CYBERCRIME AND COMPUTER RELATED CRIMES ACT, 2018

No. 18 **of 2018**

ARRANGEMENT OF SECTIONS

SECTION

PART I — *Preliminary*

1. Short title and commencement
2. Interpretation
3. Jurisdiction

PART II — *Offences*

4. Unauthorised access to a computer or computer system
5. Unauthorised access to a computer service
6. Access with intent to commit or facilitate commission of an offence
7. Unauthorised interference with data
8. Unauthorised interference with a computer or computer system
9. Unlawful interception of data
10. Unlawful possession of devices or data
11. Unauthorised disclosure of password or access code
12. Damage to a computer or computer system
13. Critical national infrastructure
14. Cyber extortion
15. Cyber fraud
16. Cyber harassment
17. Cyber stalking
18. Offensive electronic communication
19. Pornographic or obscene material
20. Revenge pornography
21. Racist or xenophobic material
22. Racist or xenophobic motivated insult
23. Unlawful disclosure by service provider

PART III — *Procedural Powers*

24. Preservation order
25. Disclosure of preserved data
26. Production order

27. Access, search and seizure
28. Real time collection of content or traffic data
29. Deletion order
30. Acting without an order
31. Limited use of disclosed data and information
32. Non-compliance with order or notice

PART IV — *Miscellaneous Provisions*

33. Extradition
34. Regulations
35. Repeal of Cap. 08:06
36. Savings

An Act to repeal and re-enact, with amendments, the Cybercrime and Computer Related Crimes Act.

Date of Assent: 29.06.18

Date of Commencement: ON NOTICE

ENACTED by the Parliament of Botswana.

PART I — *Preliminary*

Short title and commencement

1. This Act may be cited as the Cybercrime and Computer Related Crimes Act, 2018, and shall come into operation on such day as the Minister may, by Order published in the *Gazette*, appoint.

Interpretation

2. In this Act, unless the context otherwise requires —

"access" means, in relation to any computer or computer system, to instruct, communicate with, store data in, retrieve data from, or otherwise make use of any of the resources of the computer or computer system

"access code" or "password" means any —

(*a*) data by which a computer service or computer or computer system is capable of being obtained, accessed or used; or

(*b*) means of gaining access to the whole or part of a computer or computer system;

"automatic processing" includes the following operations, if carried out in whole or in part by automated means —

(*a*) the storage of data;

(*b*) the carrying out of logical or arithmetical operations on the data referred to in paragraph (*a*), including its alteration, era sure, retrieval or dissemination;

"Commissioner" means the Commissioner of Police appointed by the President in terms of section 112 of the Constitution;

"computer data storage medium" means any device, article or material from which data or information is capable of being stored or reproduced, with or without the aid of any other device or material;

"computer or computer system" means an electronic, magnetic or optical device or a group of interconnected or related devices, including the Internet, one or more of which, pursuant to a programme, performs the automatic processing of data;

"computer service" includes data processing or the storage or retrieval of data;

"data" means —

(*a*) any representation of facts, information or concepts in a form suitable for processing in a computer or computer system;

(*b*) any information recorded in a form in which it can be processed by equipment operating automatically in response to instructions given for that purpose; or

(*c*) any programme suitable to cause a computer or computer system to perform a function,

and includes traffic data and subscriber information;

"device" includes —

(*a*) a computer programme, code, software or application;

(*b*) a component of a computer or computer system, such as a graphic card, memory card, chip or processor;

(*c*) a computer data storage medium; or

(*d*) any input or output device;

"Director-General" means the Director-General of the Directorate on Corruption and Economic Crime appointed by the President in terms of section 4 of the Corruption and Economic Crime Act; Cap. 08:05

"electronic communication" means the transfer of a sign, signal or data of any nature transmitted in whole or in part by an electrical, digital, magnetic, electromagnetic, optical, wire, wireless, radio, photo electronic or photo optical system or any other similar form;

"function" includes the logic, control, arithmetic, deletion, storage and retrieval, and communication and telecommunication to, from or within a computer or computer system;

"funds" means assets of every kind, whether corporeal or incorporeal, tangible or intangible, movable or immovable, however acquired, and legal documents in any form, including electronic or digital, evidencing title to or interest in such assets;

"hinder" in relation to a computer or computer system includes —

(*a*) cutting the electricity supply to a computer or computer system;

(*b*) causing electromagnetic interference to a computer or computer system;

(*c*) corrupting a computer or computer system by any means;

(*d*) inputting, transmitting, damaging, deleting, suppressing, altering or modifying data; and

(*e*) impairing, by any means, the connectivity, infrastructure or support of a computer or computer system;

"information and communication service" means any service involving the use of information and communication technology, including telecommunication services;

"information and communication technology" means any technology employed in the collecting, storing, using or sending out of information, including any technology involving the use of a computer or computer system or a telecommunication system;

"intercept" means the aural or other acquisition of the contents of any electronic, magnetic, optical or oral data communication during transmission, through the use of any device;

"interfere" or "interference" includes —

(*a*) an action carried out by a person who is not himself or herself entitled to determine whether the interference of the kind in question should be made; or

(*b*) an action carried out by a person whose act causes the interference does not have consent, from any person who is so entitled, to the interference of the kind in question; and

(*c*) where the act in question, or any intended effect of it, is temporary or permanent;

"national emergency organisations" include the police service, security forces, fire brigade, ambulance services, medical services, veterinary services and environmental disaster agencies, whether or not such organisations are owned and managed on a private or public basis;

"programme" means an instruction or a set of instructions, expressed in words, codes, schemes or any other form, which is capable, when incorporated in a machine-readable medium, of causing a computer or computer system to achieve a particular task, result or function;

"property" means money or any other movable, immovable, corporeal or incorporeal thing, whether located in Botswana or elsewhere, and includes any rights, securities and any interest in privileges and claims over that thing, as well as —

(*a*) any currency, whether or not the currency is legal tender in Botswana, and any bill, security, bond, negotiable instrument or any instrument capable of being negotiated which is payable to the bearer or endorsed "payable to the bearer", whether expressed in Botswana currency or otherwise;

(*b*) any balance held in Botswana currency or in any other currency in accounts with any bank which carries on business in Botswana or elsewhere;

(*c*) any balance held in any currency with a bank outside Botswana;

(*d*) any motor vehicle, ship, aircraft, boat, work of art, jewelry, precious metal or any other item of value;

(*e*) any right or interest in property;

(*f*) any funds or other assets, including all property and any interest, dividend or income on or value accruing to or generated by such funds or assets; and

(*g*) any information, including an electronically produced programme or data or copy thereof, whether tangible or intangible, human or computer-readable data, or data in transit;

"publish" includes —

(*a*) distributing, transmitting, disseminating, circulating, delivering, exhibiting, lending for gain, exchanging, bartering, selling or offering for sale, letting on hire or offering to let on hire, offering in any other way, or making available in any way;

(*b*) having in possession or custody, or under control, for the purpose of doing an act referred to in paragraph (*a*); or

(*c*) printing, photographing, copying or making in any other manner, whether of the same or of a different kind of nature, for the purpose of doing any act referred to in paragraph (*a*);

"racist or xenophobic material" means any material which advocates, promotes or incites hatred, discrimination or violence against any person or group of persons based on race, colour, descent, nationality, ethnic origin, tribe or religion;

"repealed Act" means the Cybercrime and Computer Related Crimes Act repealed under section 35;

"service provider" means any public or private person who —

(*a*) provides to users of its services the ability to communicate by means of a computer or computer system;

(*b*) processes or stores computer data on its behalf or on behalf of the users of its services; or

(*c*) provides an information and communication service, including telecommunication;

"subscriber" means a person who lawfully uses the services of a service provider;

"subscriber information" means any information, other than traffic data, contained in the form of computer data or any other form, that is held by a service provider and relating to any subscriber, by which can be established information available on the basis of a service agreement or arrangement, including information on the —

(*a*) site of installation of communication equipment; or

(*b*) subscriber's identity, postal or geographical address or billing or payment information;

"telecommunication" means a transmission, emission or reception of signs, signals, writing, images, sounds or intelligence of any nature, by wire, radio, optical or other electromagnetic systems, whether or not such signs, signals, writing, images, sounds or intelligence have been subjected to rearrangement, computation or other processes, by any means, in the course of their transmission, emission or reception;

"traffic data" means any data that —

(*a*) relates to communication by means of a computer or computer system;

(*b*) is generated by a computer or computer system that is part of the chain of communication; and

(*c*) shows the communication's origin, destination, route, time, data, size, duration or type of underlying service;

"unauthorised access" includes where a person —

(*a*) is not himself or herself entitled to access of the kind in question;

(*b*) does not have consent, from any person who is so entitled, to access of the kind in question; or

(*c*) exceeds the access he or she is authorised; and

"underlying service" means the type of service that is being used within a computer or computer system.

Jurisdiction

3. The courts of Botswana shall have jurisdiction where an act or an omission constituting an offence under this Act has been committed —

(*a*) in the territory of Botswana;

(*b*) by a national of Botswana outside the territory of Botswana, if the person's conduct would also constitute an offence under the law of the country where the offence was committed and if the person has not been prosecuted for the offence in that country;

(*c*) on a ship or aircraft registered in Botswana;

(*d*) in part in Botswana; or

(*e*) outside the territory of Botswana and where any result of the offence has an effect in Botswana.

PART II — *Offences*

Unauthorised access to a computer or computer system

4. (1) Subject to subsection (2), any person who —

(*a*) intentionally accesses or attempts to access the whole or any part of a computer or computer system knowing that the access he or she intends to secure is unauthorised; or

(*b*) causes a computer or computer system to perform any function as a result of unauthorised access to such system,

commits an offence and is liable to a fine not exceeding P20 000 or to imprisonment for a term not exceeding one year, or to both.

(2) For the purposes of this section, it is immaterial that the unauthorised access is not directed at a —

(*a*) particular programme or data;

(*b*) programme or data of any kind; or

(*c*) programme or data held in any particular computer or computer system.

Unauthorised access to a computer service

5. (1) Subject to subsection (4), a person commits an offence where such person knowingly and by any means, without authorisation or exceeding the authorisation he or she is given —

(*a*) secures access or intends to secure access to any computer or computer system for the purpose of obtaining, directly or indirectly, any computer service; or

(*b*) intercepts , intends to access or causes to be intercepted, directly or indirectly, any function of, or any data within, a computer or computer system.

(2) For the purposes of this section —

(*a*) "authorisation" includes, in relation to a function of a computer or computer system, listening to or recording a function of a computer or computer system or acquiring the substance, meaning or purport of such a function; and

(*b*) it is immaterial that the unauthorised access or interception in subsection (1) is not directed at a —

(*i*) particular programme or data,

(*ii*) programme or data of any kind, or

(*iii*) programme or data held in any particular computer or computer system.

(3) A person who commits an offence under subsection (1) is liable to a fine not exceeding P40 000 or to imprisonment for a term not exceeding two years, or to both.

(4) A person shall not be liable under subsection (1) where he or she —

(*a*) has the express or implied consent of both the person who sent the data and the intended recipient of such data; or

(*b*) is acting in reliance of a statutory power arising under an enactment or a power conferred under any Act.

Access with intent to commit or facilitate commission of an offence

6. (1) A person who, with intent to commit an offence, causes a computer or computer system to perform any function for the purpose of securing access to —

(*a*) any programme or data held in a computer or computer system; or

(*b*) a computer service,

commits an offence and is liable to a fine not exceeding P20 000 or to imprisonment for a term not exceeding one year, or to both.

(2) For the purposes of this section it is immaterial that —

(*a*) the offence facilitated under paragraph (b) is committed by a person referred to under subsection (1) or any other person; or

(*b*) the act is committed on the same occasion as when the access is secured or at any other time.

Unauthorised interference with data

7. (1) A person who intentionally and without lawful excuse or justification, does or attempts to do any of the following acts —

(*a*) damages, deteriorates, deletes, alters or modifies computer data;

(*b*) renders computer data meaningless, useless or ineffective;

(*c*) obstructs, interrupts or interferes with the lawful use of computer data; or

(*d*) denies access to computer data to any person entitled to it,

commits an offence and is liable to a fine not exceeding P40 000 or to imprisonment for a term not exceeding two years, or to both.

(2) Where, as a result of the commission of an offence under subsection (1), the following is impaired, suppressed, altered or modified —

(*a*) the operation of a computer or computer system;

(*b*) access to any programme or data held in any computer or computer system; or

(*c*) the operation of any programme or the reliability of any data,

the person is liable to a fine not exceeding P20 000 or to imprisonment for a term not exceeding one year, or to both.

Unauthorised interference with a computer or computer system

8. (1) A person who intentionally, without lawful excuse or justification —

(*a*) hinders or interferes with the functioning of a computer or computer system; or

(*b*) hinders or interferes with a person who is lawfully using or operating a computer or computer system,

commits an offence and is liable to a fine not exceeding P10 000 or to imprisonment for a term not exceeding six months, or to both.

(2) A person who intentionally, without lawful excuse or justification, commits an act which causes, directly or indirectly —

(*a*) a denial, including a partial denial, of access to a computer or computer system; or

(*b*) an impairment of any programme or data stored in a computer or computer system,

commits an offence and is liable to a minimum fine of P40 000 or to imprisonment for a minimum term of two years, or to both.

Unlawful interception of data

9. A person who intentionally, without lawful excuse or justification, and by technical means, intercepts —

(*a*) any non-public transmission to, from or within a computer or computer system; or

(*b*) any electromagnetic emissions that are carrying data from a computer or computer system,

commits an offence and is liable to a fine not exceeding P40 000 or to imprisonment for a term not exceeding two years, or to both.

Unlawful possession of devices or data

10. (1) A person who intentionally, without lawful excuse or justification, manufactures, sells, procures for use, imports, exports, distributes or otherwise makes available, a computer or computer system or any other device, designed or adapted for the purpose of committing an offence under this Act, commits an offence and is liable to a fine of P40 000 or to imprisonment for a term of two years, or to both.

(2) A person who intentionally, without lawful excuse or justification, receives, or is in possession of, one or more of the devices under subsection (1), commits an offence and is liable to a fine of P40 000 or to imprisonment for a term of two years, or to both.

(3) A person who is found in possession of any data or programme with the intention that the data or programme be used, by the person himself or herself or by another person, to commit or facilitate the commission of an offence under this Act, commits an offence and is liable to a fine of P40 000 or to imprisonment for a term of two years, or to both.

(4) For the purposes of subsection (3), "possession of any data or programme" includes having —

(*a*) possession of a computer or computer system or data storage device that holds or contains the data or programme;

(*b*) possession of a document in which the data or programme is recorded; and

(*c*) control of the data or programme that is in the possession of another person.

Unauthorised disclosure of password or access code

11. A person who intentionally, without lawful excuse or justification, discloses, sells, procures for use, distributes or otherwise makes available, any password, access code or other means of gaining access to the whole or part of a computer or computer system —

(*a*) for wrongful gain;

(*b*) for any unlawful purpose;

(*c*) to overcome security measures for the protection of data; or

(*d*) with the knowledge that it is likely to cause prejudice to any person,

commits an offence and is liable to a fine not exceeding P10 000 or to imprisonment for a term not exceeding six months, or to both.

Damage to a computer or computer system

12. (1) In this section, "computer contaminant" includes any programme which —

(*a*) modifies, destroys, records or transmits any data or programme residing within a computer or computer system;

(*b*) usurps the normal operation of a computer or computer system; or

(*c*) destroys, damages, degrades or adversely affects the performance of a computer or computer system or attaches itself to another computer resource and operates when a programme, data or instruction is executed or some other event takes place in that computer or computer system.

(2) A person who intentionally introduces, or causes to be introduced, a computer contaminant into any computer or computer system which causes, or is capable of causing, any of the effects referred to under subsection (1) to such computer or computer system, commits an offence and is liable to a fine not exceeding P100 000 or to imprisonment for a term not exceeding five years, or to both.

Critical national infrastructure

13. (1) In this section, "critical national infrastructure" means computer systems, devices, networks, programmes or data, including those of national emergency organisations, so vital to Botswana that the incapacity or destruction of, or the interference with, such systems and assets would have a debilitating impact on national security, national economic security, public health and safety or a combination of any of these.

(2) Where a person obtains access to critical national infrastructure in the course of the commission of an offence under this Act, the person commits an offence and is liable to a fine not exceeding P100 000 or to imprisonment for a term not exceeding five years, or to both.

(3) For the purposes of any prosecution under this section, it shall be presumed, until the contrary is proved, that the person referred to under subsection (2) knew that the computer formed part of critical national infrastructure.

Cyber extortion

14. A person who performs or threatens to perform any of the acts described under this Part, for the purposes of obtaining any unlawful advantage by —

(*a*) undertaking to cease or desist from such actions; or

(*b*) undertaking to restore any damage caused as a result of those actions,

commits an offence and is liable to a fine not exceeding P20 000 or to imprisonment for a term not exceeding 10 years, or to both.

Cyber fraud

15. (1) A person who performs any of the acts described under this Part, for purposes of obtaining any unlawful advantage by causing forged data to be produced, with the intent that it be considered or acted upon as if it were authentic, commits an offence and is liable to a fine not exceeding P100 000 or to imprisonment for a term not exceeding seven years, or to both.

(2) A person who, with intent to procure any advantage for himself or herself or another person, fraudulently causes loss of property to another person by —

(*a*) any input, alteration, deletion, delaying transmission or suppression of data; or

(*b*) any interference with the functioning of a computer or computer system,

commits an offence and is liable to a fine not exceeding P100 000 or to imprisonment for a term not exceeding seven years, or to both.

Cyber harassment

16. A person who uses a computer or computer system, or who knowingly permits a device to be used, for any of the following purposes —

(*a*) making any request, suggestion or proposal which is obscene, lewd, lascivious or indecent; or

(*b*) threatening to inflict injury or physical harm to the person or property of any person,

commits an offence and is liable to a fine not exceeding P10 000 or to imprisonment for a term not exceeding six months, or to both.

Cyber stalking

17. A person who willfully, maliciously or repeatedly uses electronic communication to harass another person, or makes a threat with the intent to place that person in reasonable fear for his or her safety or for the safety of his or her immediate family, commits an offence and is liable to a fine not exceeding P20 000 or to imprisonment for a term not exceeding one year, or to both.

Offensive electronic communication

18. A person who willfully, maliciously or repeatedly uses electronic communication of an offensive nature to disturb or attempt to disturb the peace, quiet or privacy of any person with no purpose to legitimate communication, whether or not a conversation ensues, commits an offence and is liable to a fine not exceeding P20 000 or to imprisonment for a term not exceeding one year, or to both.

Pornographic or obscene material

19. (1) In this section —

(*a*) "child" means a person who is under the age of 18 years;

(*b*) "child pornography" includes material that visually or otherwise depicts —

(i) a child engaged in sexually explicit conduct,

(ii) a person who appears to be a child engaged in sexually explicit conduct, or

(iii) realistic images representing a child engaged in sexually explicit conduct; and

(*c*) "sexually explicit conduct" means any conduct, whether real or simulated, which involves —

(i) sexual intercourse, including genital-genital, oral-genital, anal genital or oral-anal, between children, or between an adult and a child, of the same or opposite sex,

(ii) bestiality,

(iii) masturbation,

(iv) sadistic or masochistic sexual abuse, or

(v) the exhibition of the genitals or pubic area of a child.

(2) A person who —

(*a*) publishes child pornography or obscene material relating to children through a computer or computer system;

(*b*) produces child pornography or obscene material relating to children for the purpose of its publication through a computer or computer system;

(*c*) possesses child pornography or obscene material relating to children in a computer or computer system or on a computer data storage medium;

(*d*) publishes or causes to be published an advertisement likely to be understood as conveying that the advertiser distributes or shows child pornography or obscene material relating to children; or

(*e*) accesses child pornography or obscene material relating to children through a computer or computer system,

commits an offence and is liable to a fine not exceeding P100 000, or to imprisonment for a term not exceeding five years, or to both.

(3) A person who, by means of a computer or computer system, communicates with a person who is, or who the accused believes is —

(*a*) under the age of 18 years, for the purpose of facilitating the commission of the offence of child pornography under this Act, or the offences of prostitution, rape or indecent assault under the Penal Code; Cap. 08:01

(*b*) under the age of 16 years, for the purpose of facilitating the commission of the offences of abduction or kidnapping of that person under the Penal Code; or

(*c*) under the age of 16 years, for the purpose of facilitating the commission of the offence of defilement or any sexual offence of that person under the Penal Code,

commits an offence and is liable to a fine not exceeding P100 000 or to imprisonment for a term not exceeding five years, or to both.

(4) Evidence that the person in paragraph (*a*), (*b*) or (*c*) of subsection (3) was represented to the accused as being under the age of 18 years or 16 years, as the case may be, shall be, in absence of evidence to the contrary, proof that the accused believed that the person was under that age.

(5) It shall not be a defence to a charge under subsection (3) that the accused believed that the person he or she was communicating with was at least 16 or 18 years of age, as the case may be, unless the accused took reasonable steps to ascertain the age of the person.

(6) For the purposes of subsection (3), it does not matter that the person in paragraph (*a*), (*b*) or (*c*) of subsection (3) is a fictitious person, represented to the accused as a real person.

Revenge pornography

20. A person who, by means of a computer or computer system, discloses or publishes a private sexual photograph or film without the consent of the person who appears in the photograph or film, and with the intention of causing that person distress, commits an offence and is liable to a fine not exceeding P40 000 or to imprisonment for a term not exceeding two years, or to both.

Racist or xenophobic material

21. A person who, by means of a computer or computer system —

(*a*) produces racist or xenophobic material;

(*b*) offers or makes available racist or xenophobic material;

(*c*) distributes or transmits racist or xenophobic material,

commits an offence and is liable to a fine not exceeding P40 000 or to imprisonment for a term not exceeding two years, or to both.

Racist or xenophobic motivated insult

22. A person who, by means of a computer or computer system, insults another person on the basis of race, colour, descent, nationality, ethnic origin, tribe or religion commits an offence and is liable to a fine not exceeding P40 000 or to imprisonment for a term not exceeding two years, or to both.

Unlawful disclosure by service provider

23. A service provider who, without lawful authority, discloses —

(*a*) that an order under this Act has been made;

(*b*) any act done under an order; or

(*c*) any data collected or recorded under an order,

commits an offence and is liable to a minimum fine of P1 000 000 but not exceeding P5 000 000.

PART III — *Procedural Powers*

Preservation order

24. A police officer or any person authorised by the Commissioner or by the Director-General, in writing, may, upon confirmation by the court and as soon as reasonably practicable to do so, order for the preservation of data that has been stored or processed by means of a computer or computer system or any other information and communication technology, where there are reasonable grounds to believe that such data is vulnerable to loss or modification.

Disclosure of preserved data

25. A police officer or any person authorised by the Commissioner or by the Director-General, in writing, may, by written notice given to a person in control of a computer or computer system, require the person to —

(*a*) ensure that the data specified in the notice is preserved for the period specified in the notice; or

(*b*) disclose sufficient traffic data about a specified communication to identify the service provider or the path through which the data was transmitted.

Production order

26. (1) A police officer or any person authorised by the Commissioner or by the Director-General, in writing, may apply to a judicial officer for an order compelling —

(*a*) a person to submit specified data in that person's possession or control, which is stored in a computer or computer system; and

(*b*) a service provider to submit subscriber information in relation to its services in that service provider's possession or control.

(2) Where the data in subsection (1) consists of data stored in an electronic, magnetic or optical form on a device, the request shall be deemed to require the person to produce or give access to it in a form in which it can be taken away and in which it is visible and legible.

Access, search and seizure

27. (1) Where a police officer, or any person authorised by the Commissioner or by the Director-General, in writing, has reasonable grounds to believe that stored data or information would be relevant for the purposes of an investigation or the prosecution of an offence, he or she may apply to a judicial officer for the issue of an order to enter any premises to access, search and seize such data or information.

(2) A police officer or any person authorised by the Commissioner or by the Director-General, in writing, in the execution of an order issued under subsection (1), shall —

(*a*) seize or secure a computer or computer system or any information and communication technology medium;

(*b*) make and retain a copy of such data or information;

(*c*) maintain the integrity of the relevant stored data or information;

(*d*) print, photograph, copy or make in any other manner for the purpose of doing an act referred to in paragraph (a); or

(*e*) render inaccessible or remove the stored data or information from the computer or computer system, or any information and communication technology medium.

(3) A police officer or any person authorised by the Commissioner or Director-General, in writing, in the execution of an order issued under subsection (1), may order any person who has knowledge about the functioning of the computer system or the measures provided under subsection (2) to protect the data contained therein in order to provide, as is reasonable, the necessary information to enable the undertaking of the measures provided under subsection (2).

Real time collection of content or traffic data

28. A police officer or any person authorised by the Commissioner or by the Director-General, in writing, may apply to a judicial officer, ex-parte, for an order —

(*a*) for the collection or recording of content or traffic data, in real time, associated with specified communications transmitted by means of a computer or computer system; or

(*b*) compelling a service provider, within its technical capabilities, to —

(i) effect such collection and recording referred to in paragraph (a), or

(ii) assist the person making the application to effect such collection and recording.

Deletion order

29. The Director of Public Prosecutions, or any person authorised by him or her, in writing, may apply to a judicial officer for an order that data in a computer or computer system or other information communication technology medium which contains pornography, obscene material or child pornography be —

(*a*) no longer stored on and made available through the computer or computer system or any other medium; or

(*b*) deleted or destroyed.

Acting without an order

30. A police officer of the rank of sergeant or above such rank may carry out the powers conferred on him or her under this Act without applying for an order under this Act if such application would result in an undue delay in the investigation of any offence under this Act.

Limited use of disclosed data and information

31. (1) Data obtained under this Act by a police officer, or any person authorised by the Commissioner or by the Director-General, in writing, shall be used for the purpose for which the data was originally sought, unless such data is sought in —

(*a*) accordance with any other enactment;

(*b*) compliance with an order of court;

(*c*) the prevention of injury or other damage to the health of a person or serious loss of or damage to property; or

(*d*) the public interest.

(2) Subject to subsection (3), on receipt of a request, in writing, a police officer or any person authorised by the Commissioner or by the Director-General shall permit a person who had the custody or control of a computer or computer system to access and copy computer data on the computer or computer system.

(3) A police officer or any person authorised by the Commissioner or by the Director-General, in writing, may refuse to give access to computer data or provide copies of such computer data if he or she has reasonable grounds for believing that the giving of access or the provision of copies —

(*a*) would constitute a criminal offence; or

(*b*) would prejudice —

(i) the investigation in connection with which the search was carried out,

(ii) another ongoing investigation, or

(iii) any criminal proceedings that are pending or that may be brought in relation to any of those investigations.

Non-compliance with order or notice

32. A person who fails to comply with an order or notice issued under this Part commits an offence and is liable to a fine not exceeding P20 000 or to imprisonment for a term not exceeding one year, or to both.

PART IV — *Miscellaneous Provisions*

Extradition

Cap. 08:06

33. An offence under this Act shall be considered to be an extraditable crime for which extradition may be granted or obtained under the Extradition Act.

Regulations

34. The Minister may make regulations for the better carrying out of the provisions and purposes of this Act.

Repeal of Cap. 08:06

35. The Cybercrime and Computer Related Crimes Act is hereby repealed.

Savings

36. Notwithstanding the repeal effected under section 35 —

(*a*) anything made, given, issued or done under the repealed Act shall have the same effect as if it was made, given, issued or done under this Act;

(*b*) any application made to a court under the repealed Act shall continue to be dealt with and determined as if it was made under this Act; and

(*c*) any legal proceedings which, before the coming into operation of this Act, were pending shall be continued or enforced in the same manner as they would have continued or were enforced before the coming into operation of this Act.

PASSED by the National Assembly this 12th day of April, 2018.

BARBARA N. DITHAPO,
Clerk of the National Assembly.