found, for the purposes of protecting the content of such data;

"false news" means incorrect deceptive information or propaganda, misinformation or hoaxes deliberately spread under the guise of being authentic news via traditional print and broadcast news media or online social media written and published with the intent to mislead for gains;

"Financial Institution" means any individual, body, association or group of persons, whether corporate or unincorporated which carries on the business of 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

---

or any act in relation to a computer system which impairs the operation of the computer system, program, or data;

"law enforcement agencies" means any agency for the time being responsible for implementation and enforcement of the provisions of this Act;

"Minister" means the Minister responsible for Information and Communications;

"modification" means in relation to a computer system, program or data, the alteration or modification with respect to the contents of a computer system by the operation of a function of the computer system or any other computer if ;

- (a) a program or data held in the computer system is altered or erased;
- (b) a program or data is added to its contents; or
- (c) an act occurs which impairs the normal operation of a computer system,

and any act which contributes towards causing such alteration or modification shall be deemed to have caused it;

"password" means any data by which a computer service or a computer system is capable of being obtained or used;

"person" includes a natural person, a corporation, company, partnership, firm, association or societies;

"Phishing" means the criminal and fraudulent process

"racist or 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, colour, descent or national or ethnic origin, as well as religion if used as a pretext for any of these factors.

"Requested State" means a state being requested to provide legal assistance under the terms of this Act;

"Requesting State" means a state requesting for legal assistance and may for the purposes of this Act include an international entity to which Sierra Leone is obligated;

"service provider" means a public or private entity that provides to users of its services the means to communicate by use of a computer system including any other entity that processes or stores computer data on behalf of that entity or its users;

"seize" with respect to a program or data be defined to include:

- (a) secure a computer system or part of it or a device;
- (b) make and retain a digital image or secure a copy of any program or data, including using an on-site equipment;
- (c) render the computer system inaccessible;
- (d) remove data in the accessed computer system;  
or
- (e) obtain output of data from a computer system;

access number, billing and payment information available on the basis of a service agreement or arrangement; or

- (c) any other information on the site of an installation of communication equipment available on the basis of a service agreement or arrangement;

"traffic data" means 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 the type of underlying service;

"unauthorised" means access of any kind, to a computer system, program or data, by a person who-

- (a) is not entitled to access that computer system, program or data; and
- (b) does not have or exceeds the level of authorisation consented to by the person entitled to grant such consent, for the particular kind or type of access with respect to that computer system, program or data:

Provided that any act or access in exercise of powers under this Act shall not be deemed to be unauthorised.



- (a) provision of support to computer systems and networks in preventing and combating cybercrime in Sierra Leone;
- (b) formulation and implementation of national cyber security policy and cyber security strategy;
- (c) overseeing of the management of computer forensic laboratories;
- (d) provision of support to the Judiciary and other law enforcement agencies in the discharge of their functions in relation to cybercrime in Sierra Leone;
- (e) promotion of Sierra Leone's involvement in international cyber security cooperation; and
- (f) doing 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.

4. (1) There is established, a National Cybersecurity Advisory Council comprising the Vice President as Chairman and the following other members-

Establishment  
of the  
National  
Cybersecurity  
Advisory  
Council.

- (a) the Minister of Finance;
- (b) the Attorney-General and Minister of Justice;
- (c) the Minister of Internal Affairs;
- (d) the Minister of Foreign Affairs and International Cooperation;
- (e) the National Security Coordinator, Office of National Security;

(3) The meeting of the Council shall be presided over by the Vice President and the Council shall meet, at least, 4 times a year.

5. (1) The Council shall-

Functions and Powers of the Council.

(a) provide strategic leadership, oversight and guidance on implementation and development of national cyber security legal framework in Sierra Leone in order to ensure that-

(i) Sierra Leone's cybercrime policies and laws are in conformity with regional and international standards;

(ii) there is maintenance of international cooperation required for preventing and combating cybercrimes and promoting cybersecurity; and

(iii) effective prosecution of cybercrimes and cyber security matters.

(b) make recommendation to Government on issues relating to the prevention and combating of cybercrime and the promotion of cyber security in Sierra Leone;

(c) provide general policy guidelines for the implementation of this Act; and

(d) promote the development of educational programs and research in cyber security defences, techniques and processes.

(2) The Council shall have power to regulate its proceedings and make standing orders with respect to the holding of its meetings, notices to be given, the keeping of minutes of its proceedings and such others matters as Council may from time to time determine.

(5) (i) The Council shall, as soon as possible but not later than 6 months after the end of each financial year, submit to the Minister a report of the activities, operations, undertakings, properties and finances of the National Computer Security Incidence Response Coordination Center for that year, including the Auditor General's Report.

(ii) The Minister shall within 30 days of the receipt of the report referred to in sub-section (5)(i) lay a copy before Parliament.

### PART III-CRITICAL NATIONAL INFORMATION INFRASTRUCTURE

7. (1) The Minister shall in consultation with the National Cybersecurity Council recommend to the President who may by Order published in the Gazette, designate certain computer systems, computer data or traffic data vital to Sierra Leone or any combination of those matters, as constituting Critical National Information Infrastructure. Designation Of Critical National Information Infrastructure.

(2) A Presidential Order made under subsection (1), shall prescribe minimum standards, guidelines, rules or procedures reasonably required in respect of-

- (a) the protection or preservation of Critical National Information Infrastructure;
- (b) the general management of Critical National Information Infrastructure;
- (c) the implementation of critical information systems to ensure all systems are secured by default and system and user activities are logged to facilitate accurate and efficient information systems operations audits.
- (d) access to, transfer and control of data in Critical National Information Infrastructure;

- (c) the collection of evidence in electronic form of a criminal offence under this Act or any other law.

(2) In a trial of an offence under any law, the fact that evidence has been generated, transmitted or seized from or identified in a search of a computer system, shall not of itself prevent that evidence from being presented, relied upon or admitted provided that the evidence has been properly obtained and preserved.

(3) The powers and procedures provided under this Part are without prejudice to the operation of, or powers granted under the Criminal Procedure Act, when exercised lawfully by any other law enforcement agency or service or any regulatory authority that by itself does not investigate or prosecute an offence.

**10.** (1) Upon an application by an enforcement officer or other authorised person to a Judge of the High Court that there is reasonable grounds to believe that there may be in a specified computer system, program, data, computer data storage medium material specifying the basis of the belief and the scope of the warrant required which-

Search and  
Seizure of  
Stored  
Computer  
data.

- (a) may be reasonably required as evidence in proving a specifically identified offence in a criminal investigation or criminal proceedings;
- (b) has been acquired by a person as a result of the commission of an offence,

the Judge may issue a warrant which shall authorise the enforcement officer or other authorised person, with such assistance as may be necessary, to access, seize or secure a specified computer system, program, data or computer data storage medium.

(2) A warrant issued under subsection (1) shall authorize an enforcement officer or other authorised person to-

---

a computer system into an intelligible format for the purposes of the warrant;

- (j) require a person possessing knowledge about the functioning of a computer system or measures applied to protect a computer data therein, to provide the necessary computer data or information, to enable an enforcement officer or other authorised person in conducting an activity authorised under this section;
- (k) have access to such reasonable technical and other assistance as he may require for the purposes of the warrant.
- (l) 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) An application under subsection (1) shall provide reasons explaining why it is believed that-

- (a) the material sought will be found on the premises to be searched; or
- (b) the purpose of an investigation search may be frustrated or seriously prejudiced unless an investigating officer arriving at the premises can secure immediate entry to them.

(4) The court may 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

- (i) not practical to secure the computer data; or
  - (ii) necessary to ensure that data will not be destroyed, altered or otherwise interfered with;
- (b) exercise reasonable care while the computer system or computer data storage medium is retained.

(8) An enforcement officer or other authorised person who intentionally, recklessly or negligently misuses the powers granted under this section commits an offence and is liable on conviction to a fine not less than Le 10,000,000 and not more than Le 50,000,000 or to a term of imprisonment not less than 1 year and not more than 5 years or to both such fine and imprisonment.

(9) A person who willfully obstructs an enforcement officer or other authorised person in the lawful exercise of the powers under this section commits an offence and is liable on conviction to a fine not less than Le5,000,000 and not more than Le30,000,000 or to a term of imprisonment not less than 6 months and not more than 3 years or to both such fine and imprisonment and in the case of a corporation, partnership or association to a fine not less than Le 50,000,000 and not more than Le100,000,000.

**11.** (1) Where a computer system or data has been removed or rendered inaccessible, following a search or seizure, the person who made the search or seizure shall, at the time of the search or seizure or as soon as practicable after the search -

Record of and  
Access to  
Seized Data.

- (a) make a list of what has been seized or rendered inaccessible, with the date and time of seizure; and
- (b) give a copy of that list to -

(5) The National Computer Security Incident Response Team shall develop standards, policies, procedures and guidelines to be used in the implementation of this Act subject to the approval of the National Cyber Security Advisory Council in respect of:

- (a) the warrant request process;
- (b) the process of collecting and handling evidence;
- (c) chain of custody of evidence collected;
- (d) processes related to device collection;
- (e) processes related to email collection;
- (f) the storage and inventory of data or evidence collected;
- (g) the process of examining evidence;
- (h) the analysis of data and evidence collected; and
- (i) evidence reporting.

**12.** (1) Where it is necessary or desirable for the purposes of an investigation under this Act, a Judge of the High Court may upon an application by an enforcement officer or other authorised person, order-

Production  
Order.

- (a) a person in possession or control of specified data stored in a computer system or a computer data storage medium; or
- (b) a service provider in possession or control of specified subscriber information relating to services offered -

- 
- (a) a specified computer data sought is likely to be available with a person mentioned in subparagraph (a) or (b) of subsection (1);
  - (b) an investigation may be frustrated or seriously prejudiced unless the specified computer data or the subscriber information, as the case may be, is produced;
  - (c) the type of evidence suspected is likely to be produced by a person mentioned in subparagraph (a) or (b) of subsection (1);
  - (d) subscribers, users or unique identifiers who are the subject of an investigation or prosecution, may be disclosed as a result of the production of the specified computer data;
  - (e) an identified offence is an offence in respect of which the order is sought;
  - (f) measures taken shall prepare and ensure that the specified computer data will be produced-
    - (i) whilst maintaining the privacy of other users, customers and third parties; and
    - (ii) without the disclosure of data of any party who is not part of the investigation; and
  - (g) measures taken shall prepare and ensure that the production of the specified computer data is carried out through technical means such as mirroring or copying of relevant data and not through physical custody of computer systems or devices.



(4) The period of preservation of data under subsection (3) may be extended by a Judge of the High Court for a further specified period of time, on an application by an enforcement officer or other authorised person, where such extension is reasonably required for the purposes of-

- (a) an investigation or prosecution;
- (b) avoiding a risk or vulnerability that the computer data may be modified, lost, destroyed or rendered inaccessible; or
- (c) averting overly burdensome cost of such preservation on the person in control of the computer system.

(5) A person to whom a notice under subsection (1) is given shall-

- (a) be responsible to preserve the data for -
  - (i) a period not exceeding 30 days as specified in subsection (3); or
  - (ii) any extended period permitted by a Judge of the High Court under subsection (4).
- (b) respond expeditiously to requests for assistance, whether to facilitate requests for police assistance or mutual assistance requests, and
- (c) disclose as soon as practicable, a sufficient amount of the non-content data to enable an enforcement officer or other authorised person to identify any other telecommunications providers involved in the transmission of the communication.

- 
- (d) preventing the investigation of being frustrated or seriously prejudiced; and
  - (e) averting overly burdensome cost of such extension on the person in control of the computer system.

(4) An application under subsection (1) shall state reasons explaining why it is believed that-

- (a) a traffic data sought will be available with the person in control of the computer system;
- (b) a type of traffic data suspected will be found on that computer system;
- (c) the subject of an investigation or prosecution may be found on that computer system;
- (d) an identified offence is an offence in respect of which the order is sought;
- (e) measures shall be taken to maintain the privacy of other users, customers and third parties; and
- (f) there will be no disclosure of data of any party not part of the investigation.

(5) A Judge of the High Court may also require a service provider to keep confidential, an Order under subsection (1) and a warrant issued under subsection (1) of section 10.

(6) A service provider who without reasonable excuse fails to comply with an Order under subsection (1) commits an offence and is liable on conviction to a fine not less than Le 100,000,000 and not more than Le 5,000,000,000.

- (e) measures taken shall be guided by regulations made pursuant to this Act which shall ensure that the real-time collection or recording is carried out whilst maintaining the privacy of other users, customers and third parties without the disclosure of information and data of any party not part of the investigation;
- (f) the investigation may be frustrated or seriously prejudiced unless the real time collection or recording is permitted;
- (g) to achieve the purpose for which the warrant is being applied, real time collection or recording by a person in control of a computer system is necessary; and
- (h) adequate provision is made to ensure the safe storage and protection of the content data obtained and be used solely for matters relating to investigations.

(4) A period of real-time collection or recording of content data under subsection (3) may be extended by a Judge of the High Court for a further reasonable specified period of time the same to be for an additional period not more than 30 days, on an application by an enforcement officer or other authorised person, where the extension is reasonably required for the purposes of-

- (a) an investigation or prosecution;
- (b) achieving the objective for which the warrant is to be issued;
- (c) ensuring that the real-time collection or recording of content data is carried out whilst

- (a) maintaining and making his services available; or
- (b) the disclosure of any data or other information to the extent required or in compliance with the exercise of powers under this Act.

**17.** (1) The High Court shall have jurisdiction over any Territorial violation of this Act, including any violation committed by a Sierra jurisdiction. Leone national regardless of the place of commission.

(2) The Jurisdiction of the High Court under subsection (1), shall lie if an offence under this Act was committed -

- (a) within Sierra Leone;
- (b) with the use of a computer system wholly or partly situated in Sierra Leone; or
- (c) when by such commission, damage is caused to a natural or juridical person who, at the time the offence was committed, was in Sierra Leone.

**18.** Subject to the powers of the Attorney-General and Minister Prosecution of of Justice, law enforcement agencies shall have power to prosecute Extraditable offences under this Act. In the case of offences committed under Offences. section 24 and 26 of this Act, the approval of the Attorney-General must be obtained before prosecution.

**19.** (1) The Court in imposing sentence on any person Forfeiture to convicted of an offence under this Act, may order that the convicted the State. person forfeits to the Republic of Sierra Leone-

- (a) any asset, money or property, whether tangible or intangible, traceable to proceeds of such offence; and
- (b) any computer, equipment, software, electronic device or any other device used or intended to be used to commit or to facilitate the commission of such offence;

- (a) assist the foreign state in initiating or carrying out an investigation or prosecution; or
- (b) lead to a request for co-operation by a foreign state.

provided that such foreign state shall have or undertake to effect mutual exchange of information with Sierra Leone in such manner as shall be agreed upon between the authorised personnel of such foreign state and the Attorney-General subject to the approval of Parliament

(2) Information provided under subsection (1), may be subject to such conditions including confidentiality, as the Attorney-General may require.

(3) Where a foreign state cannot comply with conditions required under subsection (2), it shall notify the Attorney-General, who shall determine whether the information should nevertheless be provided and where the foreign state accepts the information subject to the conditions, it shall be bound by them.

**22.** (1) The Attorney-General may cooperate with any foreign state or international agency for the purpose of-

Powers of the Attorney-General.

- (a) investigating or prosecuting offences under this Act; or
- (b) collecting electronic evidence related to an offence punishable under the laws of Sierra Leone.

(2) The Attorney-General shall communicate directly with the appropriate authority of a foreign state responsible for sending, answering, executing or transmitting requests for mutual assistance or extradition.

(3) Notwithstanding subsection (2), in case of urgency, requests may be sent directly from judicial authority to judicial authority, provided that the appropriate authority of the requested state is notified by the appropriate authority of the requesting state.

(4) The Attorney-General shall, where appropriate, before refusing or postponing assistance, after having consulted with the foreign state, consider whether the request may be granted partially or subject to such conditions, as he deems necessary.

(5) The Attorney-General shall promptly inform a foreign state of-

- (a) the outcome of the execution of a request for mutual assistance;
- (b) any reason that renders impossible, the execution of a request for mutual assistance or is likely to delay it significantly; or
- (c) any reason for refusal or postponement of a request for mutual assistance.

(6) A foreign state may request that Sierra Leone keeps confidential the fact of any request for mutual assistance, except to the extent necessary for its execution and if Sierra Leone cannot comply with the request for confidentiality, it shall promptly inform the foreign state, which shall then determine whether the request should nevertheless be executed.

**24.** (1) This Act complements the Extradition Act, 1974 (Act Extradition. No. 11 of 1974) which makes provision for the extradition of persons accused or convicted of an offence in another country.

(2) Extradition shall not be requested for an offence unless it is an offence in both the foreign state and in Sierra Leone.

(3) An offence under this Act shall be extraditable if the penalty imposed is imprisonment for a term of not less than one year or a fine equivalent to the penalty of one year imprisonment.

(4) Extradition will be subject to the conditions provided for by the law of the foreign state or applicable extradition treaties, including the grounds on which the foreign state may refuse extradition.

- (c) stored computer data to be preserved and its relationship to the offence;
- (d) available information identifying the custodian of the stored computer data or the location of the computer system;
- (e) necessity of the preservation of data; and
- (f) intention to submit a request for mutual assistance for the search, access, seizure, security, or disclosure of the stored computer data.

(3) Upon receiving a request under subsection (1), the Attorney-General shall take all appropriate measures to expeditiously preserve the specified data in accordance with the procedures and powers under this Act.

(4) A request under subsection (1) shall be effected where the conduct alleged does not constitute a crime in both the foreign state and in Sierra Leone.

(5) A preservation of data effected in response to a request under subsection (1) shall be for a period not less than 90 days, in order to enable the foreign state, to submit a request for the search, access, seizure, security or disclosure of the data and following the receipt of such a request, the data shall continue to be preserved until a final decision is taken on that pending request.

27. (1) Where during the course of executing a request under section 26, with respect to a specified communication, it is discovered that a service provider in another state was involved in the transmission of the communication, the Attorney-General shall expeditiously disclose to the foreign state, sufficient amount of traffic data to identify that service provider and the path through which the communication was transmitted.

Expedited disclosure of preserved traffic data.

(2) Expedited disclosure of preserved traffic data under subsection (1) may only be withheld where the -

- 
- (f) a statement setting out any wishes of the foreign state concerning confidentiality relating to the request and the reasons for those wishes;
  - (g) details of the period within which the foreign state wishes the request to be complied with;
  - (h) where applicable, details of the property, computer, computer system or device to be traced, restrained, seized or confiscated and of the grounds for believing that the property is believed to be in Sierra Leone;
  - (i) details of the stored computer data, data or program to be seized and its relationship to the offence;
  - (j) information identifying the custodian of the stored computer data or the location of the computer, computer system or device;
  - (k) an agreement on the question of the payment of the damages or costs of fulfilling the request;
  - (l) details to the effect that warrant in regard the matter under investigation has already been obtained to extend the investigations overseas; and
  - (m) any other information that may assist in giving effect to the request.

(3) Upon receiving a request under subsection (1), the Attorney- General shall take all appropriate measures to obtain necessary authorisation including a warrant to execute in accordance with the procedures and powers under this Act or any other law.



- 
- (b) the offence that is the subject of a criminal investigation or prosecution and a brief summary of the related facts;
  - (c) the name of the authority with access to the relevant traffic data;
  - (d) the location at which the traffic data may be held;
  - (e) the intended purpose for the required traffic data;
  - (f) sufficient information to identify the traffic data;
  - (g) further details of relevant traffic data;
  - (h) the necessity for use of powers under this section; and
  - (i) the terms for the use and disclosure of the traffic data to third parties.

(3) Upon receiving a request under subsection (1), the Attorney- General shall take all appropriate measures to obtain necessary authorisation including a warrant to execute upon the request in accordance with the procedures and powers under this Act or any other law.

(4) Upon obtaining necessary authorisation including a warrant to execute a request under subsection (1), the Attorney-General may seek the support and cooperation of the foreign state during the search and seizure.

(5) Upon conducting the measures under this section, the Attorney-General shall provide the results of such measures as well as real-time collection of traffic data associated with specified communication to the foreign state.

(3) Upon receiving a request under subsection (1), the Attorney-General shall take appropriate action to execute the request in accordance with the procedures and powers under this Act.

(4) The Attorney-General shall, on executing the request under subsection (3), provide the results of such action as well as real time collection or recording of content data of specified communication to the foreign state.

**32.** (1) The National Cybersecurity Coordinator or his authorized representative shall designate a point of contact available on a 24-hour, 7-days-a-week basis, in order to ensure the provision of immediate assistance for the purpose of investigation or prosecution of offences related to computer systems and data, or for the collection of evidence in electronic form. Point of contact.

(2) Immediate assistance to be provided under subsection (1) shall include -

- (a) the provision of technical advice;
- (b) the preservation of data pursuant to expedited preservation of stored computer data and expedited disclosure of preserved traffic data; and
- (c) the collection of evidence, the provision of legal information, and locating of suspects.

(3) A point of contact under subsection (1), shall -

- (a) be resourced with and possess the requisite capacity to securely and efficiently carry out communication with other points of contact in other states, on an expedited basis;
- (b) have the authority and be empowered to coordinate and enable access to international

(d) uses the computer data.

(3) For the purposes of this section, "unauthorised" means access of any kind, to a computer system, program or data, by a person who has been authorised to access a specific data in a computer system and without lawful excuse, whether temporary or not, cause a computer system to perform a function other than those authorised, with intent to secure access to the whole or a part of a computer system or to enable such access to be secured.

(4) The absence of authority to secure access to the whole or any part of a computer system under subsection (1) includes instances where there may exist general authority to access a computer system but a specific type, nature or method of access may not be authorised.

(5) For the purposes of this section intention or recklessness needs not relate to-

- (a) a particular computer system;
- (b) a particular program or data; or
- (c) a program or data of any particular kind.

(6) A person shall be deemed to have contravened subsection (1)-

- (a) in the absence of proof that the accused has the requisite knowledge to access the computer, program or data;
- (b) notwithstanding the fact that committing the offence is impossible;
- (c) in the absence of a program or data of any particular kind.

**34.** (1) A person, including a corporation, partnership, or association, who intentionally or without reasonable authorisation causes a computer system to perform a function with intent to secure access to computer or program or data used directly in connection

Unauthorised  
access to  
protected  
system.

- (b) causes physical injury or death to any person; or
- (c) threatens public health or public safety,

commits an offence and is liable upon conviction to a fine not less than Le 100,000,000 and not more than Le 250,000,000 or to a term of imprisonment not less than 2 years and not exceeding 5 years or to both such fine and imprisonment and in the case of a corporation, partnership, or association, to a fine not less than Le 500,000,000 and not exceeding Le 1,000,000,000.

(2) Where a person, including a corporation, partnership, or association, intentionally and without authorisation, intercepts or causes to be intercepted, the transmission of data to or from a computer system over a telecommunication under subsection (1), commits an offence and is liable upon conviction to a fine not less than Le 100,000,000 and not more than Le 250,000,000 or to a term of imprisonment not less than 2 years and not exceeding 5 years or to both such fine and imprisonment and in the case of a corporation, partnership, or association, to a fine not less than Le 500,000,000 and not exceeding Le 1,000,000,000.

It is immaterial whether -

- (a) the unauthorised interception is not directed at-
  - (i) a telecommunications system;
  - (ii) a particular computer system;
  - (iii) a program or data of any kind; or
  - (iv) a program or data held in any particular computer system;
- (b) an unauthorised interception or an intended effect of it is permanent or temporary.

imprisonment not less than 2 years and not exceeding 5 years or to both such fine and imprisonment and in the case of a corporation, partnership, or association, to a fine not less than Le 500,000,000 and not exceeding Le 1,000,000,000

**37.** A person, including a corporation, partnership, or association, who intentionally or without authorisation does an unauthorised act in relation to a computer system which - Unauthorised system interference.

- (a) interferes with, hinders, damages, prevents, suppresses, deteriorates, impairs or obstructs the functioning of a computer system;
- (b) interferes with, hinders, damages, prevents, suppresses, deteriorates, impairs or obstructs the communication between or with a computer system;
- (c) interferes with or hinders access to a computer system;
- (d) impairs the operation of a computer system;
- (e) impairs the reliability of a computer system;
- (f) impairs the security of a computer system;  
or
- (g) enables any of the acts mentioned in paragraphs (a) to (f) to be done,

commits an offence and is liable upon conviction to a fine not less than Le 100,000,000 and not more than Le 250,000,000 or to a term of imprisonment not less than 2 years and not exceeding 5 years or to both such fine and imprisonment and in the case of a corporation, partnership, or association, to a fine not less than Le 500,000,000 and not exceeding Le 1,000,000,000

(3) For the purpose of subsection (1), possession of a program or a computer password, access code, or similar data includes having-

- (a) possession of a computer system which contains the program or a computer password, access code, or similar data;
- (b) possession of a data storage device in which the program or a computer password, access code, or similar data is recorded; or
- (c) control of a program or a computer password, access code, or similar data that is in the possession of another person.

**39.** A person, including a corporation, partnership, or association, who intentionally or without authorisation discloses to another person a password, access code or other means of gaining access to any program or data held in a computer system-

Unauthorised disclosure of password.

- (a) for any wrongful gain;
- (b) for any unlawful purpose; or
- (c) to occasion any loss,

commits an offence and is liable upon conviction to a fine not less than Le 10,000,000 and not more than Le 30,000,000 or to a term of imprisonment not less than 1 year and not exceeding 3 years or to both such fine and imprisonment and in the case of a corporation, partnership, or association, to a fine not less than Le 50,000,000 and not exceeding Le 100,000,000.

**40.** (1) A person, including a corporation, partnership, or association, who intentionally or without authorisation inputs, alters, deletes or suppresses 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 of whether or not the data is directly

Computer related forgery.

- (c) copying, transferring or moving data or program to another computer system, device or storage medium other than that in which it is held or to a different location in any other computer system, device or storage medium in which it is held;
- (d) using any data or program; or
- (e) having any data or program output from the computer system in which it is held, whether by having it displayed or in any other manner,

with fraudulent or dishonest intent of procuring, without right, an economic benefit for himself or for another person commits an offence and is liable upon conviction to a fine not less than Le 30,000,000 and not more than Le 50,000,000 or to a term of imprisonment not less than 2 years and not exceeding 5 years or to both such fine and imprisonment and in the case of a corporation, partnership, or association, to a fine not less than Le 100,000,000 and not exceeding Le 250,000,000"

**42.** (1) A person, including a corporation, partnership, or association, who is engaged in the services of any financial institution, and as a result of his special knowledge commits identity theft, phishing of its employer, staff, service providers and consultants with the intent to defraud commits an offence and is liable upon conviction to a fine not less than Le 50,000,000 and not more than Le 100,000,000 or to a term of imprisonment not less than 3 years and not exceeding 7 years or to both such fine and imprisonment and in the case of a corporation, partnership, or association, to a fine not less than Le 100,000,000 and not exceeding Le 250,000,000.

Identity theft  
and  
impersonation.

(2) A person, including a corporation, partnership, or association, who fraudulently-

offence and shall be liable on conviction to a fine not less than Le 50,000,000 and not more than Le 100,000,000 or to a term of imprisonment not less than 3 years and not exceeding 7 years or to both such fine and imprisonment and in the case of a corporation, partnership, or association, to a fine not less than Le100,000,000 and not exceeding Le 250,000,000

**43.** A person, including a corporation, partnership, or association, who with the intent to defraud and or misrepresent, forges through electronic devices another person's signature or company mandate commits an offence and shall be liable on conviction to a fine not less than Le 50,000,000 and not more than Le 1,000,000,000 or to a term of imprisonment not less than 3 years and not exceeding 5 years or to both such fine and imprisonment and in the case of a corporation, partnership, or association, to a fine not less than Le500,000,000 and not exceeding Le 5,000,000,000. Electronic signature.

**44.** (1) A person, including a corporation, partnership, or association, who individually or with another person, willfully and repeatedly communicates, either directly or indirectly, with another person, if he knows or ought to have known that his conduct - Cyber stalking and cyber bullying.

- (a) is likely to cause that person apprehension or fear of violence to him or damage or loss on his property; or
- (b) detrimentally affects that person;

commits an offence and shall be liable on conviction to a fine not less than Le 30,000,000 and not more than Le 50,000,000 or to a term of imprisonment not less than 2 years and not exceeding 5 years or to both such fine and imprisonment and in the case of a corporation, partnership, or association, to a fine not less than Le 100,000,000 and not exceeding Le 250,000,000

(2) A person, including a corporation, partnership, or association, who recklessly or intentionally sends a message or other matter by means of a computer system or network that-



(2) In awarding penalty against an offender under this section, a court shall have regard to the following-

- (a) refusal by the person to relinquish, upon formal request by the rightful owner without reasonable excuse of a name, business name, trademark, domain name, or other word or phrase registered, owned or in use by any individual, body corporate or belonging to the Government of Sierra Leone; or
- (b) any attempt by the offender to obtain compensation in any form for the release to the rightful owner for use of the name, business name, trademark, domain name or other word or phrase registered, owned or in use by the individual, body corporate or belonging to the Government of Sierra Leone.

(3) In addition to the penalty specified in this section, the court may make an order directing an offender to relinquish such registered name, mark, trademark, domain name or other word or phrase to the rightful owner.

**46.** A person, including a corporation, partnership, or association, who, through input, alteration, modification, deletion, suppression or generation of a program or data or through use of a computer, computer system or electronic device willfully infringes any right protected under the Copyright Act, 2011(Act No. 8 of 2011) or any law in force for protection of copyrights and related rights, commits an offence and is liable on conviction to a fine not less than Le 100,000,000 and not more than Le 250,000,000 or to a term of imprisonment not less than 2 years and not exceeding 5 years or to both such fine and imprisonment and in the case of a corporation, partnership, or association, to a fine not less than Le500,000,000 and not exceeding Le 1,000,000,000 without prejudice to civil remedies that may be available.

Infringement  
of copyright  
and related  
rights.

- (iii) a child's mental or physical disability or situation of dependence is a b u s e d;

commits an offence and shall be liable on conviction to a fine not less than Le 100,000,000 and not more than Le 250,000,000 or to a term of imprisonment not less than 5 years and not exceeding 10 years or to both such fine and imprisonment and in the case of a corporation, partnership, or association, to a fine not less than Le 500,000,000 and not exceeding Le 1,000,000,000

(3) Notwithstanding subsection (1) a person shall not be deemed to have committed an offence if he does an act intended for a bona fide scientific or medical research or law enforcement.

(4) For purposes of this section-

"child" means a person under the age of 18 years;

"child pornography" includes data which, whether visual or audio, depicts-

- (a) a child engaged in sexually explicit conduct;
- (b) a person who appears to be a child engaged in sexually explicit conduct; or
- (c) realistic images representing a child engaged in sexually explicit conduct.

**48.** (1) A person, including a corporation, partnership, or association who: Online adult sexual abuse.

- (a) take or share an intimate image or voice material of a depicted person without his/her consent;

partnership, or association, to a fine not less than Le 500,000,000 and not exceeding Le 1,000,000,000.

(2) In this section, the expressions "intimate image or voice material" shall include video, images or voice media created by the depicted person which he/she has not willingly put into the public domain; video, images or voice media taken by another; video, images or voice media in the possession of the perpetrator by any means whatsoever including been stolen from a hacked computer or other digital device of the depicted person; video, image or voice material that may have been doctored by superimposing the face or voice of a depicted person unto an existing intimate or sexually explicit image or some other voice media.

**49.** (1) A person, including a corporation, partnership, or association, who intentionally abets the commission of, aids to commit, attempts to commit or does any act preparatory to or in furtherance of the commission of an offence under this Act commits an offence and is liable upon conviction to the same penalty as that prescribed in respect of the substantive offence under this Act. Attempting and Aiding or Abetting.

(2) An offence may be deemed to have been committed under subsection (1), notwithstanding where the act in question took place.

**50.** (1) No person shall engage in the operation of a business of providing computers for accessing the internet, playing games, chatting or doing other computer-related tasks unless the business. Registration of cyber cafes.

**51.** (1) A person who accesses or cause to be accessed a computer or computer system or network for purposes of a terrorist act, commits an offence and is liable on conviction to a term of imprisonment not less than 10 years and not exceeding 20 years.

Cyber  
Terrorism.

(2) For purposes of this section, "terrorist act" shall have the same meaning as provided under the Anti-Money Laundering and Combating of Financing of Terrorism Act, 2012 (Act No. 2 of 2012).

**52.** (1) A person, including a corporation, partnership, or association, who with intent-

Racist  
Xenophobic  
Offences.

- (a) distributes or otherwise makes available, racist or xenophobic material to the public through a computer system or network;
- (b) threatens through a computer system or network any other person or group of persons for the reason of belonging to a group distinguished by race, colour, descent, national or ethnic origin, gender religion, as well as disability
- (c) insults publicly through a computer system or network any other person or group of persons distinguished by race, colour, descent or national or ethnic origin, as well as religion; or

10,000,000 and not more than Le 30,000,000 or to a term of imprisonment not less than 1 year and not exceeding 3 years or to both such fine and imprisonment and in the case of a corporation, partnership, or association, to a fine not less than Le50,000,000 and not exceeding Le 100,000,000.

**54.** (1) A person or institution which, being a computer based service provider and or vendor does an act with intent to defraud and by virtue of his position as a service provider, forges, illegally uses security codes of the consumer with the intent to gain a financial and or material advantage or with intent to provide less value for money in his or its services to a consumer commits an offence and upon conviction is liable to a fine not less than Le 30,000,000 and not more than Le 50,000,000 or to a term of imprisonment not less than 1 year and not exceeding 3 years or to both such fine and imprisonment and in the case of a corporation, partnership, or association, to a fine not less than Le100,000,000 and not exceeding Le 250,000,000.

Breach of confidence by service providers.

(2) Where an offence under this Act committed by a body corporate is proved to have been committed on the instigation or with the connivance of or attributable to willful neglect on the part of a director, manager, secretary or other like officer of the body corporate or any officer purporting to act in any such capacity, he, as well as the body corporate, where practicable, shall be deemed to have committed the offence.

(3) Notwithstanding subsection (1), where a body corporate is convicted of an offence under this Act, which threatens national security the Court may in the case of multiple or repeated

- (c) authority to exercise control within a legal person, acting either individually or as part of an organ of the legal person,

and fails to exercise reasonable and proper control over such legal person commits an offence under this Act, and is liable on conviction to a fine not less than Le 10,000,000 and not more than Le 30,000,000 or to a term of imprisonment not less than 1 year and not exceeding 3 years or to both such fine and imprisonment and in the case of a corporation, partnership, or association, to a fine not less than Le 100,000,000 and not exceeding Le 250,000,000.

(2) Where a natural person commits a criminal offence under this Act, for the benefit of a legal person, due to the lack of supervision or control by a natural person, the legal person shall be liable for the offence under this Act.

**57.** Without prejudice to the offences prescribed under this Act and subject to the provisions of the Children and Young Persons Act Cap.44 and the Child Rights Act 2007, where an act done by a child would be deemed to be an offence under this Act such child shall be treated as a juvenile and dealt with accordingly Acts by children.

#### PART VII-MISCELLANEOUS PROVISIONS

**58.** The Minister may by Statutory Instrument make Regulations. Regulations as it considers necessary or expedient for giving effects to any of the provisions of this Act.