Seychelles

Cybercrime legislation

Comparative analysis of domestic legislation against the provisions of the Convention on Cybercrime

Convention on Cybercrime (Budapest Convention)	**Domestic legislation** **Cybercrimes and Other Related Crimes Act 2021**
Article 1 – "Computer system", "computer data", "service provider", "traffic data": For the purposes of this Convention:	**Interpretation** **2.** In this Act, unless the context otherwise requires –
	"access" in relation to a computer system means to instruct, communicate with, store data in, retrieve data from or otherwise make use of any of the resources of a computer system;
b "computer data" means any representation of facts, information or concepts in a form suitable for processing in a computer system, including a program suitable to cause a computer system to perform a function;	"computer data" means any representation of facts, information or concepts in a form suitable for processing in a computer system, including a program suitable to cause a computer system to perform a function;
"computer 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 system" means any computer data processing device or a group of such interconnected or related devices one or more of which pursuant to a program performs automatic processing of computer data performing logical arithmetic or storage functions and – (a) includes any computer data storage facility or communications facility directly related to or operating in conjunction with such device or group of such interconnected or related devices, whether available in a single or distributed or decentralised form; (b) any reference in this Act to any program or computer data held in a computer system includes a reference to any program or computer data held in any removable storage medium which is for the time being in the computer system; (c) and a computer system is to be regarded as containing any program or computer data held in any such medium;
	"Convention" means the Budapest Convention on Cybercrime adopted by the Committee of Ministers of the Council of Europe and entered into force on 1 July 2004;

"service provider" means: i 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;	"electronic 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;
	"investigatory authority" means the Police Force of Seychelles or any other body empowered to investigate any offence;
	"function" includes logic, control, arithmetic, deletion, storage and retrieval and communication or telecommunication to, from or within a computer system;
	"message" means a verbal, written, recorded, drawn or picture communication sent to or left for a recipient;
	"Minister" means the Minister responsible for internal Affairs;
	"seize" includes - (a) make and retain a copy of computer data, including by using on-site equipment; and (b) render inaccessible, or remove, computer data in the accessed computer system; and (c) take a printout of output of computer data;
"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.	"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.
Article 2 – Illegal access Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, the access to the whole or any part of a computer system without right. A Party may require that the offence be committed by infringing security measures, with the intent of obtaining computer data or other dishonest intent, or in relation to a computer system that is connected to another computer system.	**Unauthorised access to computer system** **4.(**1) A person who causes a computer system to perform a function with the intent to secure unauthorised access to any computer data held in a computer system, 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) For the purpose of subsection (1) – (a) access by a person to a computer system is unauthorised, where the 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 from any person who is so entitled.

	(b) for the purposes of this section, it is immaterial that the unauthorised access is not directed at - (i) any particular program or computer data; (ii) a program or computer data of any kind; or (iii) a program or computer data held in any particular computer system. **Access with criminal intent** **5.(**1) A person who causes a computer system to perform any function for the purpose of securing access to any computer data held in any computer system, with criminal intent, 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. (2) For the purpose of subsection (1) - (a) the access referred to in subsection (1) is authorised or unauthorised; (b) the further offence to which this section applies is committed at the same time when the access is secured or at any other time.
Article 3 – Illegal interception Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, the interception without right, made by technical means, of non-public transmissions of computer data to, from or within a computer system, including electromagnetic emissions from a computer system carrying such computer data. A Party may require that the offence be committed with dishonest intent, or in relation to a computer system that is connected to another computer system.	**Unauthorised interception** **6.** (1) A person who – (a) intentionally intercepts or causes to be intercepted any function or non-public transmission to, from or within, a computer system and - (i) does so by technical means; and (ii) does not have authority to intercept the function or transmission or to cause the interception; (b) intentionally uses or causes to be used, directly or indirectly, a computer system for the purpose of committing an offence, 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 both. (2) For the purposes of subsection (1), intercepting includes listening to or viewing, by use of technical means, or recording, a function of a computer system or acquiring the substance, meaning or purport of any such function.
Article 4 – Data interference 1. Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, the damaging, deletion, deterioration, alteration or suppression of computer data without right. 2. A Party may reserve the right to require that the conduct described in paragraph 1 result in serious harm.	**Unauthorised interference with computer data** **7.** (1) A person who, without authority, intentionally does any of the following acts – (a) destroys or alters computer data; (b) renders computer data meaningless, useless, inaccessible, ineffective, unreliable, impaired; (c) obstructs, interrupts or interferes with the lawful use of computer data; (d) obstructs, interrupts or interferes with any person in the lawful use of computer data; (e) denies access to computer data to any person entitled to it; or (f) accesses or intercepts any computer data without authority, 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.

Article 5 – System interference Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, the serious hindering without right of the functioning of a computer system by inputting, transmitting, damaging, deleting, deteriorating, altering or suppressing computer data.	**Unauthorised interference of computer system operation** **8.** (1) A person who intentionally, whether directly or indirectly, and without authority - (a) interferes with, or interrupts or obstructs the use of, a computer system; or (b) impedes or prevents access to, or impairs the usefulness or effectiveness of, any computer data in 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. (2) For the purposes of subsection (1), interference, interruption, obstruction or impendence in relation to a computer system, includes - **(a) cutting the electricity supply to a computer system;** (b) corrupting a computer system by any means; and (c) inputting, deleting or altering computer data.
Article 6 – Misuse of devices 1. Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally and without right: a the production, sale, procurement for use, import, distribution or otherwise making available of: i a device, including a computer program, designed or adapted primarily for the purpose of committing any of the offences established in accordance with the above Articles 2 through 5; ii a computer password, access code, or similar data by which the whole or any part of a computer system is capable of being accessed, with intent that it be used for the purpose of committing any of the offences established in Articles 2 through 5; and b the possession of an item referred to in paragraphs a.i or ii above, with intent that it be used for the purpose of committing any of the offences established in Articles 2 through 5. A Party may require by law that a number of such items be possessed before criminal liability attaches. 2. This article shall not be interpreted as imposing criminal liability where the production, sale, procurement for use, import, distribution or otherwise making available or possession referred to in paragraph 1 of this article is not for the purpose of committing an offence established in accordance with Articles 2 through 5 of this Convention, such as for the authorised testing or protection of a computer system.	**Unlawful possession of illegal devices** **9.** A person who - (a) intentionally, **without justification**, produces, sells, procures for use, imports, exports, distributes or otherwise makes available - (i) a device, including computer data, that is designed or adapted for the purpose of committing an offence against section 6, 7, or 8; or (ii) a computer system password, access code or similar computer data by which the whole or any part of a computer system is capable of being accessed; (b) has any item mentioned in subparagraph (i) or (ii) of paragraph (a) in his or her possession with the intent that it be used by any person for the purpose of committing an offence against section 6, 7, or 8, 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. **Unauthorised disclosure of access credentials** **12.** A person who, **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 a computer system or computer data - (a) for wrongful gain; (b) for any unlawful purpose; (c) to overcome security measures for the protection of computer data; or (d) with the knowledge that it is likely to cause prejudice 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.

3. Each Party may reserve the right not to apply paragraph 1 of this article, provided that the reservation does not concern the sale, distribution or otherwise making available of the items referred to in paragraph 1 a.ii of this article.	
Article 7 – Computer-related forgery Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally and **without right**, the input, alteration, deletion, or suppression of computer data, resulting in inauthentic data with the intent that it be considered or acted upon for legal purposes as if it were authentic, regardless whether or not the data is directly readable and intelligible. A Party may require an intent to defraud, or similar dishonest intent, before criminal liability attaches.	**Computer system related forgery** **11.** A person who causes loss of property to another person by any input, alteration, deletion or suppression of computer data resulting in inauthentic computer data with the intent to be considered or acted upon for legal purposes as if it were authentic, regardless whether or not the computer data is directly readable and intelligible, 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.
Article 8 – Computer-related fraud Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally and without right, the causing of a loss of property to another person by: a any input, alteration, deletion or suppression of computer data; b any interference with the functioning of a computer system, with fraudulent or dishonest intent of procuring, without right, an economic benefit for oneself or for another person.	**Electronic fraud** **10.** A person who intentionally and without right causes loss of property to another person by - (a) any input, alteration, deletion or suppression of computer data; or (b) any interference with the functioning of a computer system, with intent to procure for himself or herself or another person, an advantage or economic benefit, 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 10 years or to both.
Article 9 – Offences related to child pornography 1. Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally and without right, the following conduct: a producing child pornography for the purpose of its distribution through a computer system; b offering or making available child pornography through a computer system; c **distributing or transmitting** child pornography through a computer system;	**Pornographic or obscene material** **17.** (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,

d procuring child pornography through a computer system for oneself or for another person; e possessing child pornography in a computer system or on a computer-data storage medium. 2. For the purpose of paragraph 1 above, the term "child pornography" shall include pornographic material that visually depicts: a a minor engaged in sexually explicit conduct; b a person appearing to be a minor engaged in sexually explicit conduct; 3. For the purpose of paragraph 2 above, the term "minor" shall include all persons under 18 years of age. A Party may, however, require a lower age-limit, which shall be not less than 16 years. 4. Each Party may reserve the right not to apply, in whole or in part, paragraphs 1, sub-paragraphs d. and e, and 2, sub-paragraphs b. and c.	(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 system; (b) produces child pornography or obscene material relating to children for the purpose of its publication through a computer system; (c) possesses child pornography or obscene material relating to children in a 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 system, 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. (3) A person who, by means of a 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; (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 any sexual offence with that person under the Penal Code, 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. (4) Evidence that the person in subsection (3)(a), (b) or (c) 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 subsection (3)(a), (b) or (c) is a fictitious person, represented to the accused as a real person.
Article 10 – Offences related to infringements of copyright and related rights 1. Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law the infringement of copyright, as defined under the law of that Party, pursuant to the obligations it has undertaken under the Paris Act of 24 July 1971 revising the Bern Convention for the Protection of Literary and Artistic Works, the Agreement on Trade-Related Aspects of Intellectual Property Rights and the WIPO Copyright Treaty, with the exception of any	Copyright Act 2014 **3. Interpretation** "computer" means an electronic or similar device having information-processing capabilities; "computer programme" is a set of instructions expressed in words, codes, schemes or in any other form, which is capable, when incorporated in a medium that the computer can read, of causing a computer to perform or achieve a particular task or result;

moral rights conferred by such conventions, where such acts are committed wilfully, on a commercial scale and by means of a computer system. 2. Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law the infringement of related rights, as defined under the law of that Party, pursuant to the obligations it has undertaken under the International Convention for the Protection of Performers, Producers of Phonograms and Broadcasting Organisations (Rome Convention), the Agreement on Trade-Related Aspects of Intellectual Property Rights and the WIPO Performances and Phonograms Treaty, with the exception of any moral rights conferred by such conventions, where such acts are committed wilfully, on a commercial scale and by means of a computer system. 3. A Party may reserve the right not to impose criminal liability under paragraphs 1 and 2 of this article in limited circumstances, provided that other effective remedies are available and that such reservation does not derogate from the Party's international obligations set forth in the international instruments referred to in paragraphs 1 and 2 of this article.	**15. Reproduction and adaptation of computer programmes** (1) The reproduction, in a single copy, or the adaptation of a computer programme by the lawful owner of a copy of that computer programme shall be permitted without the authorisation of the author or other owner of copyright, provided that the copy or adaptation is necessary— (a) for use of the computer programme with a computer for the purpose and extent for which the computer programme has been obtained; or (b) for archival purposes and for the replacement of the lawfully owned copy of the computer programme in the event that the said copy of the computer programme is lost, destroyed or rendered unusable. (2) No copy or adaptation of a computer programme shall be used for any purpose other than those specified in subsection (1), and any such copy or adaptation shall be destroyed in the event that continued possession of the copy of the computer programme ceases to be lawful. **31. Offences and penalties** (1) A person who will fully and on a commercial scale infringes any reproduction rights protected under this Act commits an offence and shall on conviction be liable to imprisonment for a term not exceeding five years or with a fine not exceeding SCR50,000 or with both such imprisonment and fine.
	Cyber extortion **13.** 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 shall be liable, on conviction, to a fine of level 4 on the standard scale or to imprisonment for a term not exceeding 5 years or to both.
	Cyber harassment **14.** A person who uses a 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; or (c) sending, delivering or showing a message, visual or otherwise, which is abusive, obscene, indecent, threatening, false or misleading, causing annoyance, inconvenience or is likely to cause distress or needless anxiety 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.

	Cyber stalking **15.** A person who wilfully, 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 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.
	Offensive electronic communications **16.** A person who wilfully, 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 shall, on conviction, be liable to a fine of level 4 on the standard scale or to imprisonment for a term not exceeding 5years, or to both.
	Pornographic publication **18.** A person who, by means of a computer system, discloses or publishes a private sexual photograph or film without the consent of the person who appears in the photograph or film 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.
	Unlawful disclosure by electronic service provider **19.** An electronic 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 computer data collected or recorded under an order, 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.
Article 11 – Attempt and aiding or abetting 1. Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, aiding or abetting the commission of any of the offences established in accordance with Articles 2 through 10 of the present Convention with intent that such offence be committed. 2. Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, an attempt to commit any of the offences	

established in accordance with Articles 3 through 5, 7, 8, and 9.1.a and c. of this Convention. 3. Each Party may reserve the right not to apply, in whole or in part, paragraph 2 of this article.	
Article 12 – Corporate liability 1. Each Party shall adopt such legislative and other measures as may be necessary to ensure that legal persons can be held liable for a criminal offence established in accordance with this Convention, committed for their benefit by any natural person, acting either individually or as part of an organ of the legal person, who has a leading position within it, 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. 2. In addition to the cases already provided for in paragraph 1 of this article, each Party shall take the measures necessary to ensure that a legal person can be held liable where the lack of supervision or control by a natural person referred to in paragraph 1 has made possible the commission of a criminal offence established in accordance with this Convention for the benefit of that legal person by a natural person acting under its authority. 3. Subject to the legal principles of the Party, the liability of a legal person may be criminal, civil or administrative. 4. Such liability shall be without prejudice to the criminal liability of the natural persons who have committed the offence.	
Article 13 – Sanctions and measures 1. Each Party shall adopt such legislative and other measures as may be necessary to ensure that the criminal offences established in accordance with Articles 2 through 11 are punishable by effective, proportionate and dissuasive sanctions, which include deprivation of liberty. 2. Each Party shall ensure that legal persons held liable in accordance with Article 12 shall be subject to effective, proportionate and dissuasive criminal or non-criminal sanctions or measures, including monetary sanctions.	

Article 14 – Scope of procedural provisions 1. Each Party shall adopt such legislative and other measures as may be necessary to establish the powers and procedures provided for in this section for the purpose of specific criminal investigations or proceedings. 2. Except as specifically provided otherwise in Article 21, each Party shall apply the powers and procedures referred to in paragraph 1 of this article to: a the criminal offences established in accordance with Articles 2 through 11 of this Convention; b other criminal offences committed by means of a computer system; and c the collection of evidence in electronic form of a criminal offence. 3. a Each Party may reserve the right to apply the measures referred to in Article 20 only to offences or categories of offences specified in the reservation, provided that the range of such offences or categories of offences is not more restricted than the range of offences to which it applies the measures referred to in Article 21. Each Party shall consider restricting such a reservation to enable the broadest application of the measure referred to in Article 20. b Where a Party, due to limitations in its legislation in force at the time of the adoption of the present Convention, is not able to apply the measures referred to in Articles 20 and 21 to communications being transmitted within a computer system of a service provider, which system: i is being operated for the benefit of a closed group of users, and ii does not employ public communications networks and is not connected with another computer system, whether public or private, that Party may reserve the right not to apply these measures to such communications. Each Party shall consider restricting such a reservation to enable the broadest application of the measures referred to in Articles 20 and 21.	
Article 15 – Conditions and safeguards 1. Each Party shall ensure that the establishment, implementation and application of the powers and procedures provided for in this Section are subject to	

conditions and safeguards provided for under its domestic law, which shall provide for the adequate protection of human rights and liberties, including rights arising pursuant to obligations it has undertaken under the 1950 Council of Europe Convention for the Protection of Human Rights and Fundamental Freedoms, the 1966 United Nations International Covenant on Civil and Political Rights, and other applicable international human rights instruments, and which shall incorporate the principle of proportionality. 2. Such conditions and safeguards shall, as appropriate in view of the nature of the procedure or power concerned, *inter alia,* include judicial or other independent supervision, grounds justifying application, and limitation of the scope and the duration of such power or procedure. 3. To the extent that it is consistent with the public interest, in particular the sound administration of justice, each Party shall consider the impact of the powers and procedures in this section upon the rights, responsibilities and legitimate interests of third parties.	
Article 16 – Expedited preservation of stored computer data 1. Each Party shall adopt such legislative and other measures as may be necessary to enable its competent authorities to order or similarly obtain the expeditious preservation of specified computer data, including traffic data, that has been stored by means of a computer system, in particular where there are grounds to believe that the computer data is particularly vulnerable to loss or modification. 2. Where a Party gives effect to paragraph 1 above by means of an order to a person to preserve specified stored computer data in the person's possession or control, the Party shall adopt such legislative and other measures as may be necessary to oblige that person to preserve and maintain the integrity of that computer data for a period of time as long as necessary, up to a maximum of ninety days, to enable the competent authorities to seek its disclosure. A Party may provide for such an order to be subsequently renewed. 3. Each Party shall adopt such legislative and other measures as may be necessary to oblige the custodian or other person who is to preserve the computer data to keep confidential the undertaking of such procedures for the period of time provided for by its domestic law.	**Preservation Order** **20.** (1) An investigatory authority may order the expeditious preservation of computer data that has been stored by means of a computer system or any other information and communication technologies, where there are reasonable grounds to believe that such computer data is vulnerable to loss or modification. (2) For the purposes of subsection (1), computer data includes traffic data. (3) An order made under subsection (1) shall remain in force for a period not exceeding 90 days. (4) Where the computer data is required to be preserved beyond 90 days, the investigatory authority shall make an application to the Court and the Court may make such order for preservation of the computer data as it may deem fit. (5) The powers and procedures for the purposes of subsections (1), (2) and (3) shall apply to all offences under this Act.

4. The powers and procedures referred to in this article shall be subject to Articles 14 and 15.	
Article 17 – Expedited preservation and partial disclosure of traffic data 1. Each Party shall adopt, in respect of traffic data that is to be preserved under Article 16, such legislative and other measures as may be necessary to: a ensure that such expeditious preservation of traffic data is available regardless of whether one or more service providers were involved in the transmission of that communication; and b ensure the expeditious disclosure to the Party's competent authority, or a person designated by that authority, of a sufficient amount of traffic data to enable the Party to identify the service providers and the path through which the communication was transmitted. 2. The powers and procedures referred to in this article shall be subject to Articles 14 and 15.	**Disclosure of preserved computer data** **21.** (1) The investigatory authority may, for the purposes of an investigation or the prosecution of an offence, order the disclosure of - (a) all preserved traffic computer data, irrespective of whether one or more electronic service providers were involved in the transmission of such computer data; (b) sufficient traffic computer data to identify the electronic service providers and the path through which the computer data was transmitted. (2) The powers and procedures for the purposes of subsection (1) apply to all offences under this Act.
Article 18 – Production order 1. Each Party shall adopt such legislative and other measures as may be necessary to empower its competent authorities to order: a a 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; and b a service provider offering its services in the territory of the Party to submit subscriber information relating to such services in that service provider's possession or control. 2. The powers and procedures referred to in this article shall be subject to Articles 14 and 15. 3. For the purpose of this article, the term "subscriber information" means any information contained in the form of computer data or any other form that is held by a service provider, relating to subscribers of its services other than traffic or content data and by which can be established: a the type of communication service used, the technical provisions taken thereto and the period of service; b the subscriber's identity, postal or geographic address, telephone and other access number,	**Production Order** **22.** (1) Where the disclosure of computer data is required for the purposes of an investigation or the prosecution of an offence, an investigatory authority may apply to the court for a Production Order compelling - (a) any person to submit specified computer data in that person's possession or control, which is stored in a computer system or computer data storage medium; (b) any electronic service provider offering its services to submit subscriber information in relation to such services in that electronic service provider's possession or control. (2) Where any material to which an investigation relates consists of computer data stored in a computer system, disc, cassette, or on microfilm, or preserved by any mechanical or electronic 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.

billing and payment information, available on the basis of the service agreement or arrangement; c any other information on the site of the installation of communication equipment, available on the basis of the service agreement or arrangement.	
Article 19 – Search and seizure of stored computer data 1. Each Party shall adopt such legislative and other measures as may be necessary to empower its competent authorities to search or similarly access: a a computer system or part of it and computer data stored therein; and b a computer-data storage medium in which computer data may be stored in its territory. 2. Each Party shall adopt such legislative and other measures as may be necessary to ensure that where its authorities search or similarly access a specific computer system or part of it, pursuant to paragraph 1.a, and have grounds to believe that the data sought is stored in another computer system or part of it in its territory, and such data is lawfully accessible from or available to the initial system, the authorities shall be able to expeditiously extend the search or similar accessing to the other system. 3. Each Party shall adopt such legislative and other measures as may be necessary to empower its competent authorities to seize or similarly secure computer data accessed according to paragraphs 1 or 2. These measures shall include the power to: a seize or similarly secure a computer system or part of it or a computer-data storage medium; b make and retain a copy of those computer data; c maintain the integrity of the relevant stored computer data; d render inaccessible or remove those computer data in the accessed computer system. 4. Each Party shall adopt such legislative and other measures as may be necessary to empower its competent authorities to order any person who has knowledge about the functioning of the computer system or measures applied to protect the computer data therein to provide, as is reasonable, the necessary information, to enable the undertaking of the measures referred to in paragraphs 1 and 2.	**Powers of access, search and seizure for purposes of investigation** **23.** (1) Where an investigatory authority has reasonable grounds to believe that stored computer data would be relevant for the purposes of an investigation or the prosecution of an offence, it may apply to the court for the issue of a warrant to search, access or secure computer data. (2) To secure computer data under subsection (1), the powers of the investigatory authority shall include the power to - (a) search, seize or secure a computer system or any information and communication technologies medium; (b) make and retain a copy of such computer data or information; (c) maintain the integrity of the relevant stored computer data or information; or (d) render inaccessible or remove the stored computer data or information from the computer system, or any information and communication technologies medium. **Deletion Order** **25.** (1) The court may, upon application by an investigatory authority, and being satisfied that a computer system or any other information and communication technologies medium contains indecent material of a child, order that such computer data be - (a) no longer stored on and made available through the computer system or any other medium; or (b) deleted or destroyed. (2) For the purposes of this section, "indecent material" means- (a) any indecent or obscene writing, photograph, sketch, drawing or picture whether partly or wholly generated by computer; (b) any indecent or obscene printed matter, print, painting, poster drawing, model or cinematographic film or video film, cassette or disc; or (c) any other indecent or obscene object.

5. The powers and procedures referred to in this article shall be subject to Articles 14 and 15.	
Article 20 – Real-time collection of traffic data 1. Each Party shall adopt such legislative and other measures as may be necessary to empower its competent authorities to: a collect or record through the application of technical means on the territory of that Party, and b compel a service provider, within its existing technical capability: i to collect or record through the application of technical means on the territory of that Party; or ii to co-operate and assist the competent authorities in the collection or recording of, traffic data, in real-time, associated with specified communications in its territory transmitted by means of a computer system. 2. Where a Party, due to the established principles of its domestic legal system, cannot adopt the measures referred to in paragraph 1.a, it may instead adopt legislative and other measures as may be necessary to ensure the real-time collection or recording of traffic data associated with specified communications transmitted in its territory, through the application of technical means on that territory. 3. Each Party shall adopt such legislative and other measures as may be necessary to oblige a service provider to keep confidential the fact of the execution of any power provided for in this article and any information relating to it. 4. The powers and procedures referred to in this article shall be subject to Articles 14 and 15.	**Real time collection of traffic data** **24.** Where the investigatory authority has reasonable grounds to believe that any computer data would be relevant for the purposes of an investigation or the prosecution of an offence, it may apply to the court for an order - (a) allowing the collection or recording of traffic data, in real time, associated with specified communications transmitted by means of any computer system; or (b) compelling an electronic service provider, within its technical capabilities, to effect such collection and recording referred to in paragraph (a), or assist the investigatory authority to effect such collection and recording.
Article 21 – Interception of content data 1. Each Party shall adopt such legislative and other measures as may be necessary, in relation to a range of serious offences to be determined by domestic law, to empower its competent authorities to: a collect or record through the application of technical means on the territory of that Party, and b compel a service provider, within its existing technical capability: i to collect or record through the application of technical means on the territory of that Party, or	

ii to co-operate and assist the competent authorities in the collection or recording of, content data, in real-time, of specified communications in its territory transmitted by means of a computer system. 2. Where a Party, due to the established principles of its domestic legal system, cannot adopt the measures referred to in paragraph 1.a, it may instead adopt legislative and other measures as may be necessary to ensure the real-time collection or recording of content data on specified communications in its territory through the application of technical means on that territory. 3. Each Party shall adopt such legislative and other measures as may be necessary to oblige a service provider to keep confidential the fact of the execution of any power provided for in this article and any information relating to it. 4. The powers and procedures referred to in this article shall be subject to Articles 14 and 15.	
Article 22 – Jurisdiction 1. Each Party shall adopt such legislative and other measures as may be necessary to establish jurisdiction over any offence established in accordance with Articles 2 through 11 of this Convention, when the offence is committed: a in its territory; or b on board a ship flying the flag of that Party; or c on board an aircraft registered under the laws of that Party; or d by one of its nationals, if the offence is punishable under criminal law where it was committed or if the offence is committed outside the territorial jurisdiction of any State. 2. Each Party may reserve the right not to apply or to apply only in specific cases or conditions the jurisdiction rules laid down in paragraphs 1.b through 1.d of this article or any part thereof. 3. Each Party shall adopt such measures as may be necessary to establish jurisdiction over the offences referred to in Article 24, paragraph 1, of this Convention, in cases where an alleged offender is present in its territory and it does not extradite him or her to another Party, solely on the basis of his or her nationality, after a request for extradition.	**Application of the Act** **3.** This Act applies to an act - (a) that occurs wholly or partly in the territory of Seychelles; (b) that occurs wholly or partly on a ship flying the flag of Seychelles; (c) that occurs wholly or partly on board an aircraft registered under the laws of Seychelles; and (d) directly or indirectly connected to, or affecting, a person, computer system or event within Seychelles. **Jurisdiction** **28.** (1) Notwithstanding any other written law, the Supreme Court shall have jurisdiction to try an offence under this Act or any regulations made thereunder and may, on conviction, impose any penalty or forfeiture provided for under this Act. (2) The Supreme Court shall have jurisdiction where the act constituting an offence under this Act has been, wholly or partly, committed outside Seychelles - (a) on board a Seychelles ship; or (b) on board an aircraft registered in Seychelles. **Penal Code - Chapter 158 (1955)** **7. Offence committed partly within and partly beyond the jurisdiction** When an act which, if wholly done within the jurisdiction of the court, would be an offence against this Code, is done partly within and partly beyond the jurisdiction, every person who within the jurisdiction does or makes any part of such act may be tried and punished under this Code in the same manner as if such act had been done wholly within the jurisdiction.

4. This Convention does not exclude any criminal jurisdiction exercised by a Party in accordance with its domestic law. When more than one Party claims jurisdiction over an alleged offence established in accordance with this Convention, the Parties involved shall, where appropriate, consult with a view to determining the most appropriate jurisdiction for prosecution.	
Article 23 - General principles relating to international co-operation The Parties shall co-operate with each other, in accordance with the provisions of this chapter, and through the application of relevant international instruments on international co-operation in criminal matters, arrangements agreed on the basis of uniform or reciprocal legislation, and domestic laws, to the widest extent possible for the purposes 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.	**Mutual Assistance in Criminal Matters Act 2022** Act does not limit cooperation with international organizations 4. (1) Nothing in this Act derogates from existing forms of cooperation or prevents the development of other forms of cooperation, whether formal or informal, in respect of any criminal matter between Seychelles and any foreign State or authority such as the International Criminal Police Organization (INTERPOL). (2) This Act does not prevent the provision or obtaining of international assistance in criminal matters under any other written law.
Article 24 – Extradition 1. a This article applies to extradition between Parties for the criminal offences established in accordance with Articles 2 through 11 of this Convention, provided that they are punishable under the laws of both Parties concerned by deprivation of liberty for a maximum period of at least one year, or by a more severe penalty. b Where a different minimum penalty is to be applied under an arrangement agreed on the basis of uniform or reciprocal legislation or an extradition treaty, including the European Convention on Extradition (ETS No. 24), applicable between two or more parties, the minimum penalty provided for under such arrangement or treaty shall apply. 2. The criminal offences described in paragraph 1 of this article shall be deemed to be included as extraditable offences in any extradition treaty existing between or among the Parties. The Parties undertake to include such offences as extraditable offences in any extradition treaty to be concluded between or among them. 3. If a Party that makes extradition conditional on the existence of a treaty receives a request for extradition	**Extradition** **29.** Any offence under this Act may, with the consent of the Attorney General, be an extraditable crime for which extradition may be granted or obtained under the Extradition Act (Cap 78). **Mutual Assistance in Criminal Matters Act** **Chapter 135A** **3. Act does not restrict other forms of cooperation nor authorise extradition** (1) Nothing in this Act prevents the provision or the obtaining of mutual assistance in criminal matters otherwise than as provided in this Act or otherwise than pursuant to other forms of co-operation between Seychelles and a foreign country, jurisdiction or organisation. (2) This Act does not authorise the extradition or the arrest or detention with a view to the extradition of any person.

from another Party with which it does not have an extradition treaty, it may consider this Convention as the legal basis for extradition with respect to any criminal offence referred to in paragraph 1 of this article. 4. Parties that do not make extradition conditional on the existence of a treaty shall recognise the criminal offences referred to in paragraph 1 of this article as extraditable offences between themselves. 5. Extradition shall be subject to the conditions provided for by the law of the requested Party or by applicable extradition treaties, including the grounds on which the requested Party may refuse extradition. 6. If extradition for a criminal offence referred to in paragraph 1 of this article is refused solely on the basis of the nationality of the person sought, or because the requested Party deems that it has jurisdiction over the offence, the requested Party shall submit the case at the request of the requesting Party to its competent authorities for the purpose of prosecution and shall report the final outcome to the requesting Party in due course. Those authorities shall take their decision and conduct their investigations and proceedings in the same manner as for any other offence of a comparable nature under the law of that Party. 7. a Each Party shall, at the time of signature or when depositing its instrument of ratification, acceptance, approval or accession, communicate to the Secretary General of the Council of Europe the name and address of each authority responsible for making or receiving requests for extradition or provisional arrest in the absence of a treaty. b The Secretary General of the Council of Europe shall set up and keep updated a register of authorities so designated by the Parties. Each Party shall ensure that the details held on the register are correct at all times.	
Article 25 – General principles relating to mutual assistance 1. The Parties shall afford one another mutual assistance to the widest extent possible 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.	**Act does not limit cooperation with international organizations** 4. (1) Nothing in this Act derogates from existing forms of cooperation or prevents the development of other forms of cooperation, whether formal or informal, in respect of any criminal matter between Seychelles and any foreign State or authority such as the International Criminal Police Organization (INTERPOL). (2) This Act does not prevent the provision or obtaining of international assistance in criminal matters under any other written law.

2. Each Party shall also adopt such legislative and other measures as may be necessary to carry out the obligations set forth in Articles 27 through 35. 3. Each Party may, in urgent circumstances, make requests for mutual assistance or communications related thereto by expedited means of communication, including fax or e-mail, to the extent that such means provide appropriate levels of security and authentication (including the use of encryption, where necessary), with formal confirmation to follow, where required by the requested Party. The requested Party shall accept and respond to the request by any such expedited means of communication. 4. Except as otherwise specifically provided in articles in this chapter, mutual assistance shall be subject to the conditions provided for by the law of the requested Party or by applicable mutual assistance treaties, including the grounds on which the requested Party may refuse co-operation. The requested Party shall not exercise the right to refuse mutual assistance in relation to the offences referred to in Articles 2 through 11 solely on the ground that the request concerns an offence which it considers a fiscal offence. 5. Where, in accordance with the provisions of this chapter, the requested Party is permitted to make mutual assistance conditional upon the existence of dual criminality, that condition shall be deemed fulfilled, irrespective of whether its laws place the offence within the same category of offence or denominate the offence by the same terminology as the requesting Party, if the conduct underlying the offence for which assistance is sought is a criminal offence under its laws.	
Article 26 – Spontaneous information 1. A Party may, within the limits of its domestic law and without prior request, forward to another Party information obtained within the framework of its own investigations when it considers that the disclosure of such information might assist the receiving Party in initiating or carrying out investigations or proceedings concerning criminal offences established in accordance with this Convention or might lead to a request for co-operation by that Party under this chapter. 2. Prior to providing such information, the providing Party may request that it be kept confidential or only used subject to conditions. If the receiving Party cannot comply with such request, it shall notify the providing Party, which	**Spontaneous information** **31.** (1) An authority may, without prior request, forward to the investigatory authority information obtained within the framework of its own investigation when it considers that the disclosure of such information might assist in initiating or carrying out investigations or proceedings concerning criminal offences established in accordance with this Act. (2) Prior to the disclosure of computer data under subsection (1) - (a) the authority may request the investigatory authority to maintain the confidentiality of the information provided; and (b) where the investigatory authority cannot comply with such request, it shall notify the authority, which may then determine whether the information should nevertheless be provided. (3) For the purposes of this section, "authority" means any public body, agency, organ or department established by law.

shall then determine whether the information should nevertheless be provided. If the receiving Party accepts the information subject to the conditions, it shall be bound by them.	
Article 27 – Procedures pertaining to mutual assistance requests in the absence of applicable international agreements 1. Where there is no mutual assistance treaty or arrangement on the basis of uniform or reciprocal legislation in force between the requesting and requested Parties, the provisions of paragraphs 2 through 9 of this article shall apply. The provisions of this article shall not apply where such treaty, arrangement or legislation exists, unless the Parties concerned agree to apply any or all of the remainder of this article in lieu thereof. 2. a Each Party shall designate a central authority or authorities responsible for sending and answering requests for mutual assistance, the execution of such requests or their transmission to the authorities competent for their execution. b The central authorities shall communicate directly with each other; c Each Party shall, at the time of signature or when depositing its instrument of ratification, acceptance, approval or accession, communicate to the Secretary General of the Council of Europe the names and addresses of the authorities designated in pursuance of this paragraph; d The Secretary General of the Council of Europe shall set up and keep updated a register of central authorities designated by the Parties. Each Party shall ensure that the details held on the register are correct at all times. 3. Mutual assistance requests under this article shall be executed in accordance with the procedures specified by the requesting Party, except where incompatible with the law of the requested Party. 4. The requested Party may, in addition to the grounds for refusal established in Article 25, paragraph 4, refuse assistance if: a the request concerns an offence which the requested Party considers a political offence or an offence connected with a political offence, or	**Mutual Assistance in Criminal Matters Act** **Chapter 2022** **Requests to be made by the Attorney General** **7.** (1) A request by Seychelles to a foreign State for assistance in a criminal matter under this Part shall be made by or through the Attorney General or an authority designated as a Central Authority under subsection (3). (2) A request under subsection (1) shall be made through the diplomatic channel. (3) For the purposes of this Act, the Central Authority is — (a) the Attorney General; or (b) any authority who the President may, by notice published in the Gazette, designate as a Central Authority on such terms and conditions as the President may determine. (4) An authority designated as a Central Authority under subsection (3) shall have the same powers as the Attorney General and shall provide or obtain international assistance in criminal matters on such terms and conditions as the President may determine.

b it considers that execution of the request is likely to prejudice its sovereignty, security, *ordre public* or other essential interests. 5. The requested Party may postpone action on a request if such action would prejudice criminal investigations or proceedings conducted by its authorities. 6. Before refusing or postponing assistance, the requested Party shall, where appropriate after having consulted with the requesting Party, consider whether the request may be granted partially or subject to such conditions as it deems necessary. 7. The requested Party shall promptly inform the requesting Party of the outcome of the execution of a request for assistance. Reasons shall be given for any refusal or postponement of the request. The requested Party shall also inform the requesting Party of any reasons that render impossible the execution of the request or are likely to delay it significantly. 8. The requesting Party may request that the requested Party keep confidential the fact of any request made under this chapter as well as its subject, except to the extent necessary for its execution. If the requested Party cannot comply with the request for confidentiality, it shall promptly inform the requesting Party, which shall then determine whether the request should nevertheless be executed. 9. a In the event of urgency, requests for mutual assistance or communications related thereto may be sent directly by judicial authorities of the requesting Party to such authorities of the requested Party. In any such cases, a copy shall be sent at the same time to the central authority of the requested Party through the central authority of the requesting Party. b Any request or communication under this paragraph may be made through the International Criminal Police Organisation (Interpol). c Where a request is made pursuant to sub-paragraph a. of this article and the authority is not competent to deal with the request, it shall refer the request to the competent national authority and inform directly the requesting Party that it has done so. d Requests or communications made under this paragraph that do not involve coercive action may be directly transmitted by the competent authorities of the requesting Party to the competent authorities of the requested Party.	

e Each Party may, at the time of signature or when depositing its instrument of ratification, acceptance, approval or accession, inform the Secretary General of the Council of Europe that, for reasons of efficiency, requests made under this paragraph are to be addressed to its central authority.	
Article 28 – Confidentiality and limitation on use 1. When there is no mutual assistance treaty or arrangement on the basis of uniform or reciprocal legislation in force between the requesting and the requested Parties, the provisions of this article shall apply. The provisions of this article shall not apply where such treaty, arrangement or legislation exists, unless the Parties concerned agree to apply any or all of the remainder of this article in lieu thereof. 2. The requested Party may make the supply of information or material in response to a request dependent on the condition that it is: a kept confidential where the request for mutual legal assistance could not be complied with in the absence of such condition, or b not used for investigations or proceedings other than those stated in the request. 3. If the requesting Party cannot comply with a condition referred to in paragraph 2, it shall promptly inform the other Party, which shall then determine whether the information should nevertheless be provided. When the requesting Party accepts the condition, it shall be bound by it. 4. Any Party that supplies information or material subject to a condition referred to in paragraph 2 may require the other Party to explain, in relation to that condition, the use made of such information or material.	**Mutual Assistance in Criminal Matters Act** **Chapter 2022** **Request for taking of evidence** 11. (…) (3) Any evidence, thing or photograph or copy of a thing received by the Attorney General pursuant to a request under subsection (1) or (2) may, subject to the provisions of the Criminal Procedure Code, Cap. 54, Evidence Act, Cap. 74, or any other law, be admitted as evidence at any proceedings to which the request relates.
Article 29 – Expedited preservation of stored computer data 1. A Party may request another Party to order or otherwise obtain the expeditious preservation of data stored by means of a computer system, located within the territory of that other Party and in respect of which the requesting Party intends to submit a request for mutual assistance for the search or similar access, seizure or similar securing, or disclosure of the data.	**Expedited preservation of stored computer data** **32.** (1) An investigatory authority may order the expeditious preservation of computer data that has been stored by means of a computer system located within or outside its territory where a mutual assistance request has been obtained from another investigatory authority for the search or similar access, seizure or similar securing, or disclosure of the computer data. (2) A request for preservation made under subsection (1) shall specify - (a) the investigatory authority seeking the preservation;

2. A request for preservation made under paragraph 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 Party 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 from another Party, the requested Party shall take all appropriate measures to preserve expeditiously the specified data in accordance with its domestic law. For the purposes of responding to a request, dual criminality shall not be required as a condition to providing such preservation. 4. A Party that requires dual criminality as a condition for responding to a request for mutual assistance for the search or similar access, seizure or similar securing, or disclosure of stored data may, in respect of offences other than those established in accordance with Articles 2 through 11 of this Convention, reserve the right to refuse the request for preservation under this article in cases where it has reasons to believe that at the time of disclosure the condition of dual criminality cannot be fulfilled. 5. In addition, a request for preservation may only be refused if: a the request concerns an offence which the requested Party considers a political offence or an offence connected with a political offence, or b the requested Party considers that execution of the request is likely to prejudice its sovereignty, security, *ordre public* or other essential interests. 6. Where the requested Party believes that preservation will not ensure the future availability of the data or will threaten the confidentiality of or otherwise prejudice the requesting Party's investigation, it shall promptly so inform the requesting Party, which shall then determine whether the request should nevertheless be executed.	(b) the offence that is the subject of an investigation or prosecution 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 investigatory authority 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 from another investigatory authority, the requested authority shall take all appropriate measures to preserve expeditiously the specified computer data in accordance with its domestic law. (4) For the purposes of responding to a request under this section, dual criminality shall not be required as a condition for providing such preservation. (5) An investigatory authority that requires dual criminality as a condition for responding to a request for mutual assistance for the search or similar access, seizure or similar securing, or disclosure of stored computer data may, in respect of offences, reserve the right to refuse the request for preservation under this Act in cases where it has reasons to believe that at the time of disclosure the condition of dual criminality cannot be fulfilled. (6) A request for preservation may be refused where – (a) the compliance with the request would be contrary to the Constitution; (b) it is of prejudice to the sovereignty, international relations, security, public order, or other public interest of Seychelles; (c) there is reasonable belief that the request for assistance has been made for the purpose of prosecuting a person on account of that person's race, sex, religion, nationality, ethnic origin or political opinions, or that a person's position may be prejudiced for any of those reasons; (d) in the absence of dual criminality, the granting the request would require a court in Seychelles to make an order in respect of any person or property, for conduct which does not constitute an offence, nor gives rise to a confiscation or restraining order, in Seychelles; (e) the request relates to an offence under military law, or a law relating to military obligations, which would not be an offence under ordinary criminal law; (f) the request relates to a political offence or an offence of a political character; (g) the request relates to an offence, the prosecution of which, in the foreign State, would be incompatible with laws of Seychelles on double jeopardy; (h) the request requires Seychelles to carry out measures that are inconsistent with its laws and practice, or that cannot be taken in respect of criminal matters arising in Seychelles; or granting the request in whole or in part would be likely to prejudice the conduct of proceedings in Seychelles. (7) Any preservation effected in response to the request referred to in subsection (1) shall be for a period of not less than sixty days, in order to enable the requesting party to submit a request for the search or similar access, seizure or similar securing, or disclosure of the computer data, and following the receipt of such request, the computer data shall continue to be preserved pending a decision on that request. **Mutual Assistance in Criminal Matters Act, 2022** **Request for the preservation of communication data** **50.** (1) A foreign State may request the Attorney General to assist in the preservation of communications data.

7. Any preservation effected in response to the request referred to in paragraph 1 shall be for a period not less than sixty days, in order to enable the requesting Party to submit a request for the search or similar access, seizure or similar securing, or disclosure of the data. Following the receipt of such a request, the data shall continue to be preserved pending a decision on that request.	(2) The Attorney General may assist in the preservation of communications data where there are reasonable grounds to believe that the communications data held in Seychelles will be relevant to a criminal investigation or proceedings in the foreign State. (3) A request for the preservation of communications data by a foreign State to the Attorney General under this section shall — (a) contain a brief description of criminal investigation and the reasons for the necessity of the preservation of the communications data; (b) contain a description of the communications data to be preserved and its relationship to the criminal investigation or prosecution, and in particular identifying whether the communications data to be preserved includes — (i) subscriber information; (ii) traffic data; (iii) any other information falling within the definition of communications data; (c) contain information to identify the custodian of the stored communications data or the location computer system or relevant technology; (d) indicate the manner and time within which the foreign State intends to submit a substantive request for assistance for the production of the required communications data. (4) Where the Attorney General approves a request under this section, the Attorney General or the Commissioner of Police may make an ex-parte application to the Supreme Court for an order to preserved the required communications data. (5) The preservation of communications data pursuant to a request made under this section shall not exceed a period of 120 days, unless the Supreme Court determines otherwise.
Article 30 – Expedited disclosure of preserved traffic data 1. Where, in the course of the execution of a request made pursuant to Article 29 to preserve traffic data concerning a specific communication, the requested Party discovers that a service provider in another State was involved in the transmission of the communication, the requested Party shall expeditiously disclose to the requesting Party a sufficient amount of traffic data to identify that service provider and the path through which the communication was transmitted. 2. Disclosure of traffic data under paragraph 1 may only be withheld if: a the request concerns an offence which the requested Party considers a political offence or an offence connected with a political offence; or b the requested Party considers that execution of the request is likely to prejudice its sovereignty, security, *ordre public* or other essential interests.	**Expeditious disclosure of preserved traffic data** **33.** (1) Where, in the course of the execution of a request made to subject to Article 29 of the Convention to preserve traffic data concerning a specific communication, the requested investigatory authority discovers that an electronic service provider in another State was involved in the transmission of the communication, the requested investigatory authority shall expeditiously disclose to the requesting investigatory authority a sufficient amount of traffic data to identify that electronic service provider and the path through which the communication was transmitted. (2) The disclosure of traffic data under subsection (1) may be withheld where – (a) the compliance with the request would be contrary to the Constitution; (b) it is of prejudice to the sovereignty, international relations, security, public order, or other public interest of Seychelles; (c) in the reasonable belief that the request for assistance has been made for the purpose of prosecuting a person on account of that person's race, sex, religion, nationality, ethnic origin or political opinions, or that a person's position may be prejudiced for any of those reasons;

	(d) in the absence of dual, criminality, accepting the request would require a court in Seychelles to make an order in respect of any person or property in respect of conduct which does not constitute an offence, nor gives rise to a confiscation or restraining order, in Seychelles; (e) the request relates to an offence under military law, or a law relating to military obligations, which would not be an offence under ordinary criminal law; (f) the request relates to a political offence or an offence of a political character; (g) the request relates to an offence, the prosecution of which, in the foreign State, would be incompatible with laws of Seychelles on double jeopardy; (h) the request requires Seychelles to carry out measures that are inconsistent with its laws and practice, or that cannot be taken in respect of criminal matters arising in Seychelles; or granting the request in whole or in part, on the ground that granting the request immediately would be likely to prejudice the conduct of proceedings in Seychelles.
Article 31 – Mutual assistance regarding accessing of stored computer data 1. A Party may request another Party 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 requested Party, including data that has been preserved pursuant to Article 29. 2. The requested Party shall respond to the request through the application of international instruments, arrangements and laws referred to in Article 23, and in accordance with other relevant provisions of this chapter. 3. The request shall be responded to on an expedited basis where: a there are grounds to believe that relevant data is particularly vulnerable to loss or modification; or b the instruments, arrangements and laws referred to in paragraph 2 otherwise provide for expedited co-operation.	**Mutual assistance regarding accessing of stored computer data** **34.** (1) An investigatory authority may request another investigative authority to search or similarly access, seize or similarly secure, and disclose computer data stored by means of a computer system located within the territory of the requested Party, including computer data that has been preserved subject to Article 29 of the Convention. (2) The requested investigatory authority may respond to the request through the application of international instruments, arrangements and laws subject to Article 23 of the Convention, and in accordance with other relevant provisions of this Act. (3) The request shall be responded to on an expedited basis where - (a) there are grounds to believe that relevant computer data is particularly vulnerable to loss or modification; or (b) the instruments, arrangements and laws referred to in subsection (2) otherwise provide for expedited co-operation.
Article 32 – Trans-border access to stored computer data with consent or where publicly available A Party may, without the authorisation of another Party: 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 Party, if the Party obtains the lawful and voluntary consent of the person who has the lawful authority to disclose the data to the Party through that computer system.	**Trans-border access to stored computer data with consent or where publicly available** **35.** An investigatory authority may, without the authorisation of another authority - (a) access publicly available open source stored computer data, regardless of where the computer data is located geographically; or (b) access or receive, through a computer system in its territory, stored computer data located in another authority, where the investigation authority obtains the lawful and voluntary consent of the person who has the lawful authority to disclose the computer data to the investigation authority through that computer system.

Article 33 – Mutual assistance in the real-time collection of traffic data 1. The Parties shall provide mutual assistance to each other in the real-time collection of traffic data associated with specified communications in their territory transmitted by means of a computer system. Subject to the provisions of paragraph 2, this assistance shall be governed by the conditions and procedures provided for under domestic law. 2. Each Party shall provide such assistance at least with respect to criminal offences for which real-time collection of traffic data would be available in a similar domestic case.	**Mutual assistance in the real-time collection of traffic data** **36.** (1) The investigatory authorities shall provide mutual assistance to each other in the real-time collection of traffic data associated with specified communications in their territory transmitted by means of a computer system, subject to the provisions of subsection (2), this assistance shall be governed by the conditions and procedures provided for under the laws of Seychelles. (2) The assistance under subsection (1) shall be governed by the conditions and procedures provided for under the laws of Seychelles. (3) Each investigatory authority shall provide such assistance at least with respect to offences for which real-time collection of traffic data would be available in a similar domestic case. **Mutual Assistance in Criminal Matters Act, 2022** **Request for the interception of telecommunications** 46.(1) For the purposes of a criminal investigation, the Attorney General may, in accordance with the provisions of this Act and any other written law, execute a request from a foreign State for — (a) the interception and immediate transmission of telecommunications; or (b) the interception, recording and subsequent transmission of telecommunications. (2) A request by a foreign State under this section shall include — (a) confirmation that a lawful interception order or warrant has been issued in connection with the particular criminal investigation by a court or relevant authority in the foreign State, or such actions are being done in accordance with a written law in the foreign State; (b) details of the criminal matter under investigation; (c) the desired duration of the interception; (d) if possible, the provision of sufficient technical data, including the following information — (i) the name of the authority, telecommunications service provider or person with access to the relevant data; (ii) the location at which the data is held; (iii) details of the data of the relevant interception; (iv) such other information that the Attorney General may require the foreign State to provide. **Order for the interception of telecommunications** 47.(1) Where the Attorney General approves a request under section 46, the Attorney General or the Commissioner of Police may make an ex-parte application to the Supreme Court for an order to intercept telecommunications. (2) Where the Supreme Court grants an application under subsection (1), the Supreme Court may — (a) require an authority, a telecommunications service provider or person with access to the data to intercept and retain a specified communication, or communication of a specified description, received or transmitted by that authority, telecommunications service provider or person; (b) authorize a police officer or a competent person to intercept or listen to a conversation provided by the authority, telecommunications service provider or person; (c) authorize a police officer or a competent person to enter any premises and to install on the premises a device for the interception and retention of specified telecommunications; or (d) approve the use of any technology belonging to the Seychelles or the foreign State that may facilitate the interception of telecommunications; (e) make such other orders that the Supreme Court deems appropriate.

Article 34 – Mutual assistance regarding the interception of content data The Parties shall provide mutual assistance to each other in the real-time collection or recording of content data of specified communications transmitted by means of a computer system to the extent permitted under their applicable treaties and domestic laws.	**Mutual assistance regarding the interception of content computer data** **37.** The investigatory authority shall provide mutual assistance to each other in the real-time collection or recording of content computer data of specified communications transmitted by means of a computer system to the extent permitted under their applicable treaties and the laws of Seychelles. **Mutual Assistance in Criminal Matters Act, 2022** **Request for the interception of telecommunications** 46.(1) For the purposes of a criminal investigation, the Attorney General may, in accordance with the provisions of this Act and any other written law, execute a request from a foreign State for — (a) the interception and immediate transmission of telecommunications; or (b) the interception, recording and subsequent transmission of telecommunications. (2) A request by a foreign State under this section shall include — (a) confirmation that a lawful interception order or warrant has been issued in connection with the particular criminal investigation by a court or relevant authority in the foreign State, or such actions are being done in accordance with a written law in the foreign State; (b) details of the criminal matter under investigation; (c) the desired duration of the interception; (d) if possible, the provision of sufficient technical data, including the following information — (i) the name of the authority, telecommunications service provider or person with access to the relevant data; (ii) the location at which the data is held; (iii) details of the data of the relevant interception; (iv) such other information that the Attorney General may require the foreign State to provide. **Order for the interception of telecommunications** 47.(1) Where the Attorney General approves a request under section 46, the Attorney General or the Commissioner of Police may make an ex-parte application to the Supreme Court for an order to intercept telecommunications. (2) Where the Supreme Court grants an application under subsection (1), the Supreme Court may — (a) require an authority, a telecommunications service provider or person with access to the data to intercept and retain a specified communication, or communication of a specified description, received or transmitted by that authority, telecommunications service provider or person; (b) authorize a police officer or a competent person to intercept or listen to a conversation provided by the authority, telecommunications service provider or person; (c) authorize a police officer or a competent person to enter any premises and to install on the premises a device for the interception and retention of specified telecommunications; or (d) approve the use of any technology belonging to the Seychelles or the foreign State that may facilitate the interception of telecommunications; (e) make such other orders that the Supreme Court deems appropriate.

Article 35 – 24/7 Network 1. Each Party 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. Such assistance shall include facilitating, or, if permitted by its domestic law and practice, directly carrying out the following measures: a the provision of technical advice; b the preservation of data pursuant to Articles 29 and 30; c the collection of evidence, the provision of legal information, and locating of suspects. 2. a A Party's point of contact shall have the capacity to carry out communications with the point of contact of another Party on an expedited basis. b If the point of contact designated by a Party is not part of that Party's authority or authorities responsible for international mutual assistance or extradition, the point of contact shall ensure that it is able to co-ordinate with such authority or authorities on an expedited basis. 3. Each Party shall ensure that trained and equipped personnel are available, in order to facilitate the operation of the network.	**Networking** **38.** (1) A point of contact shall be established 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 computer data, or for the collection of evidence in electronic form of a criminal offence and such assistance shall include facilitating, or, if permitted by its domestic law and practice, directly carrying out the measures for - (a) the provision of technical advice; (b) the preservation of computer data pursuant to Articles 29 and 30 of the Convention; (c) the collection of evidence, the provision of legal information, and locating of suspects. (2) An investigatory authority's point of contact shall have the capacity to carry out communications with the point of contact of another authority on an expedited basis. (3) Where the point of contact designated by an investigatory authority is not responsible for international mutual assistance or extradition, the point of contact shall ensure that it is able to co-ordinate with such authority or authorities on an expedited basis. (4) An investigatory authority shall ensure that trained and equipped personnel are available, in order to facilitate the operation of the network.