BILL

Supplement to the Sierra Leone Extraordinary Gazette Vol. CXLXI, No. 27

dated 11th May, 2020

THE CYBERCRIME ACT, 2020

ARRANGEMENT OF SECTIONS

Section.

PART 1–PRELIMINARY

1. Definitions.

PART II - CRITICAL NATIONAL INFORMATION INFRASTRUCTURE

2. Designation of certain computer systems as Critical National Information Infrastructure.
3. Audit and inspection of Critical National Information Infrastructure.

PART III - POWERS AND PROCEDURES

4. Scope of powers and procedures.
5. Search and seizure of stored computer data.
6. Record of and access to seized data.
7. Production order.
8. Expedited preservation and partial disclosure of traffic data.
9. Real-time collection of traffic data.
10. Interception of content data.
11. Confidentiality and limitation of liability.
12. Territorial jurisdiction.

PART IV - INTERNATIONAL COOPERATION

13. Spontaneous information.
14. Powers of the Attorney-General.
15. Authority to make and act on mutual assistance requests.
16. Extradition.
17. Confidentiality and limitation of use.
18. Expedited preservation of stored computer data.
19. Expedited disclosure of preserved traffic data.
20. Mutual assistance regarding accessing of stored computer data.

21. Trans-border access to stored computer data.
22. Mutual assistance in real time collection of traffic data.
23. Mutual assistance regarding interception of content data.
24. Point of contact.

PART V- OFFENCES

25. Unauthorised access.
26. Unauthorised access to protected system.
27. Unauthorised data interception.
28. Unauthorised data interference.
29. Unauthorised system interference.
30. Misuse of device.
31. Computer-related forgery.
32. Computer fraud.
33. Identity theft and impersonation.
34. Electronic signature.
35. Cyber stalking and cyber bullying.
36. Cyber Squatting.
37. Infringements of copyright and related rights.
38. Online child sexual abuse.
39. Attempting and aiding or abetting.
40. Registration of cybercafé.
41. Cyber terrorism.
42. Racist and xenophobic offences.
43. Reporting of cyber threats.
44. Breach of confidence by service providers.
45. Employees responsibility.
46. Corporate liability.

PART VI - ADMINISTRATION AND ENFORCEMENT

47. Co-ordination and enforcement.
48. Establishment of the National Cybersecurity Advisory Council.
49. Functions and powers of the Council.
50. Establishment of National Cybersecurity Fund.

PART VII -MISCELLANEOUS PROVISIONS

51. Regulations.

No. **2020**

Sierra Leone

THE CYBERCRIME ACT, 2020

Short title.

Being an Act to provide for the prevention of the abusive use of computer systems; 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; to provide for facilitation of international cooperation in dealing with cybercrime matters and to provide for other related matters.

[ ]

Date of commencement.

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

PART I – PRELIMINARY

Definitions.

1. In this Act, unless the contrary intention appears -

"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;

"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;

"computer system" means any physical or virtual device, or any set of associated physical or virtual devices; or a group of interconnected or related devices, one or more of which, pursuant to a program, performs automatic processing of data at least one of which use electronic, magnetic, optical or other technology, to perform logical, arithmetic storage and data or which perform control functions on physical or virtual devices including mobile devices and reference to a computer system includes a reference to part of a computer system;

"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;

"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;

"extradite or prosecute" means the legal obligation of states under public international law to prosecute persons who commit serious international crimes where no other state has requested extradition;

"interference" means any impairment to the confidentiality, integrity or availability of a computer system, or any program or data on a computer system, or any act in relation to a computer system which impairs the operation of the computer system, program, or data;

“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;

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

"plain text version" means original data before it has been transformed into an unintelligible format.

"program or computer program" means computer data representing instructions or statements that, when executed in a computer system, causes the computer system to perform a function;

"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;

"subscriber information" means any information contained in the form of data or any form that is held by a service provider, relating to subscribers of its services, other than traffic data or content data, 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, geographic, electronic mail address, telephone and other 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 the Act shall not be deemed to be unauthorised.

PART II-CRITICAL NATIONAL INFORMATION INFRASTRUCTURE

Designation of Critical National Information Infrastructure.

2. (1) The President may, on the recommendation of the Minister 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.

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

(a) the protection or preservation of Critical National Information Infrastructure;

(b) the general management of Critical National Information Infrastructure;

(c) access to, transfer and control of data in Critical National Information Infrastructure;

(d) infrastructural or procedural rules and requirements for securing the integrity and authenticity of data or information contained in any designated Critical National Information Infrastructure;

(e) the storage or archiving of data or information designated as Critical National Information Infrastructure;

(f) recovery plans in the event of disaster, breach or loss of the Critical National Information Infrastructure or any part of it; and

(g) any other matter required for the adequate protection, management and control of data and other resources in any Critical National Information Infrastructure.

Audit and inspection of Critical National Information Infrastructure.

3. A Presidential Order made under subsection (1) of section 2 may require the National Computer Security Incidence Response Teamestablished by the coordinating body under paragraph (c) of subsection (1) of section 47 to audit and inspect any Critical National Information Infrastructure at any time to ensure compliance with this Act.

PART III - POWERS AND PROCEDURES

Scope of powers and procedures.

4. (1) Powers and procedures under this Act shall be applicable to and may be exercised with respect to -

(a) criminal offences under this Act;

(b) criminal offences committed by means of a computer system, including mobile phones and other electronic equipment, under any other law; and

(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.

Search and seizure of stored computer data.

5. (1) Upon an application by a police 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 which -

(a) may be reasonably required as evidence in proving a specifically identified offence in a criminal investigation or criminal proceedings;