CYBERCRIME BILL 2019

Arrangement of sections

CYBERCRIME BILL 2019

CYBERCRIME BILL 2019

A BILL ENTITLED -

An Act to provide for the establishment of the cybercrime regulations and committee and for connected matters.

[ ]

ENACTED by the President and the National Assembly.

PART I – PRELIMINARY

1. Short title and commencement

This Act may be cited as The Cybercrime Act, 2019 and shall come into force on such date as the Minister may designate by Order in the gazette.

2. Interpretation

For the purpose of this Act, unless the context otherwise requires-

"computer system" means any device or a group of interconnected or related devices, one or more of which, pursuant to a program, performs automatic processing of data;

“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*;*

“service provider” means: any public or private entity that provides to users of its service the ability to communicate by means of a computer system, and any other entity that processes or stores computer data on behalf of such communication service or users of such service;

“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.

3. Objects of the Act

The objectives of the Act are to –

(a) protect the confidentiality, integrity and availability of computer systems, programs and data;

(b) prevent the unlawful use of computer systems;

(c) facilitate the prevention, detention, investigation, prosecution and punishment of cybercrime;

(d) facilitate international co-operation on matters covered under this Act.

Part II – Offences

4. Unauthorized access to computer data

(1) Subject to subsections (2), a person who causes a computer system to perform a function with intent to secure access, and knowing that the access he intends to secure is unauthorized, commits an offence.

(2) Access by a person to a computer system is unauthorized where the person-
(a) is not himself or herself entitled to control access of the kind in question; and
(b) does not have consent to access by him or herself of the kind in question from any person who is so entitled.

(3) A person secures access in relation to any computer system if he instructs, communicate with, stores data in, retrieves data from, or otherwise make use of any of the resources, of the computer system;

(4) For the purposes of this section, it is immaterial that the unauthorized access is not directed at:
(a) any particular computer data;
(b) computer data of any kind; or
(c) computer data held in any particular computer system.

(5) A person shall not be liable under subsection (1) where he or she is acting in reliance of any statutory power arising under any enactment for the purpose of obtaining information, or of taking possession of, any document or other property.

(6) A person convicted for an offence under subsection (1) is liable on conviction, in the case of:
(a) an individual, to a fine not exceeding two hundred thousand dalasis or imprisonment for a term not exceeding five years, or to both the fine and imprisonment;
(b) a body corporate, to a fine of not less than five hundred thousand dalasis.

5. Unauthorized interception of computer data

(1) Subject to subsection (5), a person who intentionally and without authorization, intercepts or causes to be intercepted, directly or indirectly, any computer data to, from or within a computer system, commits an offence.

(2) A person convicted for an offence under subsection (1) is liable on conviction, in the case of:
(a) an individual, to a fine not exceeding two hundred thousand dalasis or imprisonment for a term not exceeding five years, or to both the fine and imprisonment;
(b) a body corporate, to a fine of not less than five hundred thousand dalasis.

(3) An act of interception of any computer data to, from or within a computer system, includes listening to, or recording, or acquiring the substance, its meaning or purport of that computer data;

(4) For the purpose of this section, it is immaterial
that the unauthorized interception is not
directed at -
(a) any particular computer data;
(b) computer data of any kind; or
(c) computer data held in any particular computer system.

(5) A person is not liable under subsection (1) if he:
(a) has the express or implied consent of both
the person who sent the computer data and the intended recipient of the computer data; or
(b) is acting in reliance of an authorization under any statutory power.

6. Unauthorised acts in relation to a computer system or data

(1) A person is guilty of an offence if -

(a) he does any unauthorised act in relation to a computer system or computer data;
(b) at the time when he does the act he knows that it is unauthorised; and
(c) either subsection (2) or subsection (3) below applies.

(2) This subsection applies if the person intends by doing the act -
(a) to impair the operation of any computer system;
(b) to prevent or hinder access to any computer data held in any computer system or;
(c) to impair the operation or the reliability of any such computer data;

(3) This subsection applies if the person is reckless as to whether the act will do any of the things mentioned in paragraphs (a) to (c) of subsection (2) above.

(4) The intention referred to in subsection (2) above, or the recklessness referred to in subsection (3) above, need not relate to -
(a) any particular computer system;
(b) any particular computer data; or
(c) computer data of any particular kind.

(5) In this section—
(a) a reference to doing an act includes a reference to causing an act to be done;
(b) "act" includes a series of acts;
(c) a reference to impairing, preventing or hindering something includes a reference to doing so temporarily.

(6) An act done in relation to a computer system is unauthorised if the person doing the act (or causing it to be done)—
(a) is not himself a person who has responsibility for the computer system or computer data and is entitled to determine whether the act may be done; and
(b) does not have consent to the act from any such person.

(7) A person convicted for an offence under subsection (1) is liable on conviction, in the case of:
(a) an individual, to a fine not exceeding two hundred thousand dalasis or imprisonment for a term not exceeding five years, or to both the fine and imprisonment;
(b) a body corporate, to a fine of not less than five hundred thousand dalasis.

7. Unlawful supply or possession of computer systems or other device, or computer data

(1) A person who intentionally manufactures, sells, procures for use, imports, distributes or otherwise makes available, a computer system or any other device, or computer data designed or adapted primarily for the purpose of committing an offence under subsections [……..], commits an offence.

(2) A person who is found in possession of any computer data with the intention that the computer data be used, by the person himself or another person, to commit or facilitate the commission of an offence under subsections [……..], commits an offence.

(3) For the purposes of subsection (2), possession of any computer data includes
(a) having possession of computer system or computer data storage device that holds or contains the computer data;
(b) having possession of a document in which the computer data is recorded; or
(c) having control of computer data that is in the possession of another person.

(4) A person who commits an offence under this section is liable on conviction, in the case of:
(a) an individual, to a fine not exceeding two hundred thousand dalasis or imprisonment for a term not exceeding five years, or to both the fine and imprisonment;
(b) a body corporate, to a fine of not less than five hundred thousand dalasis.

8. Computer-related extortion, fraud and forgery

(1) A person who intentionally performs or threatens to perform any of the acts described in subsections [……..] for the purpose of obtaining a gain for himself or another, or to cause loss to another or expose another to risk of loss, including by undertaking to cease or desist from the act, or by undertaking to restore any damage caused as a result of those acts, commits of an offence.

(2) A person who processes computer data with the intent that it be considered or acted upon for legal purpose as if it were authentic, for the purpose of obtaining a gain for himself or another, or to cause loss to another or expose another to risk of loss, commits of an offence.

(3) A person who commits an offence under this section is liable on conviction, in the case of:
(a) an individual, to a fine not exceeding two hundred thousand dalasis or imprisonment for a term not exceeding five years, or to both the fine and imprisonment;
(b) a body corporate, to a fine of not less than five hundred thousand dalasis.

9. Indecent images of children

(1) A person who intentionally:
(a) takes or permits to be taken or to make, an indecent image or representation of a child;
(b) offers, distributes, makes available or shows an indecent image or representation of a child;
(c) procures through a computer system and has in his or her possession an indecent image or representation of a child, for himself or with a view to it being distributed or shown to any other person; or
(d) publishes or causes to be published an advertisement likely to be understood as conveying that the advertiser distributes or shows the indecent image or representation of a child, or intends to do so,
commits an offence.

(2) Where a person is charged with an offence under subsection (1)(b) or (c), it is a defence for the person to prove that:
(a) had reasonable grounds for distributing or showing the image or representation of a child; or having them in his possession; and
(b) had not himself seen the image or representation of a child; and did not know, or had any cause to suspect, it to be indecent.

(3) Where
(a) the impression conveyed by the image or representation is that the person shown is a child; or
(b) the predominant impression conveyed is that the person shown is a child, notwithstanding that some of the physical characteristics shown are those of an adult,
the image or representation shall be treated for all purposes of this section as showing a child.

(4) The Court before which a person is convicted of an offence under this section may, in addition to any penalty imposed, order

(a) the forfeiture of any apparatus, article or thing which is the subject matter of the offence or is used in connection with the commission of the offence; or
(b) that the material subject matter of the offence be no longer stored on and made available through the computer system, or that the material be deleted.

(5) A person who commits an offence under this section is liable on conviction, in the case of:
(a) an individual, to a fine not exceeding two hundred thousand dalasis or imprisonment for a term not exceeding […..] years, or to both the fine and imprisonment;
(b) a body corporate, to a fine of not less than five hundred thousand dalasis.

10. Offences related to infringements of copyright and related rights

Adopt provisions in s. 53. Criminal Sanctions of the Copyright Act

11. Attempt and aiding or abetting

Adopt the provisions in s. 23(1) of the Criminal Code

12. Criminal liability of directors etc.

(1) An offence committed by a body corporate is treated as committed by a person who, at the time the offence was committed, was-
(a) a director, principal officer, general manager, secretary, or other similar officer of the company; or
(b) acting or purporting to act in that capacity.

(2) Subsection (1) does not apply to a person if-

(a) the offence was committed without that person's consent or knowledge; and
(b) the person has exercised all diligence to prevent the commission of the offence as ought to have been exercised having regard to the nature of the person's functions and all the circumstances.

13. Sanction or measures

Recommendation of the Drafting Committee:

The Drafting Committee recommend that the Ministry of Justice reconsider the current sanctions to differentiate the offences in terms of level of seriousness.

Part III - Procedural Powers

14.Search and seizure of stored computer data

(1) Upon an application made under oath and affidavit by a police officer or another authorised person that demonstrates to the satisfaction of a judge that there exist reasonable grounds to believe that there may be in a specified computer system, program, data, or computer data storage medium that-

(a) is reasonably required for the purpose of a criminal investigation or criminal proceedings which may be material as evidence in proving a specifically identified offence; or

(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 a police officer or another authorised person, with such assistance as may be necessary, to:

(i) access, seize or similarly secure the specified computer system, program, data or computer data storage medium:

(ii) have access to and inspect and check the operation of any computer system to which the warrant issued under this section applies;

(iii) have access to any information, code or technology which has the capability of unscrambling encrypted data contained or available to such computer system into an intelligible format for the purpose of the warrant issued under this section;

(iv) be entitled to require any person possessing knowledge about the functioning of the computer system or measures applied to protect the computer data therein to provide, as is reasonable, the necessary computer data or information, to enable the police officer or another authorised person in conducting such activities as authorised under this section;

(v) be entitled to require any person in possession of decryption information to grant him access to such decryption information necessary to decrypt data required for the purpose of the warrant issued under this section;

(vi) to provide him with such reasonable technical and other assistance as he may require for the purposes of the warrant issued under this section.

(2) When making an application under subsection (1), the police officer or another authorised person shall provide the following substantive grounds:

(a) explain why it is believed the material sought will be found on the specified computer system, program, data or computer data storage medium to be searched;

(b) identify and explain with [specificity] the type of evidence suspected will be found on the premises; and

(c) what measures shall be taken to prepare and ensure that the search and seizure is carried out through technical means such as mirroring or copying of relevant data and not through physical custody of computer system, program, data, computer data storage medium.

(3) Where a police officer or another authorised person is authorized to search or similarly access a specified computer system, program, data, or computer data storage medium, under subsection (1) of this section, and has grounds to believe that the data sought is stored in another computer system or part of it in its territory, and such data is accessible from or available to the initial system, the police officer or another authorised person may extend the search or similar accessing to such other system or systems.

(4) Seized computer data may be used for only lawful purposes, being the purpose for which it was originally obtained, or to enforce the criminal law,

(5) The police officer or another authorised person shall:

(a) only seize a computer system under sub-section (1) when:

(i) it is not practical to seize or similarly secure the computer data; or

(ii) it is 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.

(6) Any person who wilfully obstructs the lawful exercise of the powers under this section or misuses the powers granted under this section shall be punished

with imprisonment for a term not exceeding [….], or a fine not exceeding [un….], or both.

(7) For the purposes of this section:

"decryption information" means information or technology that enables a person to readily unscramble encrypted data into an intelligible format;

"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;

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

15. Real-time collection of traffic data

(1) Upon an application made under oath and affidavit by a police officer or another authorised person that demonstrates to the satisfaction of a judge that there are reasonable grounds to believe that traffic data associated with specified communications and related to or connected with a person under investigation is reasonably required for the purposes of a specific criminal investigation, a judge may issue a warrant requiring a service provider, to-

(a) collect or record traffic data in real-time; and
(b) provide only the traffic data to the authorized officer,

Provided that such real-time collection or recording of traffic data shall not be ordered for a period beyond that which is absolutely necessary and in any event for a period of not more than 7 days.

(2) When issuing a warrant under subsection (1), the judge shall be satisfied that:

(a) the extent of interception is commensurate, proportionate and necessary for the purposes of a specific criminal investigation or prosecution;

(b) measures shall be taken to ensure that the data is intercepted whilst maintaining the privacy of other users, customers and third parties and without the disclosure of information and data of any party not part of the investigation; and

(c) the investigation may be frustrated or seriously prejudiced unless the interception is permitted.

(3) The period of real-time collection or recording of traffic data may be extended beyond 7 days if, on an application, a judge authorizes an extension for a further specified period of time, not exceeding a further period of 7 days.

(4) When making an application under subsection (1), the police officer or another authorised person shall provide the following substantive grounds and reasons also:

(a) explain why it is believed the traffic data sought will be available with the person in control of the computer system;

(b) identify and explain with specificity the type of traffic data suspected will be found on such computer system;

(c) identify and explain with specificity the subscribers, users or unique identifier the subject of an investigation or prosecution suspected may be found on such computer system;

(d) identify and explain with specificity the identified offences in respect of which the warrant is sought;

(e) what measures shall be taken to prepare and ensure that the traffic data will be sought and carried out

(i) whilst maintaining the privacy of other users, customers and third parties; and

(ii) without the disclosure of data of any party not part of the investigation.

(5) A judge may also require the service provider to keep confidential the warrant and execution of any power provided for under this section.

(6) A service provider served with an order has a duty to comply, but is not required to take any steps that it is not reasonably practicable to take.

(7) Where obligations have been imposed on a service provider under Section (…)(8), the steps which it is reasonably practicable for the service provider to take include every step which it would have been reasonably practicable for service provider to take if it had complied with its obligations under Section (…)(8).

(8) A service provider who fails to comply shall be liable for a penalty of [….]

16. Interception of content data

(1) Upon an application made under oath and affidavit by a senior officer of the national security agencies or a senior police officer that demonstrates to the satisfaction of a judge that there are reasonable grounds to authorize the interception of content data and associated traffic data, related to or connected with a person or premises under investigation for one of the following purposes:

(a) in the interests of national security;
(b) the prevention or detection of serious offences;
(c) in the interests of the economic well-being of the Gambia, so far as those interests are also relevant to the interests of national security; or
(d) to give effect to a mutual assistance request,

a judge may issue a warrant requiring a service provider, to-

(a) intercept content in real-time; and
(b) provide that content to the authorized officer as soon as reasonably practicable.

Provided that such real-time interception of content data shall not be ordered for a period beyond what is absolutely necessary and in any event not for more than 7 days.

(2) When issuing a warrant under subsection (1), the judge shall be satisfied that:

(a) the extent of interception is commensurate, proportionate and necessary for the purposes of a specific criminal investigation or prosecution;

(b) measures shall be taken to ensure that the data is intercepted whilst maintaining the privacy of other users, customers and third parties and without the disclosure of information and data of any party not part of the investigation; and

(c) the investigation may be frustrated or seriously prejudiced unless the interception is permitted.

(3) When making an application under subsection (1), the officer shall provide the following substantive grounds and reasons also:

(a) explain why it is believed the content data sought will be available with the person in control of the computer system;

(b) identify and explain with specificity the type of content data suspected will be found on such computer system;

(c) identify and explain with specificity the subscribers, users or unique identifier the subject of an investigation or prosecution suspected may be found on such computer system;

(d) identify and explain with specificity the identified offences in respect of which the warrant is sought;

(e) what measures shall be taken to prepare and ensure that the content data will be sought and carried out

(i) whilst maintaining the privacy of other users, customers and third parties; and

(ii) without the disclosure of data of any party not part of the investigation.

(4) The period of real-time interception of content data may be extended beyond 7 day period if, on an application, a judge authorizes an extension for a further specified period of time, not exceeding a further period of seven days.
(5) A 'serious offence' means an offence punishable by imprisonment for a term of five years or more.

(6) A judge shall require the service provider to keep confidential the warrant and execution of any power provided for under this section.

(7) A service provider served with a warrant has a duty to comply, but is not required to take any steps that it is not reasonably practicable to take.

(8) The Minister of Information and Communications Infrastructure may determine that a service provider must implement the capability to allow interception under this section, including specifying the technical requirements and standards for the capability.

(9) Where obligations have been imposed on a service provider under subsection (8), the steps which it is reasonably practicable for the service provider to take include every step which it would have been reasonably practicable for service provider to take if it had complied with its obligations under subsection (6).

(10) A service provider who fails to comply with a warrant shall be liable for a penalty of [….]

17. Expedited preservation of stored computer data

(1) A senior police officer may issue a written notice to a person to preserve specified computer data stored by means of a computer system when satisfied that:

(a) the specified data is reasonably required for the purpose of a criminal investigation; and

(b) there is a risk or vulnerability that the specified data may be modified, lost, destroyed or rendered inaccessible.

(2) A police officer or another authorised person may serve the notice on any person in possession or control of the computer system, requiring the person to expeditiously preserve the specified computer data.

(3) The notice must specify the time period for which the specified computer data is to be preserved and maintained for integrity, up to a maximum period of 90 days. The notice may be renewed once, for up to a further maximum period of 90 days.

(4) A person who is served a notice must keep the notice and all information about it confidential, unless expressly permitted by the senior police officer.

(5) A person served with a notice has a duty to comply as soon as reasonably practicable, but is not required to take any steps that it is not reasonably practicable to take.

(6) A person who fails to comply shall be liable for a penalty of [….]

18. Expedited preservation and partial disclosure of traffic data

(1) Where a senior police officer is satisfied that:

(a) any specified traffic data stored in any computer system or computer data storage medium or by means of a computer system in the possession of or controlled by a service provider is reasonably required for the purposes of a criminal investigation; and
(b) there is a risk or vulnerability that the specified traffic data may be modified, lost, destroyed or rendered inaccessible,

the police officer or another authorised person may, by written order given to the service provider in possession or control of the computer system or computer data storage medium, require the service provider to:

i. undertake expeditious preservation and maintance of integrity of the specified traffic data for a period specified in the notice not exceeding 7 days, regardless of whether one or more service providers were involved in the transmission of that communication; and

ii. disclose sufficient traffic data about any communication to identify-

(a) the service providers; and
(b) the path through which the communication was transmitted.

(2) The period of preservation and maintenance for integrity may be extended beyond 7 days if, on an application by the senior police officer, a judge authorizes an extension for a further specified period of time, provided that any further extensions to the period of preservation and maintenance for integrity shall only be ordered upon satisfaction that:

(a) such extension of preservation is reasonably required for the purposes of an criminal investigation or prosecution;
(b) there is a risk or vulnerability that the specified traffic data may be modified, lost, destroyed or rendered inaccessible; and
(c) the cost of such preservation is not overly burdensome upon the person in possession or control of the computer system.

(3) A service provider who is served a notice must keep the notice and all information about it confidential, unless expressly permitted by the senior police officer or the judge granting authorization under subsection (2).

(4) Service providers shall, under this section:
(a) respond expeditiously to requests for assistance, and
(b) disclose as soon as practicable, a sufficient amount of traffic data to enable a police officer or another authorised person to identify any other service providers involved in the transmission of the communication.

(5) The powers of the police officer or another authorised person under sub-section (1) apply whether there is one or more service provider involved in the transmission of communication which is subject to exercise of powers under this section.

(6) A service provider served with a notice has a duty to comply as soon as reasonably practicable, but is not required to take any steps that it is not reasonably practicable to take.

(7) A service provider who fails to comply shall be liable for a penalty of [….]

19. Production order

(1) Upon an application made under oath and affidavit by a police officer or another authorised person that demonstrates to the satisfaction of a judge that there exist reasonable grounds to believe that:

(a) specified data stored in a computer system or a computer data storage medium in the possession or control of a person in its territory; or
(b) specified subscriber information relating to services offered by a service provider in The Gambia are in that service provider's possession or control which is necessary or desirable for the purposes of any investigation,

the judge may order:

(i) such person in its territory to submit specified computer data in that person's possession or control, which is stored in a computer system or a computer data storage medium; or
(ii) such a service provider offering its services in The Gambia to submit subscriber information relating to such services in that service provider's possession or control.

(2) The judge may also require that the recipient of the order as well as any person in control of the computer system shall keep confidential the existence of the warrant and exercise of power under this section.

(3) A person who fails to comply with an order under this section granted under this section commits an offence and shall be liable to a penalty of imprisonment for a period not exceeding [period], or a fine not exceeding [amount], or both.

(4) When making an application under subsection (1), the police officer or another authorised person shall provide the following substantive grounds and reasons also:

(i) explain why it is believed that the specified computer data sought is likely to be available with the persons mentioned in subparagraph (a) and (b) of subsection (1);

(ii) why the purpose of the investigation may be frustrated or seriously prejudiced unless the specified computer data or the subscriber information, as the case may be, is produced;

(iii) identify and explain with specificity the type of evidence suspected is likely to be produced by the persons mentioned in subparagraph (a) and (b) of subsection (1);

(iv) identify and explain with specificity the subscribers, users or unique identifiers which are the subject of an investigation or prosecution which are believed may be disclosed as a result of the production of the specified computer data;

(v) identify and explain with specificity the identified offence made out in respect of which the production order is sought;

(vi) what measures shall be taken to prepare and ensure that the specified computer data will be produced:

(a) whilst maintaining the privacy of other users, customers and third parties; and

(b) without the disclosure of data of any party which is not part of the investigation; and

(vii) what measures shall be taken to 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;

Part IV - International co-operation

20. General principles relating to international co-operation

(1) The Government may cooperate with any foreign Government, 24/7 network, any foreign agency or any international agency for the purposes of investigations or proceedings concerning offences related to computer systems, electronic communication or data or for the collection of evidence in electronic form of an offence or obtaining expeditious preservation and disclosure of traffic data or data by means of a computer system or real-time collection of traffic data associated with specified communications or interception of content data or any other means, power, function or provisions under this Act.

(2) Subject to the Mutual Assistance in Criminal Matters Act [….], the Government may:

(a) make requests on behalf of The Gambia to a foreign State for mutual assistance in any investigation commenced or proceeding instituted in The Gambia, relating to any serious offence.

(b) in respect of any request from a foreign State for mutual assistance in any investigation commenced or proceeding instituted in that State relating to a serious offence:

(a) grant the request, in whole or in part, on such terms and conditions as he thinks fit;

(b) refuse the request, in whole or in part, on the ground that to grant the request would be likely to prejudice the sovereignty, security of The Gambia or would otherwise be against the public interest;

(c) after consulting with the appropriate authority of the foreign State, postpone the request, in whole or in part on the ground that granting the request immediately would be likely to prejudice the conduct of an investigation or proceeding in The Gambia; or

(d) postpone action on a request if such action would prejudice an investigation or proceeding in The Gambia.

21. Extradition

(1) The offences under Part […..] of this Act are considered extraditable offences under the Extradition Act No. 10, 1986.

22. General principles relating to mutual assistance

(1) The Cybercrime Act should make explicit reference to the Mutual Assistance in Criminal Matters Act [….], and that references in this Part to the 'Minister' should mean the Attorney-General and Minister of Justice.

(2) When The Gambia accedes to the Budapest Convention, the Minister should declare that the Mutual Assistance in Criminal Matters Act [….] is applicable to all parties to the Convention, in accordance with the procedure envisaged under s. 3 of that Act.

(3) That the Minister designates, as soon as possible, a 'Central Authority' for the purposes of mutual assistance.

23. Spontaneous information

(1) The Government may, without prior request, forward to a foreign State information obtained within the framework of its own investigations when it considers that the disclosure of such information might assist the foreign State in initiating or carrying out investigations or proceedings or might lead to a request for co-operation by the foreign state under this law.

(2) Prior to providing such information, the Government may request that it be kept confidential or only used subject to conditions.

(3) If the foreign State cannot comply with such conditions under (2), it shall notify the Government, which shall then determine whether the information should nevertheless be provided.

Recommendation of the Drafting Committee:

Consideration should be given to whether this provision should be included in the Cybercrime Act or, in the alternative, a general provision should be inserted in the *Mutual Assistance in Criminal Matters Act [….]*, which would then be applicable to any criminal offences.

24. Confidentiality and limitation on use

(1) Where the Mutual Assistance in Criminal Matters Act [….] is not applicable to a foreign country, the Government may require any foreign Government, 24/7 network, or any agency to:

(a) keep confidential the contents of any information or material provided by the Government;
(b) only use the contents and any information and material provided by the Government for the purpose of a specified criminal investigation; and
(c) comply with any such other conditions of use as specified by the Government..

(2) Requests on behalf of The Gambia to a foreign country for assistance under this provision shall be made only by or with the authority of the Minister or a judge.

25. Expedited preservation of stored computer data

(1) Subject to any limitations specified at […..], a foreign Government, foreign agency or any international agency may request the Central Authority, or the 24/7 Network, to order or otherwise obtain the expeditious preservation of data stored by means of a computer system, located within the territory of The Gambia or control of the Government and in respect of which the requesting foreign Government, foreign agency or any international agency intends to submit a request for mutual assistance for the search or similar access, seizure or similar securing, or disclosure of the data.

(2) A request for preservation made under sub-section (1) shall specify:

(a) the authority seeking the preservation;
(b) the offence that is the subject of a criminal investigation or proceedings and a brief summary of the related facts;
(c) the stored computer data to be preserved and its relationship to the offence;
(d) any available information identifying the custodian of the stored computer data or the location of the computer system;
(e) the necessity of the preservation; and
(f) that the foreign Government, foreign agency or any international agency intends to submit a request for mutual assistance for the search or similar access, seizure or similar securing, or disclosure of the stored computer data.

(3) Upon receiving the request under this section, the Central Authority shall take all appropriate measures to preserve expeditiously the specified data in accordance with the procedures and powers provided under this Act.

Any preservation effected in response to the request referred to under this section shall be for a period not less than sixty days, in order to enable the foreign Government, foreign agency or any international agency to submit a request for the search or similar access, seizure or similar securing, 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 request.**

26. Expedited disclosure of preserved traffic data

(1) Where during the course of executing a request under Section [….] or otherwise, with respect to a specified communication, the investigating agency discovers that a service provider in another State was involved in the transmission of the communication, the Central Authority, or 24/7 Network, shall expeditiously disclose to the requesting foreign Government, foreign agency or any international agency a sufficient amount of traffic data to identify that service provider and the path through which the communication was transmitted.

27. Mutual assistance regarding accessing of stored computer data

(1) Subject to any limitations specified at […..], a foreign Government, foreign agency or any international agency may request the investigation agency to order or otherwise to search or similarly access, seize or similarly secure, and disclose data stored by means of a computer system located within the territory of The Gambia, including data that has been preserved pursuant to Section [….].

(2) A request for mutual assistance regarding accessing of stored computer data shall as far as practicable:

(a) give the name of the authority conducting the investigation or proceeding to which the request relates;
(b) give a description of the nature of the criminal matter and a statement setting-out a summary of the relevant facts and laws;
(c) give a description of the purpose of the request and of the nature of the assistance being sought;
(d) in the case of a request to restrain or confiscate assets believed on reasonable grounds to be located in the requested State, give details of the offence in question, particulars of any investigation or proceeding commenced in respect of the offence, and be accompanied by a copy of any relevant restraining or confiscation order;
(e) give details of any procedure that the requesting State wishes to be followed by the requested State in giving effect to the request, particularly in the case of a request to take evidence;
(f) include a statement setting-out any wishes of the requesting State concerning any confidentiality relating to the request and the reasons for those wishes;
(g) give details of the period within which the requesting State wishes the request to be complied with;

(h) where applicable, give details of the property, computer, computer system or electronic device to be traced, restrained, seized or confiscated, and of the grounds for believing that the property is believed to be in the requested State;
(i) give details of the stored computer data, data or program to be seized and its relationship to the offence;
(j) give any available information identifying the custodian of the stored computer data or the location of the computer, computer system or electronic device;
(k) include an agreement on the question of the payment of the damages or costs of fulfilling the request; and
(l) give any other information that may assist in giving effect to the request.

(3) Upon receiving the request under this Section, the investigation agency shall take all appropriate measures to obtain necessary authorization including any warrants to execute upon the request in accordance with the procedures and powers provided under this Act.

(4) Upon obtaining necessary authorization including any warrants to execute upon the request, the investigation agency may seek the support and cooperation of the foreign Government, foreign agency or any international agency during the search and seizure.

(5) Upon conducting the search and seizure request the investigation agency shall subject to Section […] provide the results of such search and seizure as well as the electronic or physical evidence so seized to the foreign Government, foreign agency or any international agency.

28. Trans border access to stored computer data with consent or where publicly available

A police officer or another authorised person may, without the authorisation but subject to any applicable provisions of this Act:
(a) access publicly available (open source) stored computer data, regardless of where the data is located geographically; or
(b) access or receive, through a computer system in its territory, stored computer data located in another territory of a state with whom The Gambia has an applicable international agreement, if such police officer or another authorised person obtains the lawful and voluntary consent of the

person who has the lawful authority to disclose the data through that computer system.

29. Mutual assistance regarding the real-time collection of traffic data

(1) Subject to any limitations specified at […..], a foreign Government, foreign agency or any international agency may request the Central Authority to order or otherwise provide assistance in real-time collection of traffic data associated with specified communications in The Gambia transmitted by means of a computer system.

(2) A request for assistance under this section shall so far as practicable specify:

(a) the authority seeking the use of powers under this section;
(b) the offence that is the subject of a criminal investigation or proceedings 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) any further details 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 the request under this section, the Central Authority shall take all appropriate measures to obtain necessary authorization including any warrants to execute upon the request in accordance with the procedures and powers provided under this Act.

(4) Upon obtaining necessary authorization including any warrants to execute upon the request, the Central Authority may seek the support and cooperation of the foreign Government, foreign agency or any international agency during the search and seizure.

(5) Upon conducting the measures under this section the Central Authority shall provide the results of such measures as well as real-time collection of traffic data associated with specified communications to the foreign Government, foreign agency or any international agency.

30. Mutual assistance regarding the interception of content data

(1) Subject to any limitations specified at […..], a foreign Government, foreign agency or any international agency may request the Central Authority to order or otherwise provide assistance in the real-time collection or recording of content data of specified communications transmitted by means of a computer system in the territory of The Gambia transmitted by means of a computer system.

(2) A request for assistance under this section shall so far as practicable specify:

(a) the authority seeking the use of powers under this section;
(b) the offence that is the subject of a criminal investigation or proceedings and a brief summary of the related facts;
(c) the name of the authority with access to the relevant communication;
(d) the location at which or nature of the communication;
(e) the intended purpose for the required communication;
(f) sufficient information to identify the communications;
(g) details of the data of the relevant interception;
(h) the recipient of the communication;
(i) the intended duration for the use of the communication;
(j) the necessity for use of powers under this section; and
(k) the terms for the use and disclosure of the communication to third parties.

(3) Upon receiving the request under this section, the Central Authority shall, if the request is in relation to an offence punishable with at least five years imprisonment, take all appropriate measures to obtain necessary authorization including any warrants to execute upon the request in accordance with the procedures and powers provided under this Act.

(4) Upon obtaining necessary authorization including any warrants to execute upon the request, the Central Authority may seek the support and cooperation of the foreign Government, foreign agency or any international agency during the search and seizure.

(5) Upon conducting the measures under this section the Central Authority shall provide the results of such measures as well as real-time collection or recording of content data of specified communications to the foreign Government, foreign agency or any international agency.

31. 24/7 Network

(1) The Minister shall designate a point of contact available on a twenty-four hour, seven-day-a-week basis, in order to ensure the provision of immediate assistance for the purpose of investigations or proceedings concerning criminal offences related to computer systems and data, or for the collection of evidence in electronic form of a criminal offence, which assistance shall include facilitating, or, if permitted by law and practice of The Gambia, directly carrying out the following measures:

(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;
(c) the collection of evidence, the provision of legal information, and locating of suspects

within expeditious timelines to be defined by regulations under [….].

(2) The point of contact shall be resourced with and possess the requisite capacity to securely and efficiently carry out communications with other points of contact in other territories, on an expedited basis.

(3) The point of contact shall have the authority and be empowered to coordinate and enable access to international mutual assistance under this Act or if applicable extradition procedures, upon an expedited basis.

Part V – Miscellaneous Provisions

32. Regulations

The Minister may make regulations for the better carrying out of the Act.

33. Repeal and savings

Sections ……are hereby repeal from the Information and Communication Act 20….

CYBERCRIME BILL 2019

Object and reasons