CYBERCRIME AND OTHER RELATED CRIMES (AMENDMENT) BILL, 2025

(Bill No. 22 of 2025)

EXPLANATORY STATEMENT OF OBJECTS AND REASONS

The object of this Bill is to amend the Cybercrime and other related Crimes Act 2021, to ensure it is aligned with the Budapest Convention and effectively addresses cyber threats and promotes cybersecurity. The proposed amendments aim to make necessary changes to the Act so as to provide more consistency throughout the Act and to allow for international cooperation which is instrumental in cybercrime considering its cross-border nature.

Dated this 21st day of November, 2025.

SEBASTIEN PILLAY
VICE-PRESIDENT/MINISTER OF INFORMATION, COMMUNICATIONS TECHNOLOGY

CYBERCRIME AND OTHER RELATED CRIMES (AMENDMENT) BILL, 2025

(Bill No. 22 of 2025)

ARRANGEMENT OF SECTIONS

SECTIONS

CYBERCRIME AND OTHER RELATED CRIMES (AMENDMENT) BILL, 2025

(Bill No. 22 of 2025)

A BILL

FOR

AN ACT TO AMEND THE CYBERCRIME AND OTHER RELATED CRIMES ACT, 2021.

ENACTED BY THE PRESIDENT AND THE NATIONAL ASSEMBLY

Short title

1. This Act may be cited as the Cybercrime and Other Related Crimes (Amendment) Act, 2025.

Amendment of Arrangement of sections

2. The Arrangement of sections of the Cybercrime and Other Related Crimes Act, 2021, in this Act referred to as the "principal Act" is amended—

(a) in the section heading of section 5 by repealing the words "criminal intent" and substituting them with the words "intent to commit an offence";

(b) in the section heading of section 18 by repealing the words "Pornographic publication" and substituting them with the words "Revenge pornography";

(c) in the section heading of section 21 by repealing the words "Declaration of preserved computer data" and substituting them with the words "Partial disclosure of traffic data".

Amendment of section 2

3. Section 2 of the principal Act is amended—

(a) by repealing the definition of "seize" and substituting it with the following definition —

""seize" means the securing of a computer system or part of it or a computer-data storage medium and includes—

(a) making and retaining a copy of that computer data, including by using on-site equipment;

(b) taking a printout of output of computer data;

(c) maintaining the integrity of the relevant stored computer data; and

(d) rendering inaccessible or removing that computer data in the accessed computer system."

(b) by inserting in their proper alphabetical order, the following new definitions —

""content data" means

(a) the meaning or purport of the communication; or

(b) the message or information being conveyed by the communication;

and includes everything transmitted as part of communication that is not traffic data.

"function of a computer" means any operation or activity or task being performed by the computer, including, but not limited to, storing of data, processing of data, communications on network etc.;

"interception" in relation to a function of a computer, includes to monitor, or record a function of a computer, or acquire the substance, its meaning or purport of such function;

"legitimate communication" means communication which is lawful and intended for social or professional purposes;

"standard scale" means the standard scale of fines for offences established under the Criminal Offences (Standard Scale of Fines) Act, 2021;

"subscriber information" means any information contained in the form of computer data or any other form that is held by an electronic service provider, relating to subscribers of its services other than traffic or content data and by which can be established —

(a) the type of electronic communication service used, the technical provisions taken thereto and the period of service;

(b) the subscriber's identity, postal or geographic address, telephone and other access number, billing and payment information, available on the basis of the service agreement or arrangement; and

(c) any other information on the site of the installation of electronic communication equipment, available on the basis of the service agreement or arrangement.

"substance" means the actual data being handled by the computer in performing the different functions and may include but is not limited to the data that is stored, processed, transmitted etc.;

"without authorisation" in relation to a computer system or computer data, means,—

(a) access by a person to a computer system or computer data where such person —

(i) is not entitled to control access of the kind in question; and

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

(b) an act done, by a person in relation to a computer system or computer data, where such person —

(i) is not responsible for the computer system or computer data and is not entitled to determine whether the act may be done; and

(ii) does not have consent to do the act in question from any person who is so entitled.".

Amendment of section 3

4. Section 3 of the principal Act is amended—

(a) in paragraph (c) by repealing the word "and";

(b) in paragraph (d) by repealing the full stop, (".") and substituting it with the mark and word "; and";

(c) by inserting after paragraph (d), a new paragraph (e), as follows—

"(e) committed outside the territory of Seychelles if the act is carried out by a citizen of Seychelles and is punishable under criminal law where it was committed" .

Amendment of section 5

5. Section 5 of the principal Act is amended —

(a) in the section heading by repealing the words "criminal intent" and substituting them with the words "intent to commit an offence";

(b) in subsection (1) by repealing the words "criminal intent" and substituting them with the words "intent to commit an offence".

Amendment of section 6

6. Section 6 of the principal Act is amended —

(a) in subsection (1) by repealing paragraph (a), and substituting it with the following paragraph —

"(a) intentionally and without authorisation intercepts or causes to be intercepted any function or non-public transmission of computer data, to, from or within, a computer system including electromagnetic emissions from a computer system carrying such computer data and does so by technical means; or";

(b) by repealing subsection (2), and substituting it with the following new subsection —

"(2) For the purposes of subsection (1), intercepting by technical means relates to listening to, recording, monitoring or surveillance of the content of communications, to the procuring of the content of data either directly, through access and use of the computer system, or indirectly, through the use of electronic eavesdropping or tapping devices.".

Amendment of section 7

7. Section 7 of the principal Act is amended in subsection (1) —

(a) in the chapeau, by repealing the word "authority" and substituting it with the word "authorisation";

(b) by repealing paragraph (a), and substituting it with the following paragraph —

"(a) damages, deletes, deteriorates, alters, suppresses or destroys computer data;"

(c) by repealing paragraph (e).

Amendment of section 8

8. Section 8 of the principal Act is amended —

(a) by repealing subsection (1) and substituting with the following subsection —

"(1) A person who intentionally, whether directly or indirectly, and without authorisation interferes with, or interrupts or obstructs the use of a computer system commits an offence and shall, on conviction, be liable to a fine of level 5 on the standard scale or to imprisonment for a term not exceeding 20 years or to both."

(b) in subsection (2) —

(i) by repealing paragraph (a);

(ii) by renumbering the remaining paragraphs accordingly;

(iii) in the existing paragraph (c), by inserting after the word "deleting" a comma (",") and the words ", transmitting, damaging, deteriorating, suppressing".

Amendment of section 9

9. Section 9 of the principal Act is amended in paragraph (a) —

(a) in the chapeau, by repealing the word "justification" and substituting it with the word "authorisation";

(b) in subparagraph (i) by inserting after the word "adapted", the word "primarily".

Amendment of section 10

10. Section 10 of the principal Act is amended in the chapeau by repealing the word "right" and substituting it with the word "authorisation".

Amendment of section 11

11. Section 11 of the principal Act is amended —

(a) by inserting after the words "person who" the words "intentionally and without authorisation";

(b) by repealing the words "to be" after the words "data with the intent" and substituting them with the words "that it be";

(c) by repealing the number "20" and substituting it with the number "10".

Amendment of section 12

12. Section 12 of the principal Act is amended in the chapeau, by repealing the words "without lawful excuse or justification" and substituting them with the words "without authorisation".

Replacement of section 13

13. The principal Act is amended by repealing and substituting section 13 as follows—

"**Cyber Extortion**

13. Any person who unlawfully and intentionally uses a computer system to demand money or other goods or behavior from another person by threatening to inflict harm to this person, their reputation, or property for the purpose of —

(a) obtaining any advantage from such person; or

(b) compelling such person to perform or to abstain from performing any act,

commits the offence of cyber extortion and shall on conviction be liable to a fine not exceeding level 4 on the standard scale or to imprisonment for a term not exceeding 10 years or both."

Replacement of section 14

14. The principal Act is amended by repealing section 14 and substituting it with following —

"**Cyber harassment**

14.(1) A person who, with the intention to coerce, intimidate, harass, or cause emotional distress to a person, uses a computer system for any of the following purposes —

(a) making in more than one occasion, any request, suggestion or proposal of sexual nature ; or

(b) threatening in more than one occasion, to inflict injury or physical harm to the person or property of any person; or

(c) sending, delivering or showing in more than one occasion, a message, visual or otherwise, including those of a sexual nature; threatening, causing alarm or distress to any person,

commits an offence and shall, on conviction, be liable to a fine of level 4 on the standard scale or to imprisonment for a term not exceeding 5 years, or to both.

(2) Subsection (1) shall not apply where the act —

(a) was necessary for the purposes of preventing, detecting or investigating crime; or

(b) was made in the course of court proceedings or any other judicial proceeding."

Replacement of section 15

15. The principal Act is amended by repealing section 15 and substituting it as follows —

"**Cyber stalking**

15(1) A person who without authorisation uses a computer system with the intent to torment, embarrass, coerce, intimidate or harass any person by —

(a) following a person or contacts or attempts to contact such person to foster personal interaction on more than one occasion, despite a clear indication of disinterest by such person;

(b) monitoring the use by a person of the internet, electronic mail, text message or any other form of electronic communication;

(c) watching or spying upon a person in a manner that results in fear of violence or serious alarm or distress, in the mind of such person; or

(d) sending or delivering or showing a message, visual or otherwise of any person and displays or distributes it without his or her consent in a manner that harms a person.

(2) Whoever commits the offence specified in subsection (1) shall on conviction be liable to imprisonment for a term not exceeding five years or to fine not exceeding level 4 on the standard scale or to both:

Provided that, if the victim of the cyber stalking under subsection (1) is a minor, the penalty of imprisonment shall be extended by a further period not exceeding to seven years or with an additional fine not exceeding level five on the standard scale or with both.

(3) Any aggrieved person or his or her guardian, where such person is a minor, may apply to the relevant competent authority for removal, destruction of or blocking access to such information referred to in subsection (1) and the competent

authority, on receipt of such application, shall forthwith take such necessary action as deemed reasonable in the circumstances including an order for removal, destruction, preventing transmission of or blocking access to such information and the competent authority may also direct any of its licensees to secure such information including traffic data.

(4) Subsection (1) shall not apply where the act —

(a) was necessary for the purpose of preventing, detecting or investigating a crime; or

(b) was made in the course of court proceedings or any other judicial proceedings."

Replacement of section 16

16. The principal Act is amended by repealing and substituting section 16 as follows —

"**16**. A person who maliciously 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 shall, on conviction, be liable to a fine of level 4 on the standard scale or to imprisonment for a term not exceeding 5 years, or to both."

Amendment of section 17

17. Section 17 of the principal Act is amended —

(a) by repealing subsection (2) and substituting it with the following subsection —

"(2) A person who knowingly and intentionally —

(a) produces child pornography for the purpose of its distribution through a computer system;

(b) offers or make available child pornography through a computer system;

(c) distributes or transmits child pornography through a computer system;

(d) procures child pornography through a computer system for oneself or for another person;

(e) possesses child pornography in a computer system or on a computer-data storage medium.

(f) accesses child pornography through a computer system

commits an offence and shall, on conviction, be liable to a fine not exceeding level 5 on the standard scale or to imprisonment for a term not exceeding ten years or both".

Replacement of section 18

18. The principal Act is amended by repealing and substituting section 18 as follows —

"**Revenge pornography**

18.(1) A person who, intentionally causes distress to another person by means of a computer system, by disclosing or publishing a sexually explicit message, visual or otherwise, without the consent of the person who appears in the message commits an offence and shall, on conviction, be liable to a fine of level 4 on the standard scale or to imprisonment for a term not exceeding 5 years, or to both.

(2) Subsection (1) shall not apply where the disclosure —

(a) was necessary for the purposes of preventing, detecting or investigating crime; or

(b) was made in the course of, or with a view to, the publication of journalistic material and such publication of the journalistic material was, or would be, in the public interest; or

(c) was made in the course of court proceedings or any other judicial proceeding."

Amendment of section 19

19. Section 19 of the principal Act is amended in the chapeau by inserting after the words "service provider who" the word "knowingly".

Insertion of sections 19A, 19B and 19C

20. The principal Act is amended by inserting after section 19, the following new sections —

"**Infringement of copyright and related rights**

19A. Any person who, by means of a computer system or any other electronic means, intentionally infringes copyright in any work protected in terms of the Copyright Act, 2014 (Act No. 5 of 2014), commits an offence and is liable, on conviction, to a fine of level five on the standard scale, imprisonment for a term not exceeding five years, or both.

Attempt, aiding and abetting

19B.(1) Any person who intentionally aids or abets the commissioning of any of the offences established under this act commits an offence and shall, on conviction be liable to the penalty that has been specified for the principal offence.

(2) Any person who intentionally attempts to commit any of the offences established under this act commits an offence and shall, on conviction be liable to the penalty that has been specified for the principal offence.

Corporate liability

19C.(1) Any natural or legal person, who exercises management or supervisory authority, based on —

(a) a power of representation of the legal person;

(b) an authority to take decisions on behalf of the legal person;

(c) an authority to exercise control within the legal person,

and fails to exercise reasonable and proper control over such legal person commits an offence under this Act, and is liable on conviction to a fine not exceeding level 4 or to a term of imprisonment not exceeding three years or to both such fine and imprisonment and in the case of a corporation, partnership, or association, to a fine not exceeding level five.

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

Amendment of section 20

21. Section 20 of the principal Act is amended —

(a) by repealing subsection (5) and substituting it with the following subsection —

"(5) The powers and procedures for the purposes of subsections (1), (2) and (3) shall apply to —

(a) all offences under this Act;

(b) other criminal offences committed by means of a computer system; and

(c) the collection of evidence in electronic form for a criminal offence."

(b) by inserting a new subsection after subsection (5) as follows —

"(6) The person in possession or control of the computer data shall be responsible to preserve the data specified —

(a) for the period specified in the notice for preservation and maintenance of integrity, or for any extension thereof permitted by the Court; and

(b) for the period specified to keep confidential any preservation ordered under this section."

Amendment of section 21

22. Section 21 of the principal Act is amended —

(a) in the section heading by replacing the word "computer" with the word "traffic";

(b) subsection (1), —

(i) by repealing paragraph (a) and substituting it with the following paragraph —

"(a) sufficient traffic data, irrespective of whether one or more electronic service providers were involved in the transmission of such traffic data;

(ii) in paragraph (b) by repealing the word "computer" after the word "traffic";

(iii) in paragraph (b) by replacing the word "computer" after the words "which the" with the word "traffic".

(c) by repealing subsection (2) and substituting it with the following —

"(2) The powers and procedures for the purposes of subsection (1) apply to —

(a) all offences under this act;

(b) other criminal offences committed by means of a computer system; and

(c) the collection of evidence in electronic form for a criminal offence.".

Amendment of section 22

23. Section 22 of the principal Act is amended —

(a) in subsection (1)(b), by inserting after the words "offering its services" , the words "in Seychelles";

(b) in subsection (2), by repealing the words ",disc, cassette, or on microfilm, or preserved by any mechanical or electronic device" and substituting them with the words "or computer storage medium".

Amendment of section 23

24. Section 23 of the principal Act is amended by inserting a new subsection after subsection (1) as follows —

"(1A) An application made by an investigatory authority in terms of subsection (1) must demonstrate to the satisfaction of the Court that there exist reasonable grounds to believe that there may be an information system, data, device or other articles that —

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

(b) has been acquired by a person as a result of the commission of an offence,

the Court may issue a warrant which shall authorize an officer of the investigatory authority, with such assistance as may be necessary, to search any information system, data, device or storage medium relevant to the offence identified in the application and access, seize or similarly secure any information system, data, device or other articles relevant to the offence identified in the application."

Amendment of section 24

25. Section 24 of the principal Act is amended, by inserting new subsections after the existing subsection (which must now be numbered (1)) as follows —

"(2) For the purposes of subsection (1), an investigating authority making application to the Court must demonstrate to the satisfaction of the Court that there exist reasonable grounds to believe that the computer data in an information system is reasonably required for the purpose of a criminal investigation or criminal proceedings with respect to an offence, the Court may, after recording reasons, order that the person in control of the data or information system, to provide such data or access to such data to the investigating authority.

(3) The period of a warrant issued under sub-section (1) may be extended beyond seven days if, on an application, a Court authorizes an extension for a further period of time as may be specified by the Court."

Insertion of new section 24A

26. The principal Act is amended by inserting after section 24, the following section —

"Interception of content Data"

24A. Where the investigatory authority has reasonable grounds to believe that any content data is relevant for the investigation and prosecution of an offence under this Act, it may make an application to the court for an order to —

(a) collect or record content data in the territory of Seychelles by technical means in real-time of specified communications by means of a computer system;

(b) compel a service provider, within its existing technical capabilities, to —

(i) collect or record through the application of technical means on the territory of Seychelles; or

(ii) cooperate and assist the investigatory authority in the collection or recording of,

content data, in real-time, of specified communications in the territory of Seychelles, transmitted by means of a computer system; or

(c) compel a service provider to keep the confidentiality of the fact of the execution of any power provided for in this section and any information relating to it.

Amendment of section 27

27. Section 27 of the principal Act is amended in subsection (a) by repealing the word "protection" and substituting it with the word "production"