REPUBLIQUE DE VANUATU

JOURNAL OFFICIEL



REPUBLIC OF VANUATU

OFFICIAL GAZETTE

2 JANVIER 2025 | **EXTRAORDINARY GAZETTE NUMERO SPECIAL NO. 2** | **2 JANUARY 2025**

SONT PUBLIES LES TEXTES SUIVANTS

LOIS

LOI N°12 DE 2024 SUR LA RATIFICATION DE LA CONVENTION DE BUDAPEST SUR LA CYBERCRIMINALITÉ

LOI N°13 DE 2024 SUR LA PROTECTION DES DONNÉES À CARACTÈRE PERSONNEL

LOI N°14 DE 2024 RELATIVE AUX COMMUNICATIONS NUMÉRIQUES PRÉJUDICIABLES

LOI N°15 DE 2024 RELATIVE À L'AUTORITÉ DE LA SÉCURITÉ NUMÉRIQUE

LOI N°16 DE 2024 SUR LA LUTTE CONTRE LE BLANCHIMENT D'ARGENT ET LE FINANCEMENT DU TERRORISME (MODIFICATION)

NOTIFICATION OF PUBLICATION

ACT

BUDAPEST CONVENTION ON CYBERCRIME (RATIFICATION) ACT NO. 12 OF 2024

DATA PROTECTION AND PRIVACY ACT NO. 13 OF 2024

HARMFUL DIGITAL COMMUNICATIONS ACT NO. 14 OF 2024

DIGITAL SAFETY AUTHORITY ACT NO. 15 OF 2024

ANTI-MONEY LAUNDERING AND COUNTER-TERRORISM FINANCING (AMENDMENT) ACT NO. 16 OF 2024

NOTICES

COMPANIES ACT NO. 25 OF 2012

- PUBLIC NOTICE OF CEASING TO CARRY ON BUSINESS IN VANUATU NOTICE NO. 174 OF 2024

UTILITIES REGULATORY AUTHORITY
ACT NO. 11 OF 2007

- MONTHLY ADJUSTED PRICE OF ELECTRICITY OF PORT VILA FOR DECEMBER 2024
  NOTICE NO. 175 OF 2024

- MONTHLY ADJUSTED PRICE OF ELECTRICITY FOR VANUATU UTILITIES AND INFRASTRUCTURE CONCESSION FOR DECEMBER 2024
  NOTICE NO. 176 OF 2024

REPUBLIC OF VANUATU

BUDAPEST CONVENTION ON CYBERCRIME (RATIFICATION) ACT NO. 12 OF 2024

Arrangement of Sections

1 Ratification....2
2 Commencement....2

REPUBLIC OF VANUATU

Assent: **05/12/2024**
Commencement: **02/01/2025**

BUDAPEST CONVENTION ON CYBERCRIME (RATIFICATION) ACT NO. 12 OF 2024

An Act to provide for the ratification of the Budapest Convention on Cybercrime.

Be it enacted by the President and Parliament as follows-

1 Ratification

(1) The Budapest Convention on Cybercrime is ratified.

(2) A copy of the Convention is attached.

2 Commencement

This Act commences on the day on which it is published in the Gazette.

COUNCIL OF EUROPE



CONSEIL DE L'EUROPE

European Treaty Series - No. 185

Convention on Cybercrime

Budapest, 23.XI.2001

Preamble

The member States of the Council of Europe and the other States signatory hereto,

Considering that the aim of the Council of Europe is to achieve a greater unity between its members;

Recognising the value of fostering co-operation with the other States parties to this Convention;

Convinced of the need to pursue, as a matter of priority, a common criminal policy aimed at the protection of society against cybercrime, *inter alia*, by adopting appropriate legislation and fostering international co-operation;

Conscious of the profound changes brought about by the digitalisation, convergence and continuing globalisation of computer networks;

Concerned by the risk that computer networks and electronic information may also be used for committing criminal offences and that evidence relating to such offences may be stored and transferred by these networks;

Recognising the need for co-operation between States and private industry in combating cybercrime and the need to protect legitimate interests in the use and development of information technologies;

Believing that an effective fight against cybercrime requires increased, rapid and well-functioning international co-operation in criminal matters;

Convinced that the present Convention is necessary to deter action directed against the confidentiality, integrity and availability of computer systems, networks and computer data as well as the misuse of such systems, networks and data by providing for the criminalisation of such conduct, as described in this Convention, and the adoption of powers sufficient for effectively combating such criminal offences, by facilitating their detection, investigation and prosecution at both the domestic and international levels and by providing arrangements for fast and reliable international co-operation;

Mindful of the need to ensure a proper balance between the interests of law enforcement and respect for fundamental human rights as enshrined in 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 treaties, which reaffirm the right of everyone to hold opinions without interference, as well as the right to freedom of expression, including the freedom to seek, receive, and impart information and ideas of all kinds, regardless of frontiers, and the rights concerning the respect for privacy;

Mindful also of the right to the protection of personal data, as conferred, for example, by the 1981 Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data;

Considering the 1989 United Nations Convention on the Rights of the Child and the 1999 International Labour Organization Worst Forms of Child Labour Convention;

Taking into account the existing Council of Europe conventions on co-operation in the penal field, as well as similar treaties which exist between Council of Europe member States and other States, and stressing that the present Convention is intended to supplement those conventions in order to make criminal investigations and proceedings concerning criminal offences related to computer systems and data more effective and to enable the collection of evidence in electronic form of a criminal offence;

Welcoming recent developments which further advance international understanding and co-operation in combating cybercrime, including action taken by the United Nations, the OECD, the European Union and the G8;

Recalling Committee of Ministers Recommendations No. R (85) 10 concerning the practical application of the European Convention on Mutual Assistance in Criminal Matters in respect of letters rogatory for the interception of telecommunications, No. R (88) 2 on piracy in the field of copyright and neighbouring rights, No. R (87) 15 regulating the use of personal data in the police sector, No. R (95) 4 on the protection of personal data in the area of telecommunication services, with particular reference to telephone services, as well as No. R (89) 9 on computer-related crime providing guidelines for national legislatures concerning the definition of certain computer crimes and No. R (95) 13 concerning problems of criminal procedural law connected with information technology;

Having regard to Resolution No. 1 adopted by the European Ministers of Justice at their 21st Conference (Prague, 10 and 11 June 1997), which recommended that the Committee of Ministers support the work on cybercrime carried out by the European Committee on Crime Problems (CDPC) in order to bring domestic criminal law provisions closer to each other and enable the use of effective means of investigation into such offences, as well as to Resolution No. 3 adopted at the 23rd Conference of the European Ministers of Justice (London, 8 and 9 June 2000), which encouraged the negotiating parties to pursue their efforts with a view to finding appropriate solutions to enable the largest possible number of States to become parties to the Convention and acknowledged the need for a swift and efficient system of international co-operation, which duly takes into account the specific requirements of the fight against cybercrime;

Having also regard to the Action Plan adopted by the Heads of State and Government of the Council of Europe on the occasion of their Second Summit (Strasbourg, 10 and 11 October 1997), to seek common responses to the development of the new information technologies based on the standards and values of the Council of Europe;

Have agreed as follows:

Chapter I – Use of terms

Article 1 – Definitions

For the purposes of this Convention:

a "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;

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;

c "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

ii any other entity that processes or stores computer data on behalf of such communication service or users of such service.

d "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.

Chapter II – Measures to be taken at the national level

Section 1 – Substantive criminal law

Title 1 – Offences against the confidentiality, integrity and availability of computer data and systems

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.

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.

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.

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.

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 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.

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.

Title 2 – Computer-related offences

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.

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.

Title 3 – Content-related offences

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;

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;

c realistic images representing 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.

Title 4 – Offences related to infringements of copyright and related rights

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 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.

Title 5 – Ancillary liability and sanctions

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.

Section 2 – Procedural law

Title 1 – Common provisions

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.

Title 2 – Expedited preservation of stored computer data

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.

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.

Title 3 – Production order

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, 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.

Title 4 – Search and seizure of stored computer data

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.

5 The powers and procedures referred to in this article shall be subject to Articles 14 and 15.

Title 5 – Real-time collection of computer data

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.

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.

Section 3 – Jurisdiction

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.

4 This Convention does not exclude any criminal jurisdiction exercised by a Party in accordance with its domestic law.

5 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.

Chapter III – International co-operation

Section 1 – General principles

Title 1 – General principles relating to international co-operation

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.

Title 2 – Principles relating to extradition

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 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.

Title 3 – General principles relating to mutual assistance

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.

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 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.

Title 4 – Procedures pertaining to mutual assistance requests in the absence of applicable international agreements

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

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.

Section 2 – Specific provisions

Title 1 – Mutual assistance regarding provisional measures

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.

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.

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.

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.

Title 2 – Mutual assistance regarding investigative powers

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.

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.

Article 33 – Mutual assistance regarding 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.

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.

Title 3 – 24/7 Network

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.

Chapter IV – Final provisions

Article 36 – Signature and entry into force

1 This Convention shall be open for signature by the member States of the Council of Europe and by non-member States which have participated in its elaboration.

2 This Convention is subject to ratification, acceptance or approval. Instruments of ratification, acceptance or approval shall be deposited with the Secretary General of the Council of Europe.

3 This Convention shall enter into force on the first day of the month following the expiration of a period of three months after the date on which five States, including at least three member States of the Council of Europe, have expressed their consent to be bound by the Convention in accordance with the provisions of paragraphs 1 and 2.

4 In respect of any signatory State which subsequently expresses its consent to be bound by it, the Convention shall enter into force on the first day of the month following the expiration of a period of three months after the date of the expression of its consent to be bound by the Convention in accordance with the provisions of paragraphs 1 and 2.

Article 37 – Accession to the Convention

1 After the entry into force of this Convention, the Committee of Ministers of the Council of Europe, after consulting with and obtaining the unanimous consent of the Contracting States to the Convention, may invite any State which is not a member of the Council and which has not participated in its elaboration to accede to this Convention. The decision shall be taken by the majority provided for in Article 20.d. of the Statute of the Council of Europe and by the unanimous vote of the representatives of the Contracting States entitled to sit on the Committee of Ministers.

2 In respect of any State acceding to the Convention under paragraph 1 above, the Convention shall enter into force on the first day of the month following the expiration of a period of three months after the date of deposit of the instrument of accession with the Secretary General of the Council of Europe.

Article 38 – Territorial application

1 Any State may, at the time of signature or when depositing its instrument of ratification, acceptance, approval or accession, specify the territory or territories to which this Convention shall apply.

2 Any State may, at any later date, by a declaration addressed to the Secretary General of the Council of Europe, extend the application of this Convention to any other territory specified in the declaration. In respect of such territory the Convention shall enter into force on the first day of the month following the expiration of a period of three months after the date of receipt of the declaration by the Secretary General.

3 Any declaration made under the two preceding paragraphs may, in respect of any territory specified in such declaration, be withdrawn by a notification addressed to the Secretary General of the Council of Europe. The withdrawal shall become effective on the first day of the month following the expiration of a period of three months after the date of receipt of such notification by the Secretary General.

Article 39 – Effects of the Convention

1 The purpose of the present Convention is to supplement applicable multilateral or bilateral treaties or arrangements as between the Parties, including the provisions of:

- the European Convention on Extradition, opened for signature in Paris, on 13 December 1957 (ETS No. 24);
- the European Convention on Mutual Assistance in Criminal Matters, opened for signature in Strasbourg, on 20 April 1959 (ETS No. 30);
- the Additional Protocol to the European Convention on Mutual Assistance in Criminal Matters, opened for signature in Strasbourg, on 17 March 1978 (ETS No. 99).

2 If two or more Parties have already concluded an agreement or treaty on the matters dealt with in this Convention or have otherwise established their relations on such matters, or should they in future do so, they shall also be entitled to apply that agreement or treaty or to regulate those relations accordingly. However, where Parties establish their relations in respect of the matters dealt with in the present Convention other than as regulated therein, they shall do so in a manner that is not inconsistent with the Convention's objectives and principles.

3 Nothing in this Convention shall affect other rights, restrictions, obligations and responsibilities of a Party.

Article 40 – Declarations

By a written notification addressed to the Secretary General of the Council of Europe, any State may, at the time of signature or when depositing its instrument of ratification, acceptance, approval or accession, declare that it avails itself of the possibility of requiring additional elements as provided for under Articles 2, 3, 6 paragraph 1.b, 7, 9 paragraph 3, and 27, paragraph 9.e.

Article 41 – Federal clause

1 A federal State may reserve the right to assume obligations under Chapter II of this Convention consistent with its fundamental principles governing the relationship between its central government and constituent States or other similar territorial entities provided that it is still able to co-operate under Chapter III.

2 When making a reservation under paragraph 1, a federal State may not apply the terms of such reservation to exclude or substantially diminish its obligations to provide for measures set forth in Chapter II. Overall, it shall provide for a broad and effective law enforcement capability with respect to those measures.

3 With regard to the provisions of this Convention, the application of which comes under the jurisdiction of constituent States or other similar territorial entities, that are not obliged by the constitutional system of the federation to take legislative measures, the federal government shall inform the competent authorities of such States of the said provisions with its favourable opinion, encouraging them to take appropriate action to give them effect.

Article 42 – Reservations

By a written notification addressed to the Secretary General of the Council of Europe, any State may, at the time of signature or when depositing its instrument of ratification, acceptance, approval or accession, declare that it avails itself of the reservation(s) provided for in Article 4, paragraph 2, Article 6, paragraph 3, Article 9, paragraph 4, Article 10, paragraph 3, Article 11, paragraph 3, Article 14, paragraph 3, Article 22, paragraph 2, Article 29, paragraph 4, and Article 41, paragraph 1. No other reservation may be made.

Article 43 – Status and withdrawal of reservations

1 A Party that has made a reservation in accordance with Article 42 may wholly or partially withdraw it by means of a notification addressed to the Secretary General of the Council of Europe. Such withdrawal shall take effect on the date of receipt of such notification by the Secretary General. If the notification states that the withdrawal of a reservation is to take effect on a date specified therein, and such date is later than the date on which the notification is received by the Secretary General, the withdrawal shall take effect on such a later date.

2 A Party that has made a reservation as referred to in Article 42 shall withdraw such reservation, in whole or in part, as soon as circumstances so permit.

3 The Secretary General of the Council of Europe may periodically enquire with Parties that have made one or more reservations as referred to in Article 42 as to the prospects for withdrawing such reservation(s).

Article 44 – Amendments

1 Amendments to this Convention may be proposed by any Party, and shall be communicated by the Secretary General of the Council of Europe to the member States of the Council of Europe, to the non-member States which have participated in the elaboration of this Convention as well as to any State which has acceded to, or has been invited to accede to, this Convention in accordance with the provisions of Article 37.

2 Any amendment proposed by a Party shall be communicated to the European Committee on Crime Problems (CDPC), which shall submit to the Committee of Ministers its opinion on that proposed amendment.

3 The Committee of Ministers shall consider the proposed amendment and the opinion submitted by the CDPC and, following consultation with the non-member States Parties to this Convention, may adopt the amendment.

4 The text of any amendment adopted by the Committee of Ministers in accordance with paragraph 3 of this article shall be forwarded to the Parties for acceptance.

5 Any amendment adopted in accordance with paragraph 3 of this article shall come into force on the thirtieth day after all Parties have informed the Secretary General of their acceptance thereof.

Article 45 – Settlement of disputes

1 The European Committee on Crime Problems (CDPC) shall be kept informed regarding the interpretation and application of this Convention.

2 In case of a dispute between Parties as to the interpretation or application of this Convention, they shall seek a settlement of the dispute through negotiation or any other peaceful means of their choice, including submission of the dispute to the CDPC, to an arbitral tribunal whose decisions shall be binding upon the Parties, or to the International Court of Justice, as agreed upon by the Parties concerned.

Article 46 – Consultations of the Parties

1 The Parties shall, as appropriate, consult periodically with a view to facilitating:

a the effective use and implementation of this Convention, including the identification of any problems thereof, as well as the effects of any declaration or reservation made under this Convention;

b the exchange of information on significant legal, policy or technological developments pertaining to cybercrime and the collection of evidence in electronic form;

c consideration of possible supplementation or amendment of the Convention.

2 The European Committee on Crime Problems (CDPC) shall be kept periodically informed regarding the result of consultations referred to in paragraph 1.

3 The CDPC shall, as appropriate, facilitate the consultations referred to in paragraph 1 and take the measures necessary to assist the Parties in their efforts to supplement or amend the Convention. At the latest three years after the present Convention enters into force, the European Committee on Crime Problems (CDPC) shall, in co-operation with the Parties, conduct a review of all of the Convention's provisions and, if necessary, recommend any appropriate amendments.

4 Except where assumed by the Council of Europe, expenses incurred in carrying out the provisions of paragraph 1 shall be borne by the Parties in the manner to be determined by them.

5 The Parties shall be assisted by the Secretariat of the Council of Europe in carrying out their functions pursuant to this article.

Article 47 – Denunciation

1 Any Party may, at any time, denounce this Convention by means of a notification addressed to the Secretary General of the Council of Europe.

2 Such denunciation shall become effective on the first day of the month following the expiration of a period of three months after the date of receipt of the notification by the Secretary General.

Article 48 – Notification

The Secretary General of the Council of Europe shall notify the member States of the Council of Europe, the non-member States which have participated in the elaboration of this Convention as well as any State which has acceded to, or has been invited to accede to, this Convention of:

a any signature;

b the deposit of any instrument of ratification, acceptance, approval or accession;

c any date of entry into force of this Convention in accordance with Articles 36 and 37;

d any declaration made under Article 40 or reservation made in accordance with Article 42;

e any other act, notification or communication relating to this Convention.

In witness whereof the undersigned, being duly authorised thereto, have signed this Convention.

Done at Budapest, this 23rd day of November 2001, in English and in French, both texts being equally authentic, in a single copy which shall be deposited in the archives of the Council of Europe. The Secretary General of the Council of Europe shall transmit certified copies to each member State of the Council of Europe, to the non-member States which have participated in the elaboration of this Convention, and to any State invited to accede to it.

RÉPUBLIQUE DE VANUATU

LOI N°12 DE 2024 SUR LA RATIFICATION DE LA CONVENTION DE BUDAPEST SUR LA CYBERCRIMINALITÉ

Sommaire

1 Ratification.....2

2 Entrée en vigueur 2

RÉPUBLIQUE DE VANUATU

Promulguée : **05/12/2024**
Entrée en vigueur : **02/01/2025**

LOI N°12 DE 2024 SUR LA RATIFICATION DE LA CONVENTION DE BUDAPEST SUR LA CYBERCRIMINALITÉ

Prévoyant la ratification de la Convention de Budapest sur la Cybercriminalité.

Le Président de la République et le Parlement promulguent le texte suivant :

1 Ratification

1) La Convention de Budapest sur la Cybercriminalité est ratifiée.

2) Une copie de la Convention est jointe en Annexe.

2 Entrée en vigueur

La présente Loi entre en vigueur à la date de sa publication au Journal officiel.

COUNCIL OF EUROPE

CONSEIL DE L'EUROPE

Série des traités européens - n° 185

Convention sur la cybercriminalité

Budapest, 23.XI.2001

Préambule

Les Etats membres du Conseil de l'Europe et les autres Etats signataires,

Considérant que le but du Conseil de l'Europe est de réaliser une union plus étroite entre ses membres;

Reconnaissant l'intérêt d'intensifier la coopération avec les autres Etats parties à la Convention;

Convaincus de la nécessité de mener, en priorité, une politique pénale commune destinée à protéger la société de la criminalité dans le cyberespace, notamment par l'adoption d'une législation appropriée et par l'amélioration de la coopération internationale;

Conscients des profonds changements engendrés par la numérisation, la convergence et la mondialisation permanente des réseaux informatiques;

Préoccupés par le risque que les réseaux informatiques et l'information électronique soient utilisés également pour commettre des infractions pénales et que les preuves de ces infractions soient stockées et transmises par le biais de ces réseaux;

Reconnaissant la nécessité d'une coopération entre les Etats et l'industrie privée dans la lutte contre la cybercriminalité, et le besoin de protéger les intérêts légitimes dans l'utilisation et le développement des technologies de l'information;

Estimant qu'une lutte bien menée contre la cybercriminalité requiert une coopération internationale en matière pénale accrue, rapide et efficace;

Convaincus que la présente Convention est nécessaire pour prévenir les actes portant atteinte à la confidentialité, à l'intégrité et à la disponibilité des systèmes informatiques, des réseaux et des données, ainsi que l'usage frauduleux de tels systèmes, réseaux et données, en assurant l'incrimination de ces comportements, tels que décrits dans la présente Convention, et l'adoption de pouvoirs suffisants pour permettre une lutte efficace contre ces infractions pénales, en en facilitant la détection, l'investigation et la poursuite, tant au plan national qu'au niveau international, et en prévoyant des dispositions matérielles en vue d'une coopération internationale rapide et fiable;

Gardant à l'esprit la nécessité de garantir un équilibre adéquat entre les intérêts de l'action répressive et le respect des droits de l'homme fondamentaux, tels que garantis dans la Convention de sauvegarde des Droits de l'Homme et des Libertés fondamentales du Conseil de l'Europe (1950), dans le Pacte international relatif aux droits civils et politiques des Nations Unies (1966), ainsi que dans d'autres conventions internationales applicables en matière de droits de l'homme, qui réaffirment le droit à ne pas être inquiété pour ses opinions, le droit à la liberté d'expression, y compris la liberté de rechercher, d'obtenir et de communiquer des informations et des idées de toute nature, sans considération de frontière, ainsi que le droit au respect de la vie privée;

Conscients également du droit à la protection des données personnelles, tel que spécifié, par exemple, par la Convention de 1981 du Conseil de l'Europe pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel;

Considérant la Convention des Nations Unies relative aux droits de l'enfant (1989) et la Convention de l'Organisation internationale du travail sur les pires formes de travail des enfants (1999);

Tenant compte des conventions existantes du Conseil de l'Europe sur la coopération en matière pénale, ainsi que d'autres traités similaires conclus entre les Etats membres du Conseil de l'Europe et d'autres Etats, et soulignant que la présente Convention a pour but de les compléter en vue de rendre plus efficaces les enquêtes et les procédures pénales portant sur des infractions pénales en relation avec des systèmes et des données informatiques, ainsi que de permettre la collecte des preuves électroniques d'une infraction pénale;

Se félicitant des récentes initiatives destinées à améliorer la compréhension et la coopération internationales aux fins de la lutte contre la criminalité dans le cyberespace, notamment des actions menées par les Nations Unies, l'OCDE, l'Union européenne et le G8;

Rappelant les Recommandations du Comité des Ministres n° R (85) 10 concernant l'application pratique de la Convention européenne d'entraide judiciaire en matière pénale relative aux commissions rogatoires pour la surveillance des télécommunications, n° R (88) 2 sur des mesures visant à combattre la piraterie dans le domaine du droit d'auteur et des droits voisins, n° R (87) 15 visant à réglementer l'utilisation de données à caractère personnel dans le secteur de la police, n° R (95) 4 sur la protection des données à caractère personnel dans le domaine des services de télécommunication, eu égard notamment aux services téléphoniques, et n° R (89) 9 sur la criminalité en relation avec l'ordinateur, qui indique aux législateurs nationaux des principes directeurs pour définir certaines infractions informatiques, ainsi que n° R (95) 13 relative aux problèmes de procédure pénale liés à la technologie de l'information;

Eu égard à la Résolution n° 1, adoptée par les ministres européens de la Justice lors de leur 21e Conférence (Prague, 10 et 11 juin 1997), qui recommande au Comité des Ministres de soutenir les activités concernant la cybercriminalité menées par le Comité européen pour les problèmes criminels (CDPC) afin de rapprocher les législations pénales nationales et de permettre l'utilisation de moyens d'investigation efficaces en matière d'infractions informatiques, ainsi qu'à la Résolution n° 3, adoptée lors de la 23e Conférence des ministres européens de la Justice (Londres, 8 et 9 juin 2000), qui encourage les parties aux négociations à poursuivre leurs efforts afin de trouver des solutions permettant au plus grand nombre d'Etats d'être parties à la Convention et qui reconnaît la nécessité de disposer d'un mécanisme rapide et efficace de coopération internationale qui tienne dûment compte des exigences spécifiques de la lutte contre la cybercriminalité;

Prenant également en compte le plan d'action adopté par les chefs d'Etat et de gouvernement du Conseil de l'Europe à l'occasion de leur 2e Sommet (Strasbourg, 10 et 11 octobre 1997) afin de trouver des réponses communes au développement des nouvelles technologies de l'information, fondées sur les normes et les valeurs du Conseil de l'Europe,

Sont convenus de ce qui suit:

Chapitre I – Terminologie

Article 1 – Définitions

Aux fins de la présente Convention,

a l'expression «système informatique» désigne tout dispositif isolé ou ensemble de dispositifs interconnectés ou apparentés, qui assure ou dont un ou plusieurs éléments assurent, en exécution d'un programme, un traitement automatisé de données;

b l'expression «données informatiques» désigne toute représentation de faits, d'informations ou de concepts sous une forme qui se prête à un traitement informatique, y compris un programme de nature à faire en sorte qu'un système informatique exécute une fonction;

c l'expression «fournisseur de services» désigne:

i toute entité publique ou privée qui offre aux utilisateurs de ses services la possibilité de communiquer au moyen d'un système informatique, et

ii toute autre entité traitant ou stockant des données informatiques pour ce service de communication ou ses utilisateurs.

d «données relatives au trafic» désigne toutes données ayant trait à une communication passant par un système informatique, produites par ce dernier en tant qu'élément de la chaîne de communication, indiquant l'origine, la destination, l'itinéraire, l'heure, la date, la taille et la durée de la communication ou le type de service sous-jacent.

Chapitre II – Mesures à prendre au niveau national

Section 1 – Droit pénal matériel

Titre 1 – Infractions contre la confidentialité, l'intégrité et la disponibilité des données et systèmes informatiques

Article 2 – Accès illégal

Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour ériger en infraction pénale, conformément à son droit interne, l'accès intentionnel et sans droit à tout ou partie d'un système informatique. Une Partie peut exiger que l'infraction soit commise en violation des mesures de sécurité, dans l'intention d'obtenir des données informatiques ou dans une autre intention délictueuse, ou soit en relation avec un système informatique connecté à un autre système informatique.

Article 3 – Interception illégale

Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour ériger en infraction pénale, conformément à son droit interne, l'interception intentionnelle et sans droit, effectuée par des moyens techniques, de données informatiques, lors de transmissions non publiques, à destination, en provenance ou à l'intérieur d'un système informatique, y compris les émissions électromagnétiques provenant d'un système informatique transportant de telles données informatiques. Une Partie peut exiger que l'infraction soit commise dans une intention délictueuse ou soit en relation avec un système informatique connecté à un autre système informatique.

Article 4 – Atteinte à l'intégrité des données

1 Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour ériger en infraction pénale, conformément à son droit interne, le fait, intentionnel et sans droit, d'endommager, d'effacer, de détériorer, d'altérer ou de supprimer des données informatiques.

2 Une Partie peut se réserver le droit d'exiger que le comportement décrit au paragraphe 1 entraîne des dommages sérieux.

Article 5 – Atteinte à l'intégrité du système

Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour ériger en infraction pénale, conformément à son droit interne, l'entrave grave, intentionnelle et sans droit, au fonctionnement d'un système informatique, par l'introduction, la transmission, l'endommagement, l'effacement, la détérioration, l'altération ou la suppression de données informatiques.

Article 6 – Abus de dispositifs

1 Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour ériger en infraction pénale, conformément à son droit interne, lorsqu'elles sont commises intentionnellement et sans droit:

a la production, la vente, l'obtention pour utilisation, l'importation, la diffusion ou d'autres formes de mise à disposition:

i d'un dispositif, y compris un programme informatique, principalement conçu ou adapté pour permettre la commission de l'une des infractions établies conformément aux articles 2 à 5 ci-dessus;

ii d'un mot de passe, d'un code d'accès ou de données informatiques similaires permettant d'accéder à tout ou partie d'un système informatique,

dans l'intention qu'ils soient utilisés afin de commettre l'une ou l'autre des infractions visées par les articles 2 à 5; et

b la possession d'un élément visé aux paragraphes a.i ou ii ci-dessus, dans l'intention qu'il soit utilisé afin de commettre l'une ou l'autre des infractions visées par les articles 2 à 5. Une Partie peut exiger en droit interne qu'un certain nombre de ces éléments soit détenu pour que la responsabilité pénale soit engagée.

2 Le présent article ne saurait être interprété comme imposant une responsabilité pénale lorsque la production, la vente, l'obtention pour utilisation, l'importation, la diffusion ou d'autres formes de mise à disposition mentionnées au paragraphe 1 du présent article n'ont pas pour but de commettre une infraction établie conformément aux articles 2 à 5 de la présente Convention, comme dans le cas d'essai autorisé ou de protection d'un système informatique.

3 Chaque Partie peut se réserver le droit de ne pas appliquer le paragraphe 1 du présent article, à condition que cette réserve ne porte pas sur la vente, la distribution ou toute autre mise à disposition des éléments mentionnés au paragraphe 1.a.ii du présent article.

Titre 2 – Infractions informatiques

Article 7 – Falsification informatique

Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour ériger en infraction pénale, conformément à son droit interne, l'introduction, l'altération, l'effacement ou la suppression intentionnels et sans droit de données informatiques, engendrant des données non authentiques, dans l'intention qu'elles soient prises en compte ou utilisées à des fins légales comme si elles étaient authentiques, qu'elles soient ou non directement lisibles et intelligibles. Une Partie peut exiger une intention frauduleuse ou une intention délictueuse similaire pour que la responsabilité pénale soit engagée.

Article 8 – Fraude informatique

Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour ériger en infraction pénale, conformément à son droit interne, le fait intentionnel et sans droit de causer un préjudice patrimonial à autrui:

a par toute introduction, altération, effacement ou suppression de données informatiques;

b par toute forme d'atteinte au fonctionnement d'un système informatique,

dans l'intention, frauduleuse ou délictueuse, d'obtenir sans droit un bénéfice économique pour soi-même ou pour autrui.

Titre 3 – Infractions se rapportant au contenu

Article 9 – Infractions se rapportant à la pornographie enfantine

1 Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour ériger en infraction pénale, conformément à son droit interne, les comportements suivants lorsqu'ils sont commis intentionnellement et sans droit:

a la production de pornographie enfantine en vue de sa diffusion par le biais d'un système informatique;

b l'offre ou la mise à disposition de pornographie enfantine par le biais d'un système informatique;

c la diffusion ou la transmission de pornographie enfantine par le biais d'un système informatique;

d le fait de se procurer ou de procurer à autrui de la pornographie enfantine par le biais d'un système informatique;

e la possession de pornographie enfantine dans un système informatique ou un moyen de stockage de données informatiques.

2 Aux fins du paragraphe 1 ci-dessus, le terme «pornographie enfantine» comprend toute matière pornographique représentant de manière visuelle:

a un mineur se livrant à un comportement sexuellement explicite;

b une personne qui apparaît comme un mineur se livrant à un comportement sexuellement explicite;

c des images réalistes représentant un mineur se livrant à un comportement sexuellement explicite.

3 Aux fins du paragraphe 2 ci-dessus, le terme «mineur» désigne toute personne âgée de moins de 18 ans. Une Partie peut toutefois exiger une limite d'âge inférieure, qui doit être au minimum de 16 ans.

4 Une Partie peut se réserver le droit de ne pas appliquer, en tout ou en partie, les paragraphes 1, alinéas d. et e, et 2, alinéas b. et c.

Titre 4 – Infractions liées aux atteintes à la propriété intellectuelle et aux droits connexes

Article 10 – Infractions liées aux atteintes à la propriété intellectuelle et aux droits connexes

1 Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour ériger en infraction pénale, conformément à son droit interne, les atteintes à la propriété intellectuelle, définies par la législation de ladite Partie, conformément aux obligations que celle-ci a souscrites en application de l'Acte de Paris du 24 juillet 1971 portant révision de la Convention de Berne pour la protection des œuvres littéraires et artistiques, de l'Accord sur les aspects commerciaux des droits de propriété intellectuelle et du traité de l'OMPI sur la propriété intellectuelle, à l'exception de tout droit moral conféré par ces conventions, lorsque de tels actes sont commis délibérément, à une échelle commerciale et au moyen d'un système informatique.

2 Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour ériger en infraction pénale, conformément à son droit interne, les atteintes aux droits connexes définis par la législation de ladite Partie, conformément aux obligations que cette dernière a souscrites en application de la Convention internationale pour la protection des artistes interprètes ou exécutants, des producteurs de phonogrammes et des organismes de radiodiffusion (Convention de Rome), de l'Accord relatif aux aspects commerciaux des droits de propriété intellectuelle et du Traité de l'OMPI sur les interprétations et exécutions, et les phonogrammes, à l'exception de tout droit moral conféré par ces conventions, lorsque de tels actes sont commis délibérément, à une échelle commerciale et au moyen d'un système informatique.

3 Une Partie peut, dans des circonstances bien délimitées, se réserver le droit de ne pas imposer de responsabilité pénale au titre des paragraphes 1 et 2 du présent article, à condition que d'autres recours efficaces soient disponibles et qu'une telle réserve ne porte pas atteinte aux obligations internationales incombant à cette Partie en application des instruments internationaux mentionnés aux paragraphes 1 et 2 du présent article.

Titre 5 – Autres formes de responsabilité et de sanctions

Article 11 – Tentative et complicité

1 Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour ériger en infraction pénale, conformément à son droit interne, toute complicité lorsqu'elle est commise intentionnellement en vue de la perpétration d'une des infractions établies en application des articles 2 à 10 de la présente Convention, dans l'intention qu'une telle infraction soit commise.

2 Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour ériger en infraction pénale, conformément à son droit interne, toute tentative intentionnelle de commettre l'une des infractions établies en application des articles 3 à 5, 7, 8, 9.1.a et c de la présente Convention.

3 Chaque Partie peut se réserver le droit de ne pas appliquer, en tout ou en partie, le paragraphe 2 du présent article.

Article 12 – Responsabilité des personnes morales

1 Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour que les personnes morales puissent être tenues pour responsables des infractions établies en application de la présente Convention, lorsqu'elles sont commises pour leur compte par toute personne physique, agissant soit individuellement, soit en tant que membre d'un organe de la personne morale, qui exerce un pouvoir de direction en son sein, fondé:

a sur un pouvoir de représentation de la personne morale;

b sur une autorité pour prendre des décisions au nom de la personne morale;

c sur une autorité pour exercer un contrôle au sein de la personne morale.

2 Outre les cas déjà prévus au paragraphe 1 du présent article, chaque Partie adopte les mesures qui se révèlent nécessaires pour s'assurer qu'une personne morale peut être tenue pour responsable lorsque l'absence de surveillance ou de contrôle de la part d'une personne physique mentionnée au paragraphe 1 a rendu possible la commission des infractions établies en application de la présence Convention pour le compte de ladite personne morale par une personne physique agissant sous son autorité.

3 Selon les principes juridiques de la Partie, la responsabilité d'une personne morale peut être pénale, civile ou administrative.

4 Cette responsabilité est établie sans préjudice de la responsabilité pénale des personnes physiques ayant commis l'infraction.

Article 13 – Sanctions et mesures

1 Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour que les infractions pénales établies en application des articles 2 à 11 soient passibles de sanctions effectives, proportionnées et dissuasives, comprenant des peines privatives de liberté.

2 Chaque Partie veille à ce que les personnes morales tenues pour responsables en application de l'article 12 fassent l'objet de sanctions ou de mesures pénales ou non pénales effectives, proportionnées et dissuasives, comprenant des sanctions pécuniaires.

Section 2 – Droit procédural

Titre 1 – Dispositions communes

Article 14 – Portée d'application des mesures du droit de procédure

1 Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour instaurer les pouvoirs et procédures prévus dans la présente section aux fins d'enquêtes ou de procédures pénales spécifiques.

2 Sauf disposition contraire figurant à l'article 21, chaque Partie applique les pouvoirs et procédures mentionnés dans le paragraphe 1 du présent article:

a aux infractions pénales établies conformément aux articles 2 à 11 de la présente Convention;

b à toutes les autres infractions pénales commises au moyen d'un système informatique; et

c à la collecte des preuves électroniques de toute infraction pénale.

3 a Chaque Partie peut se réserver le droit de n'appliquer les mesures mentionnées à l'article 20 qu'aux infractions ou catégories d'infractions spécifiées dans la réserve, pour autant que l'éventail de ces infractions ou catégories d'infractions ne soit pas plus réduit que celui des infractions auxquelles elle applique les mesures mentionnées à l'article 21. Chaque Partie envisagera de limiter une telle réserve de manière à permettre l'application la plus large possible de la mesure mentionnée à l'article 20.

b Lorsqu'une Partie, en raison des restrictions imposées par sa législation en vigueur au moment de l'adoption de la présente Convention, n'est pas en mesure d'appliquer les mesures visées aux articles 20 et 21 aux communications transmises dans un système informatique d'un fournisseur de services:

i qui est mis en œuvre pour le bénéfice d'un groupe d'utilisateurs fermé, et

ii qui n'emploie pas les réseaux publics de télécommunication et qui n'est pas connecté à un autre système informatique, qu'il soit public ou privé,

cette Partie peut réserver le droit de ne pas appliquer ces mesures à de telles communications. Chaque Partie envisagera de limiter une telle réserve de manière à permettre l'application la plus large possible de la mesure mentionnée aux articles 20 et 21.

Article 15 – Conditions et sauvegardes

1 Chaque Partie veille à ce que l'instauration, la mise en œuvre et l'application des pouvoirs et procédures prévus dans la présente section soient soumises aux conditions et sauvegardes prévues par son droit interne, qui doit assurer une protection adéquate des droits de l'homme et des libertés, en particulier des droits établis conformément aux obligations que celle-ci a souscrites en application de la Convention de sauvegarde des Droits de l'Homme et des Libertés fondamentales du Conseil de l'Europe (1950) et du Pacte international relatif aux droits civils et politiques des Nations Unies (1966), ou d'autres instruments internationaux applicables concernant les droits de l'homme, et qui doit intégrer le principe de la proportionnalité.

2 Lorsque cela est approprié, eu égard à la nature de la procédure ou du pouvoir concerné, ces conditions et sauvegardes incluent, entre autres, une supervision judiciaire ou d'autres formes de supervision indépendante, des motifs justifiant l'application ainsi que la limitation du champ d'application et de la durée du pouvoir ou de la procédure en question.

3 Dans la mesure où cela est conforme à l'intérêt public, en particulier à la bonne administration de la justice, chaque Partie examine l'effet des pouvoirs et procédures dans cette section sur les droits, responsabilités et intérêts légitimes des tiers.

Titre 2 – Conservation rapide de données informatiques stockées

Article 16 – Conservation rapide de données informatiques stockées

1 Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour permettre à ses autorités compétentes d'ordonner ou d'imposer d'une autre manière la conservation rapide de données électroniques spécifiées, y compris des données relatives au trafic, stockées au moyen d'un système informatique, notamment lorsqu'il y a des raisons de penser que celles-ci sont particulièrement susceptibles de perte ou de modification.

2 Lorsqu'une Partie fait application du paragraphe 1 ci-dessus, au moyen d'une injonction ordonnant à une personne de conserver des données stockées spécifiées se trouvant en sa possession ou sous son contrôle, cette Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour obliger cette personne à conserver et à protéger l'intégrité desdites données pendant une durée aussi longue que nécessaire, au maximum de quatre-vingt-dix jours, afin de permettre aux autorités compétentes d'obtenir leur divulgation. Une Partie peut prévoir qu'une telle injonction soit renouvelée par la suite.

3 Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour obliger le gardien des données ou une autre personne chargée de conserver celles-ci à garder le secret sur la mise en œuvre desdites procédures pendant la durée prévue par son droit interne.

4 Les pouvoirs et procédures mentionnés dans le présent article doivent être soumis aux articles 14 et 15.

Article 17 – Conservation et divulgation rapides de données relatives au trafic

1 Afin d'assurer la conservation des données relatives au trafic, en application de l'article 16, chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires:

a pour veiller à la conservation rapide de ces données relatives au trafic, qu'un seul ou plusieurs fournisseurs de services aient participé à la transmission de cette communication; et

b pour assurer la divulgation rapide à l'autorité compétente de la Partie, ou à une personne désignée par cette autorité, d'une quantité suffisante de données relatives au trafic pour permettre l'identification par la Partie des fournisseurs de services et de la voie par laquelle la communication a été transmise.

2 Les pouvoirs et procédures mentionnés dans le présent article doivent être soumis aux articles 14 et 15.

Titre 3 – Injonction de produire

Article 18 – Injonction de produire

1 Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour habiliter ses autorités compétentes à ordonner:

a à une personne présente sur son territoire de communiquer les données informatiques spécifiées, en sa possession ou sous son contrôle, qui sont stockées dans un système informatique ou un support de stockage informatique; et

b à un fournisseur de services offrant des prestations sur le territoire de la Partie, de communiquer les données en sa possession ou sous son contrôle relatives aux abonnés et concernant de tels services.

2 Les pouvoirs et procédures mentionnés dans le présent article doivent être soumis aux articles 14 et 15.

3 Aux fins du présent article, l'expression «données relatives aux abonnés» désigne toute information, sous forme de données informatiques ou sous toute autre forme, détenue par un fournisseur de services et se rapportant aux abonnés de ses services, autres que des données relatives au trafic ou au contenu, et permettant d'établir:

a le type de service de communication utilisé, les dispositions techniques prises à cet égard et la période de service;

b l'identité, l'adresse postale ou géographique et le numéro de téléphone de l'abonné, et tout autre numéro d'accès, les données concernant la facturation et le paiement, disponibles sur la base d'un contrat ou d'un arrangement de services;

c toute autre information relative à l'endroit où se trouvent les équipements de communication, disponible sur la base d'un contrat ou d'un arrangement de services.

Titre 4 – Perquisition et saisie de données informatiques stockées

Article 19 – Perquisition et saisie de données informatiques stockées

1 Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour habiliter ses autorités compétentes à perquisitionner ou à accéder d'une façon similaire:

a à un système informatique ou à une partie de celui-ci ainsi qu'aux données informatiques qui y sont stockées; et

b à un support du stockage informatique permettant de stocker des données informatiques

sur son territoire.

2 Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour veiller à ce que, lorsque ses autorités perquisitionnent ou accèdent d'une façon similaire à un système informatique spécifique ou à une partie de celui-ci, conformément au paragraphe 1.a, et ont des raisons de penser que les données recherchées sont stockées dans un autre système informatique ou dans une partie de celui-ci situé sur son territoire, et que ces données sont légalement accessibles à partir du système initial ou disponibles pour ce système initial, lesdites autorités soient en mesure d'étendre rapidement la perquisition ou l'accès d'une façon similaire à l'autre système.

3 Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour habiliter ses autorités compétentes à saisir ou à obtenir d'une façon similaire les données informatiques pour lesquelles l'accès a été réalisé en application des paragraphes 1 ou 2. Ces mesures incluent les prérogatives suivantes:

a saisir ou obtenir d'une façon similaire un système informatique ou une partie de celui-ci, ou un support de stockage informatique;

b réaliser et conserver une copie de ces données informatiques;

c préserver l'intégrité des données informatiques stockées pertinentes;

d rendre inaccessibles ou enlever ces données informatiques du système informatique consulté.

4 Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour habiliter ses autorités compétentes à ordonner à toute personne connaissant le fonctionnement du système informatique ou les mesures appliquées pour protéger les données informatiques qu'il contient de fournir toutes les informations raisonnablement nécessaires, pour permettre l'application des mesures visées par les paragraphes 1 et 2.

5 Les pouvoirs et procédures mentionnés dans cet article doivent être soumis aux articles 14 et 15.

Titre 5 – Collecte en temps réel de données informatiques

Article 20 – Collecte en temps réel des données relatives au trafic

1 Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour habiliter ses autorités compétentes:

a à collecter ou enregistrer par l'application de moyens techniques existant sur son territoire, et

b à obliger un fournisseur de services, dans le cadre de ses capacités techniques existantes:

i à collecter ou à enregistrer par l'application de moyens techniques existant sur son territoire, ou

iii à prêter aux autorités compétentes son concours et son assistance pour collecter ou enregistrer,

en temps réel, les données relatives au trafic associées à des communications spécifiques transmises sur son territoire au moyen d'un système informatique.

2 Lorsqu'une Partie, en raison des principes établis de son ordre juridique interne, ne peut adopter les mesures énoncées au paragraphe 1.a, elle peut à la place, adopter les mesures législatives et autres qui se révèlent nécessaires pour assurer la collecte ou l'enregistrement en temps réel des données relatives au trafic associées à des communications spécifiques transmises sur son territoire par l'application de moyens techniques existant sur ce territoire.

3 Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour obliger un fournisseur de services à garder secrets le fait que l'un quelconque des pouvoirs prévus dans le présent article a été exécuté ainsi que toute information à ce sujet.

4 Les pouvoirs et procédures mentionnés dans le présent article doivent être soumis aux articles 14 et 15.

Article 21 – Interception de données relatives au contenu

1 Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour habiliter ses autorités compétentes en ce qui concerne un éventail d'infractions graves à définir en droit interne :

a à collecter ou à enregistrer par l'application de moyens techniques existant sur son territoire, et

b à obliger un fournisseur de services, dans le cadre de ses capacités techniques:

i à collecter ou à enregistrer par l'application de moyens techniques existant sur son territoire, ou

ii à prêter aux autorités compétentes son concours et son assistance pour collecter ou enregistrer,

en temps réel, les données relatives au contenu de communications spécifiques sur son territoire, transmises au moyen d'un système informatique.

2 Lorsqu'une Partie, en raison des principes établis dans son ordre juridique interne, ne peut adopter les mesures énoncées au paragraphe 1.a, elle peut à la place adopter les mesures législatives et autres qui se révèlent nécessaires pour assurer la collecte ou l'enregistrement en temps réel des données relatives au contenu de communications spécifiques transmises sur son territoire par l'application de moyens techniques existant sur ce territoire.

3 Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour obliger un fournisseur de services à garder secrets le fait que l'un quelconque des pouvoirs prévus dans le présent article a été exécuté, ainsi que toute information à ce sujet.

4 Les pouvoirs et procédures mentionnés dans le présent article doivent être soumis aux articles 14 et 15.

Section 3 – Compétence

Article 22 – Compétence

1 Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour établir sa compétence à l'égard de toute infraction pénale établie conformément aux articles 2 à 11 de la présente Convention, lorsque l'infraction est commise:

a sur son territoire; ou

b à bord d'un navire battant pavillon de cette Partie; ou

c à bord d'un aéronef immatriculé selon les lois de cette Partie; ou

d par un de ses ressortissants, si l'infraction est punissable pénalement là où elle a été commise ou si l'infraction ne relève de la compétence territoriale d'aucun Etat.

2 Chaque Partie peut se réserver le droit de ne pas appliquer, ou de n'appliquer que dans des cas ou des conditions spécifiques, les règles de compétence définies aux paragraphes 1.b à 1.d du présent article ou dans une partie quelconque de ces paragraphes.

3 Chaque Partie adopte les mesures qui se révèlent nécessaires pour établir sa compétence à l'égard de toute infraction mentionnée à l'article 24, paragraphe 1, de la présente Convention, lorsque l'auteur présumé de l'infraction est présent sur son territoire et ne peut être extradé vers une autre Partie au seul titre de sa nationalité, après une demande d'extradition.

4 La présente Convention n'exclut aucune compétence pénale exercée par une Partie conformément à son droit interne.

5 Lorsque plusieurs Parties revendiquent une compétence à l'égard d'une infraction présumée visée dans la présente Convention, les Parties concernées se concertent, lorsque cela est opportun, afin de déterminer la mieux à même d'exercer les poursuites.

Chapitre III – Coopération internationale

Section 1 – Principes généraux

Titre 1 – Principes généraux relatifs à la coopération internationale

Article 23 – Principes généraux relatifs à la coopération internationale

Les Parties coopèrent les unes avec les autres, conformément aux dispositions du présent chapitre, en application des instruments internationaux pertinents sur la coopération internationale en matière pénale, des arrangements reposant sur des législations uniformes ou réciproques et de leur droit national, dans la mesure la plus large possible, aux fins d'investigations ou de procédures concernant les infractions pénales liées à des systèmes et des données informatiques ou pour recueillir les preuves, sous forme électronique, d'une infraction pénale.

Titre 2 – Principes relatifs à l'extradition

Article 24 – Extradition

1 a Le présent article s'applique à l'extradition entre les Parties pour les infractions pénales définies conformément aux articles 2 à 11 de la présente Convention, à condition qu'elles soient punissables dans la législation des deux Parties concernées par une peine privative de liberté pour une période maximale d'au moins un an, ou par une peine plus sévère.

b Lorsqu'il est exigé une peine minimale différente, sur la base d'un traité d'extradition tel qu'applicable entre deux ou plusieurs parties, y compris la Convention européenne d'extradition (STE n° 24), ou d'un arrangement reposant sur des législations uniformes ou réciproques, la peine minimale prévue par ce traité ou cet arrangement s'applique.

2 Les infractions pénales décrites au paragraphe 1 du présent article sont considérées comme incluses en tant qu'infractions pouvant donner lieu à extradition dans tout traité d'extradition existant entre ou parmi les Parties. Les Parties s'engagent à inclure de telles infractions comme infractions pouvant donner lieu à extradition dans tout traité d'extradition pouvant être conclu entre ou parmi elles.

3 Lorsqu'une Partie conditionne l'extradition à l'existence d'un traité et reçoit une demande d'extradition d'une autre Partie avec laquelle elle n'a pas conclu de traité d'extradition, elle peut considérer la présente Convention comme fondement juridique pour l'extradition au regard de toute infraction pénale mentionnée au paragraphe 1 du présent article.

4 Les Parties qui ne conditionnent pas l'extradition à l'existence d'un traité reconnaissent les infractions pénales mentionnées au paragraphe 1 du présent article comme des infractions pouvant donner lieu entre elles à l'extradition.

5 L'extradition est soumise aux conditions prévues par le droit interne de la Partie requise ou par les traités d'extradition en vigueur, y compris les motifs pour lesquels la Partie requise peut refuser l'extradition.

6 Si l'extradition pour une infraction pénale mentionnée au paragraphe 1 du présent article est refusée uniquement sur la base de la nationalité de la personne recherchée ou parce que la Partie requise s'estime compétente pour cette infraction, la Partie requise soumet l'affaire, à la demande de la Partie requérante, à ses autorités compétentes aux fins de poursuites, et rendra compte, en temps utile, de l'issue de l'affaire à la Partie requérante. Les autorités en question prendront leur décision et mèneront l'enquête et la procédure de la même manière

que pour toute autre infraction de nature comparable, conformément à la législation de cette Partie.

7 a Chaque Partie communique au Secrétaire Général du Conseil de l'Europe, au moment de la signature ou du dépôt de son instrument de ratification, d'acceptation, d'approbation ou d'adhésion, le nom et l'adresse de chaque autorité responsable de l'envoi ou de la réception d'une demande d'extradition ou d'arrestation provisoire, en l'absence de traité.

b Le Secrétaire Général du Conseil de l'Europe établit et tient à jour un registre des autorités ainsi désignées par les Parties. Chaque Partie doit veiller en permanence à l'exactitude des données figurant dans le registre.

Titre 3 – Principes généraux relatifs à l'entraide

Article 25 – Principes généraux relatifs à l'entraide

1 Les Parties s'accordent l'entraide la plus large possible aux fins d'investigations ou de procédures concernant les infractions pénales liées à des systèmes et à des données informatiques, ou afin de recueillir les preuves sous forme électronique d'une infraction pénale.

2 Chaque Partie adopte également les mesures législatives et autres qui se révèlent nécessaires pour s'acquitter des obligations énoncées aux articles 27 à 35.

3 Chaque Partie peut, en cas d'urgence, formuler une demande d'entraide ou les communications s'y rapportant par des moyens rapides de communication, tels que la télécopie ou le courrier électronique, pour autant que ces moyens offrent des conditions suffisantes de sécurité et d'authentification (y compris, si nécessaire, le cryptage), avec confirmation officielle ultérieure si l'Etat requis l'exige. L'Etat requis accepte la demande et y répond par n'importe lequel de ces moyens rapides de communication.

4 Sauf disposition contraire expressément prévue dans les articles du présent chapitre, l'entraide est soumise aux conditions fixées par le droit interne de la Partie requise ou par les traités d'entraide applicables, y compris les motifs sur la base desquels la Partie requise peut refuser la coopération. La Partie requise ne doit pas exercer son droit de refuser l'entraide concernant les infractions visées aux articles 2 à 11 au seul motif que la demande porte sur une infraction qu'elle considère comme de nature fiscale.

5 Lorsque, conformément aux dispositions du présent chapitre, la Partie requise est autorisée à subordonner l'entraide à l'existence d'une double incrimination, cette condition sera considérée comme satisfaite si le comportement constituant l'infraction, pour laquelle l'entraide est requise, est qualifié d'infraction pénale par son droit interne, que le droit interne classe ou non l'infraction dans la même catégorie d'infractions ou qu'il la désigne ou non par la même terminologie que le droit de la Partie requérante.

Article 26 – Information spontanée

1 Une Partie peut, dans les limites de son droit interne et en l'absence de demande préalable, communiquer à une autre Partie des informations obtenues dans le cadre de ses propres enquêtes lorsqu'elle estime que cela pourrait aider la Partie destinataire à engager ou à mener à bien des enquêtes ou des procédures au sujet d'infractions pénales établies conformément à la présente Convention, ou lorsque ces informations pourraient aboutir à une demande de coopération formulée par cette Partie au titre du présent chapitre.

2 Avant de communiquer de telles informations, la Partie qui les fournit peut demander qu'elles restent confidentielles ou qu'elles ne soient utilisées qu'à certaines conditions. Si la Partie destinataire ne peut faire droit à cette demande, elle doit en informer l'autre Partie, qui devra alors déterminer si les informations en question devraient néanmoins être fournies. Si la Partie destinataire accepte les informations aux conditions prescrites, elle sera liée par ces dernières.

Titre 4 – Procédures relatives aux demandes d'entraide en l'absence d'accords internationaux applicables

Article 27 – Procédures relatives aux demandes d'entraide en l'absence d'accords internationaux applicables

1 En l'absence de traité d'entraide ou d'arrangement reposant sur des législations uniformes ou réciproques en vigueur entre la Partie requérante et la Partie requise, les dispositions des paragraphes 2 à 9 du présent article s'appliquent. Elles ne s'appliquent pas lorsqu'un traité, un arrangement ou une législation de ce type existent, à moins que les Parties concernées ne décident d'appliquer à la place tout ou partie du reste de cet article.

2 a Chaque Partie désigne une ou plusieurs autorités centrales chargées d'envoyer les demandes d'entraide ou d'y répondre, de les exécuter ou de les transmettre aux autorités compétentes pour leur exécution;

b Les autorités centrales communiquent directement les unes avec les autres;

c Chaque Partie, au moment de la signature ou du dépôt de ses instruments de ratification, d'acceptation, d'approbation ou d'adhésion, communique au Secrétaire Général du Conseil de l'Europe les noms et adresses des autorités désignées en application du présent paragraphe;

d Le Secrétaire Général du Conseil de l'Europe établit et tient à jour un registre des autorités centrales désignées par les Parties. Chaque Partie veille en permanence à l'exactitude des données figurant dans le registre.

3 Les demandes d'entraide sous le présent article sont exécutées conformément à la procédure spécifiée par la Partie requérante, sauf lorsqu'elle est incompatible avec la législation de la Partie requise.

4 Outre les conditions ou les motifs de refus prévus à l'article 25, paragraphe 4, l'entraide peut être refusée par la Partie requise:

a si la demande porte sur une infraction que la Partie requise considère comme étant de nature politique ou liée à une infraction de nature politique; ou

b si la Partie requise estime que le fait d'accéder à la demande risquerait de porter atteinte à sa souveraineté, à sa sécurité, à son ordre public ou à d'autres intérêts essentiels.

5 La Partie requise peut surseoir à l'exécution de la demande si cela risquerait de porter préjudice à des enquêtes ou procédures conduites par ses autorités

6 Avant de refuser ou de différer sa coopération, la Partie requise examine, après avoir le cas échéant consulté la Partie requérante, s'il peut être fait droit à la demande partiellement, ou sous réserve des conditions qu'elle juge nécessaires.

7 La Partie requise informe rapidement la Partie requérante de la suite qu'elle entend donner à la demande d'entraide. Elle doit motiver son éventuel refus d'y faire droit ou l'éventuel ajournement de la demande. La Partie requise informe également la Partie requérante de tout motif rendant l'exécution de l'entraide impossible ou étant susceptible de la retarder de manière significative.

8 La Partie requérante peut demander que la Partie requise garde confidentiels le fait et l'objet de toute demande formulée au titre du présent chapitre, sauf dans la mesure nécessaire à l'exécution de ladite demande. Si la Partie requise ne peut faire droit à cette demande de confidentialité, elle doit en informer rapidement la Partie requérante, qui devra alors déterminer si la demande doit néanmoins être exécutée.

9 a En cas d'urgence, les autorités judiciaires de la Partie requérante peuvent adresser directement à leurs homologues de la Partie requise les demandes d'entraide ou les communications s'y rapportant. Dans un tel cas, copie est adressée simultanément aux autorités centrales de la Partie requise par le biais de l'autorité centrale de la Partie requérante.

b Toute demande ou communication formulée au titre du présent paragraphe peut l'être par l'intermédiaire de l'Organisation internationale de police criminelle (Interpol).

c Lorsqu'une demande a été formulée en application de l'alinéa a. du présent article et lorsque l'autorité n'est pas compétente pour la traiter, elle la transmet à l'autorité nationale compétente et en informe directement la Partie requérante.

d Les demandes ou communications effectuées en application du présent paragraphe qui ne supposent pas de mesure de coercition peuvent être directement transmises par les autorités compétentes de la Partie requérante aux autorités compétentes de la Partie requise.

e Chaque Partie peut informer le Secrétaire Général du Conseil de l'Europe, au moment de la signature ou du dépôt de son instrument de ratification, d'acceptation, d'approbation ou d'adhésion, que, pour des raisons d'efficacité, les demandes faites sous ce paragraphe devront être adressées à son autorité centrale.

Article 28 – Confidentialité et restriction d'utilisation

1 En l'absence de traité d'entraide ou d'arrangement reposant sur des législations uniformes ou réciproques en vigueur entre la Partie requérante et la Partie requise, les dispositions du présent article s'appliquent. Elles ne s'appliquent pas lorsqu'un traité, un arrangement ou une législation de ce type existent, à moins que les Parties concernées ne décident d'appliquer à la place tout ou partie du présent article.

2 La Partie requise peut subordonner la communication d'informations ou de matériels en réponse à une demande:

a à la condition que ceux-ci restent confidentiels lorsque la demande d'entraide ne pourrait être respectée en l'absence de cette condition; ou

b à la condition qu'ils ne soient pas utilisés aux fins d'enquêtes ou de procédures autres que celles indiquées dans la demande.

3 Si la Partie requérante ne peut satisfaire à l'une des conditions énoncées au paragraphe 2, elle en informe rapidement la Partie requise, qui détermine alors si l'information doit néanmoins être fournie. Si la Partie requérante accepte cette condition, elle sera liée par celle-ci.

4 Toute Partie qui fournit des informations ou du matériel soumis à l'une des conditions énoncées au paragraphe 2 peut exiger de l'autre Partie qu'elle lui communique des précisions, en relation avec cette condition, quant à l'usage fait de ces informations ou de ce matériel.

Section 2– Dispositions spécifiques

Titre 1 – Entraide en matière de mesures provisoires

Article 29 – Conservation rapide de données informatiques stockées

1 Une Partie peut demander à une autre Partie d'ordonner ou d'imposer d'une autre façon la conservation rapide de données stockées au moyen d'un système informatique se trouvant sur le territoire de cette autre Partie, et au sujet desquelles la Partie requérante a l'intention de soumettre une demande d'entraide en vue de la perquisition ou de l'accès par un moyen similaire, de la saisie ou de l'obtention par un moyen similaire, ou de la divulgation desdites données.

2 Une demande de conservation faite en application du paragraphe 1 doit préciser:

a l'autorité qui demande la conservation;

b l'infraction faisant l'objet de l'enquête ou de procédures pénales et un bref exposé des faits qui s'y rattachent;

c les données informatiques stockées à conserver et la nature de leur lien avec l'infraction;

d toutes les informations disponibles permettant d'identifier le gardien des données informatiques stockées ou l'emplacement du système informatique;

e la nécessité de la mesure de conservation; et

f le fait que la Partie entend soumettre une demande d'entraide en vue de la perquisition ou de l'accès par un moyen similaire, de la saisie ou de l'obtention par un moyen similaire, ou de la divulgation des données informatiques stockées.

3 Après avoir reçu la demande d'une autre Partie, la Partie requise doit prendre toutes les mesures appropriées afin de procéder sans délai à la conservation des données spécifiées, conformément à son droit interne. Pour pouvoir répondre à une telle demande, la double incrimination n'est pas requise comme condition préalable à la conservation.

4 Une Partie qui exige la double incrimination comme condition pour répondre à une demande d'entraide visant la perquisition ou l'accès similaire, la saisie ou l'obtention par un moyen similaire ou la divulgation des données stockées peut, pour des infractions autres que celles établies conformément aux articles 2 à 11 de la présente Convention, se réserver le droit de refuser la demande de conservation au titre du présent article dans le cas où elle a des raisons de penser que, au moment de la divulgation, la condition de double incrimination ne pourra pas être remplie.

5 En outre, une demande de conservation peut être refusée uniquement:

a si la demande porte sur une infraction que la Partie requise considère comme étant de nature politique ou liée à une infraction de nature politique; ou

b si la Partie requise estime que le fait d'accéder à la demande risquerait de porter atteinte à sa souveraineté, à sa sécurité, à l'ordre public ou à d'autres intérêts essentiels.

6 Lorsque la Partie requise estime que la conservation simple ne suffira pas à garantir la disponibilité future des données, ou compromettra la confidentialité de l'enquête de la Partie requérante, ou nuira d'une autre façon à celle-ci, elle en informe rapidement la Partie requérante, qui décide alors s'il convient néanmoins d'exécuter la demande.

7 Toute conservation effectuée en réponse à une demande visée au paragraphe 1 sera valable pour une période d'au moins soixante jours afin de permettre à la Partie requérante de soumettre une demande en vue de la perquisition ou de l'accès par un moyen similaire, de la saisie ou de l'obtention par un moyen similaire, ou de la divulgation des données. Après la réception d'une telle demande, les données doivent continuer à être conservées en attendant l'adoption d'une décision concernant la demande.

Article 30 – Divulgation rapide de données conservées

1 Lorsque, en exécutant une demande de conservation de données relatives au trafic concernant une communication spécifique formulée en application de l'article 29, la Partie requise découvre qu'un fournisseur de services dans un autre Etat a participé à la transmission de cette communication, la Partie requise divulgue rapidement à la Partie requérante une quantité suffisante de données concernant le trafic, aux fins d'identifier ce fournisseur de services et la voie par laquelle la communication a été transmise.

2 La divulgation de données relatives au trafic en application du paragraphe 1 peut être refusée seulement:

a si la demande porte sur une infraction que la Partie requise considère comme étant de nature politique ou liée à une infraction de nature politique; ou

b si elle considère que le fait d'accéder à la demande risquerait de porter atteinte à sa souveraineté, à sa sécurité, à son ordre public ou à d'autres intérêts essentiels.

Titre 2 – Entraide concernant les pouvoirs d'investigation

Article 31 – Entraide concernant l'accès aux données stockées

1 Une Partie peut demander à une autre Partie de perquisitionner ou d'accéder de façon similaire, de saisir ou d'obtenir de façon similaire, de divulguer des données stockées au moyen d'un système informatique se trouvant sur le territoire de cette autre Partie, y compris les données conservées conformément à l'article 29.

2 La Partie requise satisfait à la demande en appliquant les instruments internationaux, les arrangements et les législations mentionnés à l'article 23, et en se conformant aux dispositions pertinentes du présent chapitre.

3 La demande doit être satisfaite aussi rapidement que possible dans les cas suivants:

a il y a des raisons de penser que les données pertinentes sont particulièrement sensibles aux risques de perte ou de modification; ou

b les instruments, arrangements et législations visés au paragraphe 2 prévoient une coopération rapide.

Article 32 – Accès transfrontière à des données stockées, avec consentement ou lorsqu'elles sont accessibles au public

Une Partie peut, sans l'autorisation d'une autre Partie :

a accéder à des données informatiques stockées accessibles au public (source ouverte), quelle que soit la localisation géographique de ces données; ou

b accéder à, ou recevoir au moyen d'un système informatique situé sur son territoire, des données informatiques stockées situées dans un autre Etat, si la Partie obtient le consentement légal et volontaire de la personne légalement autorisée à lui divulguer ces données au moyen de ce système informatique.

Article 33 – Entraide dans la collecte en temps réel de données relatives au trafic

1 Les Parties s'accordent l'entraide dans la collecte en temps réel de données relatives au trafic, associées à des communications spécifiées sur leur territoire, transmises au moyen d'un système informatique. Sous réserve des dispositions du paragraphe 2, cette entraide est régie par les conditions et les procédures prévues en droit interne.

2 Chaque Partie accorde cette entraide au moins à l'égard des infractions pénales pour lesquelles la collecte en temps réel de données concernant le trafic serait disponible dans une affaire analogue au niveau interne.

Article 34 – Entraide en matière d'interception de données relatives au contenu

Les Parties s'accordent l'entraide, dans la mesure permise par leurs traités et lois internes applicables, pour la collecte ou l'enregistrement en temps réel de données relatives au contenu de communications spécifiques transmises au moyen d'un système informatique.

Titre 3 – Réseau 24/7

Article 35 – Réseau 24/7

1 Chaque Partie désigne un point de contact joignable vingt-quatre heures sur vingt-quatre, sept jours sur sept, afin d'assurer une assistance immédiate pour des investigations concernant les infractions pénales liées à des systèmes et à des données informatiques, ou pour recueillir les preuves sous forme électronique d'une infraction pénale. Cette assistance englobera la facilitation, ou, si le droit et la pratique internes le permettent, l'application directe des mesures suivantes:

a apport de conseils techniques;

b conservation des données, conformément aux articles 29 et 30;

c recueil de preuves, apport d'informations à caractère juridique, et localisation des suspects.

2 a Le point de contact d'une Partie aura les moyens de correspondre avec le point de contact d'une autre Partie selon une procédure accélérée.

b Si le point de contact désigné par une Partie ne dépend pas de l'autorité ou des autorités de cette Partie responsables de l'entraide internationale ou de l'extradition, le point de contact veillera à pouvoir agir en coordination avec cette ou ces autorités, selon une procédure accélérée.

3 Chaque Partie fera en sorte de disposer d'un personnel formé et équipé en vue de faciliter le fonctionnement du réseau.

Chapitre IV – Clauses finales

Article 36 – Signature et entrée en vigueur

1 La présente Convention est ouverte à la signature des Etats membres du Conseil de l'Europe et des Etats non membres qui ont participé à son élaboration.

2 La présente Convention est soumise à ratification, acceptation ou approbation. Les instruments de ratification, d'acceptation ou d'approbation sont déposés près le Secrétaire Général du Conseil de l'Europe.

3 La présente Convention entrera en vigueur le premier jour du mois qui suit l'expiration d'une période de trois mois après la date à laquelle cinq Etats, incluant au moins trois Etats membres du Conseil de l'Europe, auront exprimé leur consentement à être liés par la Convention, conformément aux dispositions des paragraphes 1 et 2.

4 Pour tout Etat signataire qui exprimera ultérieurement son consentement à être lié par la Convention, celle-ci entrera en vigueur le premier jour du mois qui suit l'expiration d'une période de trois mois après la date de l'expression de son consentement à être lié par la Convention, conformément aux dispositions des paragraphes 1 et 2.

Article 37 – Adhésion à la Convention

1 Après l'entrée en vigueur de la présente Convention, le Comité des Ministres du Conseil de l'Europe peut, après avoir consulté les Etats contractants à la Convention et en avoir obtenu l'assentiment unanime, inviter tout Etat non membre du Conseil, n'ayant pas participé à son élaboration, à adhérer à la présente Convention. La décision est prise à la majorité prévue à l'article 20.d du Statut du Conseil de l'Europe et à l'unanimité des représentants des Etats contractants ayant le droit de siéger au Comité des Ministres.

2 Pour tout Etat adhérent à la Convention, conformément au paragraphe 1 ci-dessus, la Convention entrera en vigueur le premier jour du mois qui suit l'expiration d'une période de trois mois après la date de dépôt de l'instrument d'adhésion près le Secrétaire Général du Conseil de l'Europe.

Article 38 – Application territoriale

1 Tout Etat peut, au moment de la signature ou au moment du dépôt de son instrument de ratification, d'acceptation, d'approbation ou d'adhésion, désigner le ou les territoires auxquels s'appliquera la présente Convention.

2 Tout Etat peut, à tout autre moment par la suite, par déclaration adressée au Secrétaire Général du Conseil de l'Europe, étendre l'application de la présente Convention à tout autre territoire désigné dans la déclaration. La Convention entrera en vigueur à l'égard de ce territoire le premier jour du mois qui suit l'expiration d'une période de trois mois après la date de réception de la déclaration par le Secrétaire Général.

3 Toute déclaration faite en application des deux paragraphes précédents peut être retirée, en ce qui concerne tout territoire désigné dans cette déclaration, par notification adressée au Secrétaire Général du Conseil de l'Europe. Le retrait prendra effet le premier jour du mois qui suit l'expiration d'une période de trois mois après la date de réception de ladite notification par le Secrétaire Général.

Article 39 – Effets de la Convention

1 L'objet de la présente Convention est de compléter les traités ou les accords multilatéraux ou bilatéraux applicables existant entre les Parties, y compris les dispositions:

– de la Convention européenne d'extradition, ouverte à la signature le 13 décembre 1957, à Paris (STE n° 24);

– de la Convention européenne d'entraide judiciaire en matière pénale, ouverte à la signature le 20 avril 1959, à Strasbourg (STE n° 30);

– du Protocole additionnel à la Convention européenne d'entraide judiciaire en matière pénale, ouvert à la signature le 17 mars 1978, à Strasbourg (STE n° 99).

2 Si deux ou plusieurs Parties ont déjà conclu un accord ou un traité relatif aux matières traitées par la présente Convention, ou si elles ont autrement établi leurs relations sur ces sujets, ou si elles le feront à l'avenir, elles ont aussi la faculté d'appliquer ledit accord ou traité ou d'établir leurs relations en conséquence, au lieu de la présente Convention. Toutefois, lorsque les Parties établiront leurs relations relatives aux matières faisant l'objet de la présente Convention d'une manière différente de celle y prévue, elles le feront d'une manière qui ne soit pas incompatible avec les objectifs et les principes de la Convention.

3 Rien dans la présente Convention n'affecte d'autres droits, restrictions, obligations et responsabilités d'une Partie.

Article 40 – Déclarations

Par déclaration écrite adressée au Secrétaire Général du Conseil de l'Europe, tout Etat peut, au moment de la signature ou du dépôt de son instrument de ratification, d'acceptation, d'approbation ou d'adhésion, déclarer qu'il se prévaut de la faculté d'exiger, le cas échéant, un ou plusieurs éléments supplémentaires tels que prévus aux articles 2, 3, 6, paragraphe 1.b, 7, 9, paragraphe 3, et 27, paragraphe 9.e.

Article 41 – Clause fédérale

1 Un Etat fédéral peut se réserver le droit d'honorer les obligations contenues dans le chapitre II de la présente Convention dans la mesure où celles-ci sont compatibles avec les principes fondamentaux qui gouvernent les relations entre son gouvernement central et les Etats constituants ou autres entités territoriales analogues, à condition qu'il soit en mesure de coopérer sur la base du chapitre III.

2 Lorsqu'il fait une réserve prévue au paragraphe 1, un Etat fédéral ne saurait faire usage des termes d'une telle réserve pour exclure ou diminuer de manière substantielle ses obligations en vertu du chapitre II. En tout état de cause, il se dote de moyens étendus et effectifs permettant la mise en oeuvre des mesures prévues par ledit chapitre.

3 En ce qui concerne les dispositions de cette Convention dont l'application relève de la compétence législative de chacun des Etats constituants ou autres entités territoriales analogues, qui ne sont pas, en vertu du système constitutionnel de la fédération, tenus de prendre des mesures législatives, le gouvernement fédéral porte, avec son avis favorable, lesdites dispositions à la connaissance des autorités compétentes des Etats constituants, en les encourageant à adopter les mesures appropriées pour les mettre en œuvre.

Article 42 – Réserves

Par notification écrite adressée au Secrétaire Général du Conseil de l'Europe, tout Etat peut, au moment de la signature ou du dépôt de son instrument de ratification, d'acceptation, d'approbation ou d'adhésion, déclarer qu'il se prévaut de la ou les réserves prévues à l'article 4, paragraphe 2, à l'article 6, paragraphe 3, à l'article 9, paragraphe 4, à l'article 10, paragraphe 3, à l'article 11, paragraphe 3, à l'article 14, paragraphe 3, à l'article 22, paragraphe 2, à l'article 29, paragraphe 4, et à l'article 41, paragraphe 1. Aucune autre réserve ne peut être faite.

Article 43 – Statut et retrait des réserves

1 Une Partie qui a fait une réserve conformément à l'article 42 peut la retirer en totalité ou en partie par notification adressée au Secrétaire Général du Conseil de l'Europe. Ce retrait prend effet à la date de réception de ladite notification par le Secrétaire Général. Si la notification indique que le retrait d'une réserve doit prendre effet à une date précise, et si cette date est postérieure à celle à laquelle le Secrétaire Général reçoit la notification, le retrait prend effet à cette date ultérieure.

2 Une Partie qui a fait une réserve comme celles mentionnées à l'article 42 retire cette réserve, en totalité ou en partie, dès que les circonstances le permettent.

3 Le Secrétaire Général du Conseil de l'Europe peut périodiquement demander aux Parties ayant fait une ou plusieurs réserves comme celles mentionnées à l'article 42 des informations sur les perspectives de leur retrait.

Article 44 – Amendements

1 Des amendements à la présente Convention peuvent être proposés par chaque Partie, et sont communiqués par le Secrétaire Général du Conseil de l'Europe aux Etats membres du Conseil de l'Europe, aux Etats non membres ayant pris part à l'élaboration de la présente Convention, ainsi qu'à tout Etat y ayant adhéré ou ayant été invité à y adhérer, conformément aux dispositions de l'article 37.

2 Tout amendement proposé par une Partie est communiqué au Comité européen pour les problèmes criminels (CDPC), qui soumet au Comité des Ministres son avis sur ledit amendement.

3 Le Comité des Ministres examine l'amendement proposé et l'avis soumis par le CDPC et, après consultation avec les Etats non membres parties à la présente Convention, peut adopter l'amendement.

4 Le texte de tout amendement adopté par le Comité des Ministres conformément au paragraphe 3 du présent article est communiqué aux Parties pour acceptation.

5 Tout amendement adopté conformément au paragraphe 3 du présent article entre en vigueur le trentième jour après que toutes les Parties ont informé le Secrétaire Général de leur acceptation.

Article 45 – Règlement des différends

1 Le Comité européen pour les problèmes criminels du Conseil de l'Europe (CDPC) est tenu informé de l'interprétation et de l'application de la présente Convention.

2 En cas de différend entre les Parties sur l'interprétation ou l'application de la présente Convention, les Parties s'efforceront de parvenir à un règlement du différend par la négociation ou par tout autre moyen pacifique de leur choix, y compris la soumission du différend au CDPC, à un tribunal arbitral qui prendra des décisions qui lieront les Parties au différend, ou à la Cour internationale de justice, selon un accord entre les Parties concernées.

Article 46 – Concertation des Parties

1 Les Parties se concertent périodiquement, au besoin, afin de faciliter:

a l'usage et la mise en œuvre effectifs de la présente Convention, y compris l'identification de tout problème en la matière, ainsi que les effets de toute déclaration ou réserve faite conformément à la présente Convention;

b l'échange d'informations sur les nouveautés juridiques, politiques ou techniques importantes observées dans le domaine de la criminalité informatique et la collecte de preuves sous forme électronique;

c l'examen de l'éventualité de compléter ou d'amender la Convention.

2 Le Comité européen pour les problèmes criminels (CDPC) est tenu périodiquement au courant du résultat des concertations mentionnées au paragraphe 1.

3 Le CDPC facilite, au besoin, les concertations mentionnées au paragraphe 1 et adopte les mesures nécessaires pour aider les Parties dans leurs efforts visant à compléter ou amender la Convention. Au plus tard à l'issue d'un délai de trois ans à compter de l'entrée en vigueur de la présente Convention, le CDPC procédera, en coopération avec les Parties, à un réexamen de l'ensemble des dispositions de la Convention et proposera, le cas échéant, les amendements appropriés.

4 Sauf lorsque le Conseil de l'Europe les prend en charge, les frais occasionnés par l'application des dispositions du paragraphe 1 sont supportés par les Parties, de la manière qu'elles déterminent.

5 Les Parties sont assistées par le Secrétariat du Conseil de l'Europe dans l'exercice de leurs fonctions découlant du présent article.

Article 47 – Dénonciation

1 Toute Partie peut, à tout moment, dénoncer la présente Convention par notification au Secrétaire Général du Conseil de l'Europe.

2 La dénonciation prendra effet le premier jour du mois qui suit l'expiration d'une période de trois mois après la date de réception de la notification par le Secrétaire Général.

Article 48 – Notification

Le Secrétaire Général du Conseil de l'Europe notifie aux Etats membres du Conseil de l'Europe, aux Etats non membres ayant pris part à l'élaboration de la présente Convention, ainsi qu'à tout Etat y ayant adhéré ou ayant été invité à y adhérer :

a toute signature;

b le dépôt de tout instrument de ratification, d'acceptation, d'approbation ou d'adhésion;

c toute date d'entrée en vigueur de la présente Convention, conformément à ses articles 36 et 37;

d toute déclaration faite en application de l'article 40 ou toute réserve faite en application de l'article 42;

e tout autre acte, notification ou communication ayant trait à la présente Convention.

En foi de quoi, les soussignés, dûment autorisés à cet effet, ont signé la présente Convention.

Fait à Budapest, le 23 novembre 2001, en français et en anglais, les deux textes faisant également foi, en un seul exemplaire qui sera déposé dans les archives du Conseil de l'Europe. Le Secrétaire Général du Conseil de l'Europe en communiquera copie certifiée conforme à chacun des Etats membres du Conseil de l'Europe, aux Etats non membres qui ont participé à l'élaboration de la Convention et à tout Etat invité à y adhérer.

REPUBLIC OF VANUATU

DATA PROTECTION AND PRIVACY ACT NO. 13 OF 2024

Arrangement of Sections

PART 1 PRELIMINARY MATTERS 3
1 Interpretation 3
2 Application of the Act 5
3 Act to prevail 6

PART 2 RULES RELATING TO PROCESSING OF PERSONAL DATA 7
4 General rules relating to processing of personal data 7
5 Lawful purposes for processing personal data 8
6 Prohibition of processing of special categories of personal data 9
7 Processing personal data of a child or other vulnerable individual 10
8 Consent 11

PART 3 RIGHTS OF THE DATA SUBJECT 13
9 Access to information and personal data 13
10 Restriction of processing of personal data 14
11 Rectifying and erasing personal data 15
12 Objection to the processing of personal data 15
13 Data subject's right not to be subject to automated decision making 15
14 Representation of the data subject 16

PART 4 TRANSBORDER DATA FLOWS 17
15 Conditions for transfer outside of Vanuatu 17
16 Safeguards prior to transfer outside of Vanuatu 17
17 Cross-border transfer for specific situations 17

PART 5 ENFORCEMENT 18
18 Disclosure of document or information 18
19 Application for a search warrant 18

20 Granting of search warrant 19
21 Contents of search warrant 19
22 Extension of a search warrant....19
23 Effects of a search warrant....20

PART 6 OFFENCES 22

24 Non-compliance with a provision of this Act....22
25 Unlawful obtaining and disclosing of personal data....22
26 Alteration of personal data to prevent disclosure to a data subject 22
27 Obstruction of powers of entry to premises....22
28 Destruction, concealment or falsification of information requested by the Deputy Commissioner 22
29 Hindering or obstructing the lawful exercise of powers....22
30 Prohibition on disclosure of information, records and data....23

PART 7 MISCELLANEOUS PROVISIONS 24

31 Regulations 24
32 Commencement 24

REPUBLIC OF VANUATU

Assent: **05/12/2024**
Commencement: **02/01/2025**

DATA PROTECTION AND PRIVACY ACT NO. 13 OF 2024

An Act to provide for data protection and privacy and for related matters.

Be it enacted by the President and Parliament as follows-

PART 1 PRELIMINARY MATTERS

1 Interpretation

In this Act, unless the contrary intention appears:

biometric data means personal data resulting from specific technical processing, which relates to the physical, physiological or behavioural characteristics of a natural person. This data can be used to allow or confirm the unique identification of that natural person, such as facial images or dactyloscopic data;

child means an individual below the age of 18 years;

data centre means a facility (including a cloud) that provides shared access to applications and data using a complex network, computers, and storage infrastructure;

data controller means the natural or legal person, public authority, or any other body which, alone or jointly with others, has decision-making power with respect to data processing;

data processing means any operation or set of operations performed on personal data, such as the collection, storage, preservation, alteration, retrieval, disclosure, making available, erasure, destruction of, or the carrying out of logical or arithmetical operations on such data. Data processing includes processing of personal data in a filing system;

data processor means a natural or legal person, public authority, or any other body which processes personal data on behalf of the data controller;

data server means a computer or platform used for storing, securing, managing, and processing data;

data subject means the person who can be identified, directly or indirectly, via an identifier such as a name, ID number, location data or other biometric data;

Deputy Commissioner means the Deputy Commissioner of Data Protection and Privacy appointed under the Digital Safety Authority Act No. 15 of 2024;

designated contact person means an employee or other natural or legal person designated by the data controller or data processor;

filing system means any structured set of data which are accessible or retrievable according to specific criteria;

fundamental rights and freedoms mean the fundamental rights and freedoms provided under subarticle 5(1) of the Constitution of the Republic of Vanuatu;

genetic data means all data relating to the genetic characteristics of an individual which have been obtained as a result from an analysis of:

(a) a biological sample from the individual concerned, in particular chromosomal, Deoxyribonucleic acid (DNA) or Ribonucleic acid (RNA) analysis; or

(b) any other element enabling equivalent information to be obtained;

legitimate interest includes but is not limited to any commercial, individual or societal interest of a data subject, data processor, data controller or a third party;

personal data means any information or data, whether included in a record or not, which:

(a) relates to a data subject; or

(b) enables singling out or enables interaction with the data subject;

recipient means a natural or legal person, public authority, agency or another body, to which the personal data are disclosed and includes a third party;

special categories of personal data include the following:

(a) genetic data or personal data relating to offences, criminal proceedings and convictions; and

(b) biometric data uniquely identifying a person; and

(c) personal data relating to racial or ethnic origin, political opinions, trade-union membership, religious or other beliefs, health or sexual life;

third party means a natural or legal person, public authority, agency or body other than the data subject, data controller, data processor, designated contact person and other persons who:

(a) are under the direct authority of the data controller or processor; and

(b) are authorised to process personal data;

vulnerable individual means a person who:

(a) may be in need of community care services due to mental illness, developmental disability or delay, other disability, age, illness or emotional disturbance; and

(b) is unable to take care of himself or herself or unable to protect himself or herself against significant harm or serious exploitation.

2 Application of the Act

(1) This Act applies to the following:

(a) processing of personal data in the private and public sectors, whether by automated or non-automated means, irrespective of the nationality or place of residence of the natural person who is the subject of the processing of personal data; and

(b) processing of personal data or special categories of personal data about living individuals and not about deceased persons; and

(c) processing of personal data done within the jurisdiction of Vanuatu; and

(d) processing of personal data generated or collected in Vanuatu, irrespective of where the processing is done; and

(e) processing of personal data of individuals who are in Vanuatu by a data controller or data processor not established in Vanuatu, where the processing activities are related to:

(i) the offering of goods or services to such individuals in Vanuatu, irrespective of whether a payment of the data subject is required; or

(ii) the monitoring of the behaviour of such individuals in Vanuatu subject to their behaviour taking place within Vanuatu.

(2) This Act does not apply to the processing of personal data done purely for personal or household activities.

3 Act to prevail

If a provision of this Act conflicts with a provision of any other Act, the provisions of this Act prevail.

PART 2 RULES RELATING TO PROCESSING OF PERSONAL DATA

4 General rules relating to processing of personal data

(1) Data controllers and data processors must process personal data in accordance with the following rules:

(a) personal data must be processed:

(i) under the requirements of this Act; and

(ii) fairly and in a transparent manner in relation to the data subject; and

(b) personal data must be processed for explicit, specified, and legitimate purposes and the processing of these data must be done for those purposes and must not be incompatible with them; and

(c) personal data must be adequate, relevant, proportional, and not excessive in relation to the purposes for which they are processed, taking into account both the quantity and the quality of personal data being processed; and

(d) personal data must be accurate and, to the extent necessary, be kept up to date and every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are rectified or erased without delay; and

(e) personal data must be preserved in a form which permits identification of data subjects for no longer than is necessary for the purposes for which those data are processed; and

(f) personal data must be processed in a manner that ensures reasonable and appropriate security measures against unauthorised or unlawful processing and against accidental or unauthorised access, destruction, loss, use, modification, or disclosure.

(2) For the purposes of subparagraph (1)(a)(i), personal data is being processed fairly if the personal data is:

(a) being processed in a manner that the data subject would reasonably expect; and

(b) not processed in a manner that may have unjustified adverse effect on the data subject.

(3) For the purposes of subparagraph (1)(a)(ii), personal data is being processed in a transparent manner if:

(a) the data subject is made aware of how the personal data is to be collected, used, or otherwise processed; and

(b) the data subject is made aware as to the extent the personal data will be processed; and

(c) any information or communication relating to the processing of the personal data is easily accessible by the data subject and that information is easy to understand.

(4) Data controllers and data processors must ensure that personal data for archiving purposes must be processed in the public interest, scientific or historical research purposes or statistical purposes and must be processed subject to appropriate safeguards prescribed by Regulations.

(5) Data controllers and data processors must delete personal data once the purpose for which it was processed has been achieved or must only be kept in a form that prevents any direct or indirect identification of the data subject.

5 Lawful purposes for processing personal data

A data controller or data processor may only process personal data for any of the following purposes:

(a) the processing is based on the data subject's consent to the processing for one or more specific purpose; or

(b) the processing is necessary for entering into or for the performance of a contract to which the data subject is a party; or

(c) the processing is necessary to protect the rights or legitimate interests of the data subject or of another natural person; or

(d) the processing is necessary for compliance with a legal obligation to which the data controller is subject to or is necessary for the performance of the function set out under any Act; or

(e) the processing is necessary for a task carried out in the public interest; or

(f) the processing is necessary for the purposes of the legitimate interests of the data controller or a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject, especially where the data subject is a child.

6 Prohibition of processing of special categories of personal data

(1) The processing of special categories of personal data is prohibited.

(2) Despite subsection (1), a data controller or data processor may process special categories of personal data if the special categories of personal data are processed for any of the following purposes:

(a) subject to subsection (3), processing is based on the data subject's consent to the processing for one or more specific purpose; or

(b) processing is necessary for the purpose of carrying out obligations or exercising specific rights of the data controller or of the data subject as set out under this Act or any other Act; or

(c) subject to conditions provided for by this Act or any other Act, processing is necessary for:

(i) the assessment of the working capacity of an employee; or

(ii) for carrying out the obligations and exercising specific rights of the data controller or of the data subject in the field of employment, social security or social protection; or

(d) subject to professional secrecy and conditions provided for by this Act, processing is necessary for preventive medical purposes and purposes of medical diagnosis, administration of care or treatment, management of health services or under a contract with a health professional; or

(e) processing is necessary for reasons of public health, such as monitoring and protecting the public against a life-threatening epidemic or pandemic and its spread or for the purposes of humanitarian actions; or

(f) processing is necessary to protect the legitimate interests of the data subject or of another individual where the data subject is physically or legally incapable of giving consent; or

(g) processing is necessary for the protection of national security, defence, public safety, or the prevention, investigation or prosecution of criminal offences or the execution of criminal penalties; or

(h) processing is carried out in the course of its activities with appropriate safeguards by a foundation, association or any other charitable bodies with a political, philosophical, religious or trade union purpose and on the condition that:

(i) the processing relates solely to the members or to former members of the body (a foundation, association or any other charitable bodies) or to individuals who have regular contact with it in connection with its purposes; and

(ii) the personal data are not disclosed outside that body (a foundation, association or any other charitable bodies) without the consent of the data subjects; or

(i) processing is necessary for the establishment, exercise or defence of legal claims or whenever courts are acting in their judicial capacity; or

(j) subject to conditions provided for by this Act or any other Act, processing is necessary for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes.

(3) For the purposes of paragraphs (2)(b), (e) and (g), the data controller or the data processor must ensure that appropriate measures are in place to safeguard the fundamental rights and freedoms of data subjects.

7 Processing personal data of a child or other vulnerable individual

(1) The processing of the personal data of a child is prohibited.

(2) Despite subsection (1), a data controller or data processor may process personal data of a child for any of the following purposes:

(a) processing is based on the consent given or authorised by the child's parents, carers, or legal representatives unless an Act provides that the child may act by himself or herself without being represented by his or her parents or legal guardian; or

(b) processing is in the legitimate interests of the child; or

(c) processing is necessary to meet a legal obligation to which the data controller is subject to; or

(d) processing is in the public interest as provided by an Act; or

(e) processing is necessary in the context of preventive or counselling services offered directly to the child.

(3) If information and communication relating to processing is addressed to a child, the information and communication must be in a clear and plain language so that the child can easily understand and appropriate mechanisms for age verification must be in place.

(4) When processing personal data relating to vulnerable individuals, data controllers and data processors must:

(a) consider the specific needs of those individuals and relevant accessibility standards; and

(b) ensure that information and communication about data processing must be in a clear and plain language and is accessible to all data subjects regardless of their age, gender, abilities or characteristics.

8 Consent

(1) If the processing of personal data is based on the consent of a data subject, the data controller must be able to demonstrate evidence of such consent.

(2) A consent is deemed not to have been freely given if:

(a) that consent is given under undue influence or pressure of an economic or other nature, whether direct or indirect; or

(b) the data subject has no genuine or free choice or is unable to refuse or withdraw consent without prejudice.

(3) A request for consent must be presented in a manner that:

(a) is clearly distinguishable from other matters; and

(b) uses a clear and plain language.

(4) A data processor must ensure:

(a) that a data subject is able to withdraw any consent given at any time, free of charge; and

(b) in the case of multiple purposes – that consent must be given for each individual and specific purpose; and

(c) that the data subject is informed that he or she may withdraw consent and how he or she may do so.

(5) The withdrawal of consent does not affect the lawfulness of the data processing that occurred before the data controller received the withdrawal of consent.

PART 3 RIGHTS OF THE DATA SUBJECT

9 Access to information and personal data

(1) A data controller must ensure that a data subject is able to obtain, on the data subject's request and within a reasonable time:

(a) confirmation as to whether personal data about the data subject is being processed; and

(b) a copy of the personal data undergoing processing; and

(c) the following information:

(i) the purposes of the processing; and

(ii) the source of the personal data undergoing processing; and

(iii) the recipients or categories of recipients whom the personal data are disclosed; and

(iv) where applicable, the fact that the data controller intends to transfer personal data to another jurisdiction, and if so, to which recipients and in which jurisdiction; and

(v) the period for which personal data will be retained by the data controller or data processor; and

(vi) any other information that the data controller is required to under this Act or any other Act.

(2) The data controller must provide information under subsection (1) in the following manner:

(a) in writing; and

(b) in plain language; and

(c) free of charge; and

(d) within one month after the date of the receipt of a request.

(3) If a request under subsection (1) is too excessive or unreasonable, the data controller may:

(a) charge a reasonable fee based on the administrative costs incurred; or

(b) refuse to act on the request.

(4) If the data controller charges a fee under paragraph (3)(a) or refuses a request under paragraph (3)(b), the data controller bears the burden of proving the excessive or unreasonable nature of the request.

10 Restriction of processing of personal data

(1) A data controller may restrict the processing of personal data upon the request of a data subject in any of the following circumstances:

(a) where the accuracy of the personal data is contested by the data subject, for such period necessary to enable the controller to verify the accuracy of the personal data; or

(b) where the processing is unlawful, but the data subject opposes erasing the personal data and requests the restriction of their use instead; or

(c) where the data controller no longer needs the personal data for the purposes of the processing; or

(d) where the data subject has objected to processing under section 12 pending the verification whether the legitimate grounds of the data controller override those of the data subject.

(2) If the data controller has restricted the processing of personal data under subsection (1), the personal data can only be processed in any of the following circumstances:

(a) with the data subject’s consent; or

(b) for the establishment, exercise or defence of legal claims; or

(c) for the protection of the rights of another natural or legal person; or

(d) for reasons of public interest.

(3) The data controller who has restricted processing of personal data under subsection (1) must inform the data subject before personal data is processed for the purpose under paragraph (2)(b),(c) or (d).

11 Rectifying and erasing personal data

(1) A data controller must ensure that, on a data subject's request, the data subject receives any rectification of inaccurate or incomplete personal data, without delay and free of charge.

(2) A data controller must ensure that, on a data subject's request, the data subject's personal data is erased, without delay and free of charge, if:

(a) the personal data is no longer necessary for the purposes for which it was collected or otherwise processed; or

(b) the data subject withdraws his or her consent on which the processing is based; or

(c) the data subject objects to the processing, under section 12, and the data controller cannot demonstrate an overriding legitimate basis for the processing; or

(d) the personal data is being processed unlawfully; or

(e) the personal data must be erased to comply with a legal obligation to which the data controller is subject to.

(3) The data controller must communicate the data subject's request under subsection (1) or (2) to all recipients to whom the personal data concerned have been disclosed.

(4) Subsection (3) does not apply where the data controller can demonstrate that this is impossible or will involve disproportionate efforts to communicate the data subject's request.

12 Objection to the processing of personal data

A data controller must ensure that the data subject is able to object to the processing of his or her personal data, at any time and free of charge, unless the data controller can demonstrate:

(a) legitimate grounds for the processing which override the interests or fundamental rights and freedoms of the data subject; or

(b) the establishment, exercise, or defence of a legal claim.

13 Data subject's right not to be subject to automated decision making

(1) A data controller must ensure that, on a data subject's request, the data subject must not be subject to a decision significantly affecting him or her

based solely on the automated processing of personal data, including profiling, without having his or her views taken into consideration.

(2) For the purposes of subsection (1), **profiling** means any form of automated processing of personal data to assess certain personal aspects relating to a natural person.

(3) Subsection (1) does not apply if a decision:

(a) is authorized by law to which the data controller is subject; or

(b) is necessary for entering or for the performance of a contract between the data subject and the data controller; or

(c) is based on the data subject's consent and where appropriate guarantees have been put in place.

(4) Where paragraph (3)(b) or (c) applies, the data controller must:

(a) implement suitable measures to safeguard the data subject's fundamental rights and freedoms and legitimate interests; and

(b) provide the data subject the possibility to obtain human intervention on the part of the controller.

(5) Where a decision under subsection (1) is based on special categories of personal data, or personal data of children or personal data concerning vulnerable individuals, the processing must only be carried out if:

(a) conditions for the processing as set out in sections 6 and 7 are met; and

(b) the processing is necessary for reasons of public interest; and

(c) the processing is required by any other Act.

14 Representation of the data subject

A data controller must ensure that a data subject is able to authorise a person, non-profit body, organisation or association to lodge and pursue a complaint, on behalf of the data subject, with the Deputy Commissioner or the Court.

PART 4 TRANSBORDER DATA FLOWS

15 Conditions for transfer outside of Vanuatu

(1) Personal data generated or collected in Vanuatu must not be used elsewhere without prior authorisation of the Minister, on the recommendation of the Deputy Commissioner.

(2) Despite subsection (1), personal data generated or collected in Vanuatu may be transferred to another country or international organisation without the prior authorisation of the Minister if that country or that international organisation has been prescribed by the Minister under subsection (3).

(3) The Minister may, on the recommendation of Deputy Commissioner, by Order, list the countries and international organisations which provide an appropriate level of protection of personal data.

16 Safeguards prior to transfer outside of Vanuatu

In addition to section 15, the Minister may, on the advice of the Deputy Commissioner, prescribe safeguard procedures to be used when transferring personal data outside of Vanuatu if:

(a) the information being request is considered by the Deputy Commissioner to be urgent and sensitive in nature; and

(b) the country or international organisation to which the personal data will be transferred to has been prescribed under subsection 15(3).

17 Cross-border transfer for specific situations

Despite section 15, the Minister on the recommendation of the Deputy Commissioner may authorise the cross-border transfer of personal data to other countries or international organisations which do not ensure an appropriate level of protection may take place if:

(a) the data subject has given explicit, specific and free consent, after being informed of all risks arising with the transfer in the absence of appropriate safeguards; or

(b) the specific interests of the data subject require the transfer in a particular case; or

(c) the transfer is necessary for any purpose approved by the Commission.

PART 5 ENFORCEMENT

18 Disclosure of document or information

(1) If the Deputy Commissioner is satisfied that a data controller is in possession of a document or information that will assist the Deputy Commissioner in determining whether there has been a breach of this Act, the Deputy Commissioner may, in writing, require that data controller to provide such document or information.

(2) The data controller under subsection (1) must comply with the request within 14 days after receiving the request.

(3) The Deputy Commissioner must not disclose any document or information received under this section unless:

(a) authorised by the data controller; or

(b) required by a court order to disclose such document or information; or

(c) the Deputy Commissioner is satisfied that the document or information does not identify any particular data controller or data subject; or

(d) disclosure is required under this Act or any other Act.

19 Application for a search warrant

(1) If the Deputy Commissioner is reasonably satisfied that an offence has been committed under this Act, he or she may request the Commissioner of Police for assistance in making an application for a search warrant.

(2) An application for a search warrant must be in writing and made on oath by the Commissioner of Police, and must set out:

(a) the offence to which the application relates; and

(b) a description of the data centre or a data server; and

(c) the information relied on to support the reasonable suspicion of the commission of the offence; and

(d) the period the search warrant is required.

20 Granting of search warrant

(1) The Court may grant a search warrant if the Court is satisfied with the application of the Commissioner of Police.

(2) Without limiting subsection (1), prior to granting a search warrant, the Court must consider the following:

(a) the seriousness of the offence to which the application relates; and

(b) the reliability of the information on which the application is based, including the nature of the source of the information; and

(c) whether the public interest in the production of data from the data centre or a data server outweighs the right to privacy of a person whose privacy may be affected as a result of the production; and

(d) whether there is sufficient connection between the evidence sought and the offence to which the application relates; and

(e) whether any condition must be included in the search warrant; and

(f) the proposed duration of the search warrant; and

(g) any other matters that the Court considers relevant.

21 Contents of search warrant

A search warrant must state the following information:

(a) a description of the data centre and data server to be searched; and

(b) the offence to which the application relates; and

(c) the types of evidential material that may be searched for; and

(d) the power of the Deputy Commissioner to secure or render inaccessible a data centre or a data server; and

(e) the date and time the search warrant expires; and

(f) any conditions imposed in relation to executing the search warrant.

22 Extension of a search warrant

(1) The Court must specify in the search warrant the date and time the search warrant expires.

(2) The Court may, upon application of the Commissioner of Police, extend the date and time, when a search warrant expires, if it is satisfied that the purpose for which the search warrant was granted cannot be satisfied before the search warrant is expired.

23 Effects of a search warrant

(1) The Commissioner of Police is authorised, under a search warrant granted under section 20, to:

(a) seize an item that the Commissioner of Police believes on reasonable grounds to be:

(i) evidential material in relation to an offence to which the search warrant relates; or

(ii) evidential material that is relevant to another offence under this Act or any other Act; and

(b) access, a data centre or a data server for the purposes of obtaining information and records; and

(c) seize or secure a data server; and

(d) require a person with a knowledge of the data centre or data server to assist the Commissioner of Police in accessing the data centre or a data server; and

(e) move the data server at the place searched to another place for examination in order to determine whether it contains data that could be accessed, collated or seized under the search warrant; and

(f) use the assistance of the Deputy Commissioner or any other person as reasonably necessary for the execution of the search warrant.

(2) If the Commissioner of Police seizes the data server under subsection (1), the Commissioner of Police:

(a) may take possession of it; and

(b) may retain it for such period as he or she considers necessary for the purposes of this Act.

(3) The Commissioner of Police must return the data server under subsection (2) to the data controller if:

(a) it is no longer necessary to seize the data server; or

(b) it is not to be used in evidence.

PART 6 OFFENCES

24 Non-compliance with a provision of this Act

A person who contravenes a provision of this Act commits an offence, punishable on conviction, by a fine not exceeding VT10,000,000.

25 Unlawful obtaining and disclosing of personal data

(1) A person other than the data controller, must not knowingly or recklessly obtain, retain or disclose or procure the disclosure of personal data:

(a) without the authorisation of the data controller; and

(b) with the intention of financial gain or causing harm to the data subject.

(2) A person who contravenes subsection (1) commits an offence, punishable on conviction, by a fine not exceeding VT10,000,000.

26 Alteration of personal data to prevent disclosure to a data subject

A data controller or a data processor, or an employee of a data controller, or data processor, who alters, defaces, blocks, erases, destroys or conceals personal information with the intention of preventing disclosure of all or part of the personal information to a data subject commits an offence, punishable on conviction, by a fine not exceeding VT10,000,000.

27 Obstruction of powers of entry to premises

A person who intentionally obstructs a person in the execution of a search warrant issued under this Act commits an offence, punishable on conviction, by a fine not exceeding VT10,000,000.

28 Destruction, concealment or falsification of information requested by the Deputy Commissioner

A person who destroys, conceals or falsifies all or part of any personal information, document, equipment or material, with the intention of preventing disclosure of personal information to the Deputy Commissioner under section 18 commits an offence, punishable on conviction, by a fine not exceeding VT10,000,000.

29 Hindering or obstructing the lawful exercise of powers

(1) A person must not hinder or obstruct, the Deputy Commissioner, a police officer, or a person assisting a police officer, in exercising out his or her powers under this Act.

(2) A person who contravenes subsection (1) commits an offence, punishable on conviction, by a fine not exceeding VT1,000,000.

30 Prohibition on disclosure of information, records and data

(1) A person who obtains information, extracts, records or data under a request, or search warrant under this Act must not knowingly disclose in whole or in part the information, records or data.

(2) A person who contravenes subsection (1), commits an offence, punishable on conviction, by a fine not exceeding VT2,000,000.

PART 7 MISCELLANEOUS PROVISIONS

31 Regulations

(1) The Minister may, on the advice of the Deputy Commissioner, make Regulations not inconsistent with this Act for the better carrying out or giving effect to the provisions of this Act.

(2) Without limiting the generality of subsection (1), the Regulations may provide for any or all of the following:

(a) how personal data must be processed transparently;

(b) how joint-data controllers are to work together and the obligations that are to be imposed on each or both of the data controllers;

(c) the obligations of the data processors;

(d) security of processing;

(e) record of processing operations;

(f) obligations relating to personal data breaches;

(g) personal data breach notification to data subjects.

32 Commencement

This Act commences on the day on which it is published in the Gazette.

RÉPUBLIQUE DE VANUATU

LOI N°13 DE 2024 SUR LA PROTECTION DES DONNÉES À CARACTÈRE PERSONNEL

Sommaire

TITRE 1 DISPOSITIONS PRELIMINAIRES 3
1 Définition 3
2 Application de la loi 5
3 Loi dominante 6

TITRE 2 REGLES RELATIVES AU TRAITEMENT DE DONNEES A CARACTERE PERSONNEL 7
4 Règles générales relatives au traitement de données à caractère personnel 7
5 Fins légales pour un traitement de données à caractère personnel 8
6 Traitement de catégories particulières de données à caractère personnel 9
7 Traitement de données à caractère personnel d'un enfant ou autre personne vulnérable 11
8 Consentement 12

TITRE 3 DROITS DU SUJET DE DONNEES 13
9 Accès à des informations et à des données personnelles 13
10 Restriction sur le traitement de données personnelles 14
11 Rectification et effacement de données personnelles 15
12 Opposition au traitement de données personnelles 15
13 Droit d'un sujet de données non soumis à un processus de prise de décision automatisé 16
14 Représentation du sujet de données 17

TITRE 4 MOUVEMENTS DE DONNEES TRANSFRONTALIERS 18
15 Conditions de transfert hors du Vanuatu 18
16 Protections préalablement au transfert hors du Vanuatu 18
17 Transfert transfrontalier dans des situations spécifiques 18

TITRE 5 EXECUTION 19
18 Communication de documents ou d'informations 19
19 Requête pour mandat de perquisition 19
20 Octroi de mandat de perquisition 20
21 Contenu d'un mandat de perquisition 20
22 Prorogation d'un mandat de perquisition 21
23 Effets d'un mandat de perquisition 21

TITRE 6 DELITS 23
24 Infraction à une disposition de la présente loi 23
25 Obtention et divulgation illicites de données à caractère personnel 23
26 Modification de données personnelles pour empêcher la divulgation à un sujet de données 23
27 Entrave aux pouvoirs d'entrée dans des locaux 23
28 Destruction ou falsification d'informations demandées par le Commissaire adjoint 23
29 Entrave ou obstruction dans l'exercice légal de pouvoirs 24
30 Défense de communiquer des informations, des registres et des données 24

TITRE 7 DISPOSITIONS DIVERSES 25
31 Règlements 25
32 Entrée en vigueur 25

RÉPUBLIQUE DE VANUATU

Promulguée : **05/12/2024**
Entrée en vigueur : **02/01/2025**

LOI N°13 DE 2024 SUR LA PROTECTION DES DONNÉES À CARACTÈRE PERSONNEL

Disposant de la protection des données à caractère personnel et de questions connexes.

Le Président de la République et le Parlement promulguent le texte qui suit.

TITRE 1 DISPOSITIONS PRELIMINAIRES

1 Définition

Dans la présente loi, sous réserve du contexte :

données biométriques désigne des données personnelles obtenues à partir d'un traitement technique spécifique qui se rapportent aux caractéristiques physiques, physiologiques ou comportementales d'une personne physique. Ces données peuvent servir à permettre ou à confirmer l'identification unique de cette personne physique, telles que des images faciales ou des données dactyloscopiques ;

enfant désigne une personne de moins de 18 ans ;

centre de données désigne un dispositif (y compris un cloud) qui fournit un accès commun à des applications et des données à l'aide d'une infrastructure complexe de réseau, d'ordinateurs et de mémorisation ;

contrôleur des données désigne la personne physique ou morale, l'administration publique ou une autre organisation qui a, seule ou conjointement avec d'autres, un pouvoir décisionnel eu égard au traitement de données ;

traitement de données désigne n'importe quelle opération ou ensemble d'opérations effectuée(s) sur des données personnelles, telle(s) que la collecte, la mémorisation, la préservation, la modification, l'extraction, la communication, la mise à disposition, l'effacement ou la destruction de données personnelles ou l'exécution d'opérations logiques ou arithmétiques sur de telles données. Traitement de données inclut le traitement de données personnelles dans un système de classement ;

processeur de données désigne une personne physique ou morale, une administration publique ou une autre organisation qui traite des données personnelles pour le compte du contrôleur des données ;

serveur de données désigne un ordinateur ou une plateforme qui sert à mémoriser, sécuriser, gérer et traiter des données ;

sujet de données désigne la personne qui peut être identifiée, directement ou indirectement, via un identifiant tel qu'un nom, un numéro d'identification, des données de localisation ou d'autres données biométriques ;

Commissaire adjoint désigne le Commissaire adjoint adjoint de la protection des données à caractère personnel nommé en vertu de la loi No. de 2024 sur l'Autorité de la sécurité numérique ;

interlocuteur désigné désigne un employé ou autre personne physique ou une personne morale désignée par le contrôleur des données ou un processeur ;

système de classement désigne n'importe quel ensemble structuré de données qui sont accessibles ou récupérables suivant des critères spécifiques ;

droits et libertés fondamentaux désigne les droits et libertés fondamentaux prévus par le sous-article 5.1) de la Constitution de la République of Vanuatu;

données génétiques désigne toutes les données se rapportant aux caractéristiques génétiques d'une personne physique obtenues à partir de l'analyse :

a) d'un échantillon biologique de la personne concernée, en particulier analyse chromosomique, de l'ADN (acide désoxyribonucléique) ou de l'ARN (acide ribonucléique) ; ou

b) de tout autre élément permettant d'obtenir des informations équivalentes ;

intérêt légitime inclut, sans s'y limiter, n'importe quel intérêt d'ordre commercial, individuel ou sociétal d'un sujet de données, d'un processeur de données, d'un contrôleur de données ou d'une tierce partie ;

données personnelles ou à caractère personnel désigne toute information ou donnée, qu'elle soit portée dans un registre ou non, laquelle :

a) se rapporte à un sujet de données ; ou

b) permet de sélectionner un sujet de données ou d'interagir avec lui ;

destinataire désigne une personne physique ou morale, une administration publique, agence ou autre organisation à laquelle des données personnelles sont communiquées, et inclut une tierce partie ;

catégories particulières de données personnelles inclut ce qui suit :

a) des données génétiques ou des données personnelles en rapport avec des délits, des poursuites pénales et des condamnations ;

b) des données biométriques identifiant de manière unique une personne ; et

c) des données personnelles se rapportant à l'origine raciale ou ethnique, à des opinions politiques, à l'adhésion à un syndicat, à des croyances religieuses ou autres, à la santé ou à la vie sexuelle ;

tierce partie désigne une personne physique ou morale, une administration publique, agence ou organisation distincte du sujet de données, du contrôleur de données, du processeur de données, de l'interlocuteur désigné et d'autres personnes qui :

a) relèvent directement de l'autorité du contrôleur ou du processeur de données ; et

b) sont autorisées à traiter des données à caractère personnel ;

personne vulnérable désigne une personne qui :

a) pourrait avoir besoin de services d'aide sociale en raison de maladie mentale, d'une déficience mentale ou retard dans son développement, d'un autre handicap, de son âge, d'une maladie ou de troubles affectifs ; et

b) n'est pas en mesure de s'occuper d'elle-même ou de se protéger contre un mal significatif ou une exploitation grave.

2 Application de la loi

1) La présente loi s'applique à ce qui suit :

a) au traitement de données personnelles dans les secteurs privé et public, que ce soit par des moyens automatisés ou non, indépendamment de la nationalité ou du lieu de domicile de la personne physique qui est l'objet du traitement de données à caractère personnel ;

b) au traitement de données personnelles ou de catégories particulières de telles données concernant des personnes vivantes et non pas des personnes décédées ;

c) au traitement de données personnelles dans la juridiction du Vanuatu ;

d) au traitement de données personnelles générées ou recueillies au Vanuatu, indépendamment du lieu où le traitement est effectué ; et

e) au traitement de données personnelles de personnes physiques qui sont au Vanuatu par un contrôleur ou un processeur de données qui n'est pas établi au Vanuatu lorsque les activités de traitement se rapportent à :

i) l'offre de biens ou de services à ces personnes au Vanuatu, indépendamment de savoir si un paiement est exigé du sujet des données ; ou

ii) la surveillance du comportement de ces personnes au Vanuatu dans la mesure où leur comportement se déroule au Vanuatu.

2) La présente loi ne s'applique pas au traitement de données à caractère personnel effectué tout simplement pour des activités personnelles ou domestiques.

3 Loi dominante

Si une disposition de la présente loi est incompatible avec une disposition de n'importe quelle autre loi, ce sont les dispositions de la présente loi qui l'emportent.

TITRE 2 REGLES RELATIVES AU TRAITEMENT DE DONNEES A CARACTERE PERSONNEL

4 Règles générales relatives au traitement de données à caractère personnel

1) Les contrôleurs et les processeurs de données doivent traiter des données à caractère personnel conformément aux règles suivantes :

a) des données à caractère personnel doivent être traitées :

i) en conformité avec les conditions requises de la présente loi; et

ii) de manière juste et transparente eu égard au sujet des données ;

b) des données à caractère personnel doivent être traitées à des fins explicites, spécifiées et légitimes et le traitement desdites données devrait servir à de telles fins et ne pas être incompatibles avec ces fins ;

c) des données à caractère personnel doivent être suffisantes, pertinentes, proportionnelles et non pas excessives par rapport aux fins auxquelles elles sont traitées, en tenant compte à la fois de la quantité et de la qualité des données personnelles en train d'être traitées ;

d) des données à caractère personnel doivent être exactes et, dans la mesure où tel est nécessaire, tenues à jour et toute mesure raisonnable doit être prise pour s'assurer que des données personnelles qui ne sont pas exactes compte tenu des fins auxquelles elles sont traitées, sont corrigées ou effacées sans tarder;

e) des données à caractère personnel doivent être conservées sous une forme qui permet l'identification des sujets de données pour la durée nécessaire, sans plus, pour les besoins pour lesquels les données en question sont traitées ; et

f) des données à caractère personnel doivent être traitées d'une manière qui garantit que des mesures de sécurité raisonnables et appropriées sont prises contre tout traitement non autorisé ou illicite et contre tout accès, destruction, perte, utilisation,

modification ou divulgation, accidentellement ou de façon non autorisée.

2) Aux fins d'application du sous-alinéa 1)a)ii), une donnée personnelle est traitée de manière juste si elle :

a) est traitée d'une manière à laquelle le sujet de données pourrait raisonnablement s'attendre ; et

b) n'est pas traitée d'une manière qui pourrait avoir un effet défavorable injustifié sur le sujet de données.

3) Aux fins d'application de l'alinéa 1)a)ii), une donnée personnelle est traitée de manière transparente si :

a) le sujet de données est informé de la façon dont les données personnelles vont être recueillies, utilisées ou traitées autrement ;

b) le sujet de données est informé du degré auquel les données personnelles seront traitées ; et

c) toute information ou communication en rapport avec le traitement des données personnelles est aisément accessible et compréhensible pour le sujet des données.

4) Des contrôleurs et des processeurs de données doivent s'assurer que le traitement de données personnelles à des fins d'archivage doivent être traitées dans l'intérêt public, à des fins de recherche scientifique ou historique ou à des fins statistiques et sous réserve des protections appropriées prescrites par les règlements.

5) Des contrôleurs et des processeurs de données doivent supprimer les données personnelles dès lors que les fins auxquelles elles ont été traitées ont été réalisées ou elles ne doivent être conservées que sous une forme qui empêche toute identification directe ou indirecte du sujet des données.

5 Fins légales pour un traitement de données à caractère personnel

Un contrôleur ou un processeur de données ne peut traiter des données personnelles que si le traitement est :

a) basé sur le consentement du sujet des données à une ou plusieurs fins spécifiques ;

b) nécessaire pour conclure ou mener à bien un contrat auquel le sujet de données est partie ;

c) nécessaire pour protéger les droits ou les intérêts légitimes du sujet de données ou d'une autre personne physique ;

d) nécessaire pour être en conformité avec une obligation légale à laquelle le contrôleur de données est soumis ou nécessaire pour l'accomplissement de la fonction aux termes de n'importe quelle loi ;

e) nécessaire pour une tâche menée dans l'intérêt public ;

f) nécessaire pour les besoins des intérêts légitimes du contrôleur de données ou d'une tierce partie, sauf si les intérêts ou les droits et libertés fondamentaux du sujet de données l'emportent sur lesdits intérêts, surtout dans le cas où le sujet de données est un enfant.

6 Traitement de catégories particulières de données à caractère personnel

1) Il est interdit de procéder au traitement de catégories particulières de données personnelles.

2) Nonobstant le paragraphe 1), un contrôleur ou un processeur de données peut traiter des catégories particulières de données personnelles si le traitement est :

a) basé, sous réserve du paragraphe 3), sur le consentement du sujet des données à une ou plusieurs fins spécifiques ;

b) nécessaire dans l'accomplissement d'obligations ou l'exercice de droits spécifiques du contrôleur de données ou du sujet des données tels qu'énoncés dans la présente ou toute autre loi ;

c) nécessaire, sous réserve de conditions prévues par la présente ou toute autre loi, pour :

i) évaluer la capacité de travail d'un employé ; ou

ii) remplir des obligations ou exercer des droits spécifiques du contrôleur de données ou du sujet de données dans le domaine de l'emploi, de la sécurité sociale ou de la protection sociale ;

d) nécessaire à des fins de prévention et de diagnostic médicaux, d'administration de soins ou de traitement, de gestion de services de santé ou en vertu d'un contrat avec un professionnel de la santé, sous réserve du secret professionnel et de conditions prévues par la présente loi ;

e) nécessaire pour des raisons de santé publique, telles que la surveillance et la protection du public contre une épidémie fatale et sa propagation ou à des fins d'actions humanitaires ;

f) nécessaire pour protéger les intérêts légitimes du sujet de données ou d'une autre personne physique dans le cas où le sujet de données est physiquement ou légalement incapable de donner son consentement ;

g) nécessaire pour des raisons de sécurité et de défense nationales, de sûreté publique ou pour la prévention, l'investigation ou des poursuites pénales de délits criminels ou l'exécution de peines pénales ;

h) mené par une fondation, une association ou autre organisation à but non lucratif ayant un objet politique, philosophique, religieux ou syndical dans le cadre de ses activités, assorties de protections appropriées, et à condition que :

   i) le traitement se rapporte uniquement aux membres ou anciens membres de l'organisation (une fondation, une association ou autre organisation à but non lucratif) ou à des personnes physiques qui sont régulièrement en contact avec elle dans le cadre de ses objectifs ; et

   ii) les données personnelles ne soient pas divulguées en dehors de ladite organisation (une fondation, une association ou autre organisation à but non lucratif) sans le consentement des sujets de données ;

i) nécessaire pour l'introduction, la poursuite ou la défense d'actions en justice ou lorsque que les tribunaux agissent en leur capacité judiciaire ; ou

j) nécessaire à des fins d'archivage dans l'intérêt public, à des fins de recherche scientifique ou historique ou des fins statistiques, sous réserve de conditions prévues par la présente ou toute autre loi.

3) Aux fins d'application des alinéas 2)b), e) et g), le contrôleur de données ou le processeur de données doit s'assurer que des mesures appropriées sont en place pour protéger les droits et libertés fondamantaux des sujets de données.

7 Traitement de données à caractère personnel d'un enfant ou autre personne vulnérable

1) Il est interdit de procéder au traitement de données personnelles d'un enfant.

2) Nonobstant le paragraphe 1), un contrôleur ou un processeur de données peut traiter des données personnelles d'un enfant si le traitement est :

a) basé sur le consentement donné ou autorisé par les parents de l'enfant, ses tuteurs ou représentants légaux, sauf si une loi dispose que l'enfant peut agir de son propre chef sans être représenté par ses parents ou son tuteur légal ;

b) dans les intérêts légitimes de l'enfant ;

c) nécessaire pour remplir une obligation légale à laquelle le contrôleur de données est soumis ;

d) dans l'intérêt public comme prévu par une loi ; ou

e) nécessaire dans le contexte de services préventifs ou de soutien psychosocial proposés directement à l'enfant.

3) Si une information et une communication en rapport avec le traitement sont adressées à un enfant, elles doivent être dans un langage clair et simple de sorte que l'enfant puisse facilement les comprendre et des mécanismes appropriés doivent être en place pour en vérifier l'âge.

4) Lorsqu'ils traitents des données personnelles relatives à des personnes vulnérables, les contrôleurs et processeurs de données doivent :

a) prendre en considération les besoins particuliers de telles personnes et les normes pertinentes en termes d'accessibilité ; et

b) s'assurer que les informations et les communications sur le traitement de données sont dans un langage clair et simple et aisément accessibles pour tous les sujets de données, quels que soient leur âge, leur sexe, leurs aptitudes ou leurs caractéristiques.

8 Consentement

1) Si le traitement de données personnelles est basé sur le consentement d'un sujet de données, le contrôleur de données doit pouvoir montrer la preuve d'un tel consentement.

2) Un consentement est réputé ne pas avoir été donné librement si :

   a) ledit consentement est donné par abus d'autorité ou sous pression d'ordre économique ou autre, que ce soit directement ou indirectement ; ou

   b) le sujet des données n'a pas vraiment le choix ou n'est pas libre de choisir ou n'est pas en mesure de refuser ou de retirer son consentement sans préjudice.

3) Une demande de consentement doit être présentée d'une manière qui :

   a) se distingue clairement d'autres affaires ; et

   b) est exprimée dans un langage clair et simple.

4) Un processeur de données doit s'assurer :

   a) qu'un sujet de données a la possibilité de rétracter un consentement donné à n'importe quel moment, et à titre gratuit ;

   b) que, dans le cas de fins multiples, le consentement est donné pour chaque personne et chaque fin spécifique ; et

   c) que le sujet des données est informé qu'il peut rétracter son consentement et comment le faire.

5) La rétractation d'un consentement n'affecte pas la légalité du traitement de données qui a été effectué avant que le contrôleur de données ne la reçoive.

TITRE 3 DROITS DU SUJET DE DONNEES

9 Accès à des informations et à des données personnelles

1) Un contrôleur de données doit s'assurer qu'un sujet de données peut obtenir, sur demande et dans un délai acceptable :

a) une confirmation quant à la question de savoir si ses données personnelles sont en train d'être traitées ;

b) une copie des données personnelles sous traitement ; et

c) les informations suivantes :

i) les buts du traitement ;

ii) la source des données personnelles sous traitement ;

iii) les destinataires ou les catégories de destinataires auxquels les données personnelles sont communiquées ;

iv) si, le cas échéant, le contrôleur de données a l'intention de transférer les données personnelles a une autre juridiction, et si oui, à quels destinataires et dans quelle juridiction ;

v) la durée de temps pendant laquelle les données personnelles seront conservées par le contrôleur ou le processeur de données ; et

vi) toute autre information que le contrôleur de données est tenu de fournir en vertu de la présente ou de toute autre loi.

2) Le contrôleur de données doit fournir des informations selon le paragraphe 1) de la manière suivante :

a) par écrit ;

b) dans un langage simple ;

c) à titre gratuit ; et

d) dans le mois qui suit la date de réception d'une telle demande.

3) Si une demande selon le paragraphe 1) est trop excessive ou déraisonnable, le contrôleur de données peut :

a) imposer un droit raisonnable sur la base des frais administratifs encourus ; ou

b) refuser de donner suite à la demande.

4) Si le contrôleur de données impose un droit en application de l'alinéa 3)a) ou refuse de donner suite à une demande en application de l'alinéa 3)b), à charge pour lui d'apporter la preuve de la nature excessive ou déraisonnable de la demande.

10 Restriction sur le traitement de données personnelles

1) Un contrôleur de données doit restreindre le traitement de données personnelles à la demande d'un sujet de données dans l'une quelconque des circonstances suivantes :

a) lorsque l'exactitude des données personnelle est contestée par le sujet de données, pour la période nécessaire pour permettre au contrôleur de vérifier l'exactitude des données personnelles ;

b) lorsque le traitement est contraire à la loi mais que le sujet des données s'oppose à l'effacement des données personnelles et, à la place, demande à ce que leur utilisation soit l'objet de restriction ;

c) lorsque le contrôleur n'a plus besoin des données personnelles aux fins du traitement ;

d) lorsque le sujet de données s'est opposé au traitement en vertu de l'article 12 en attendant que soit vérifiée la question de savoir si les motifs légitimes du contrôleur l'emportent sur ceux du sujet de données.

2) Si un sujet de données a restreint le traitement de données personnelles en application du paragraphe 1), les données personnelles ne peuvent être traitées que dans l'une des circonstances suivantes :

a) avec le consentement du sujet de données ;

b) pour l'introduction, la poursuite ou la défense d'une action en justice ;

c) pour la protection des droits d'une autre personne physique ou morale ; ou

d) pour des raisons d'intérêt public.

3) Le sujet de données qui a restreint le traitement de données personnelles en application du paragraphe 1) doit être informé par le contrôleur de données avant le traitement des données personnelles à des fins mentionnées à l'alinéa 2)b), c) ou d).

11 Rectification et effacement de données personnelles

1) Un contrôleur de données doit s'assurer que, sur demande d'un sujet de données, celui-ci peut obtenir la rectification de données personnelles inexactes ou incomplètes sans tarder et à titre gratuit.

2) Un contrôleur de données doit s'assurer que, sur demande d'un sujet de données, celui-ci obtient l'effacement de données personnelles sans tarder et à titre gratuit si :

a) les données personnelles ne sont plus nécessaires aux fins auxquelles elles ont été recueillies ou autrement traitées ;

b) le sujet de données rétracte le consentement sur lequel le traitement est basé ;

c) le sujet de données s'oppose au traitement en vertu de l'article 12 et le contrôleur ne peut pas démontrer qu'il existe un fondement légitime prépondérant pour le traitement ;

d) les données personnelles sont traitées contrairement à la loi ;

e) les données personnelles doivent être effacées pour remplir une obligation légale à laquelle le contrôleur de données est soumis.

3) Le contrôleur de données doit communiquer la demande d'un sujet de données en application du paragraphe 1) ou 2) à tous les destinataires auxquels les données personnelles concernées ont été communiquées.

4) Le paragraphe 3) ne s'applique pas dans le cas où le contrôleur de données peut démontrer qu'il est impossible de communiquer la demande d'un sujet de données ou nécessiterait des efforts disproportionnés.

12 Opposition au traitement de données personnelles

Un contrôleur de données doit s'assurer qu'à la demande d'un sujet de données, celui-ci peut s'opposer au traitement de ses données personnelles à tout moment et à titre gratuit, sauf si le contrôleur de données peut démontrer :

a) des motifs légitimes pour le traitement qui l'emportent sur les intérêts ou les droits et libertés fondamentaux du sujet de données ; ou

b) l'introduction, la poursuite ou la défense d'une action en justice.

13 Droit d'un sujet de données non soumis à un processus de prise de décision automatisé

1) Un contrôleur de données doit s'assurer qu'à la demande d'un sujet de données, celui-ci n'est pas soumis à une décision qui le touche significativement ou est basée uniquement sur un traitement automatisé de données personnelles, y compris profilage, sans que ses points de vue ne soient pris en considération.

2) Aux fins d'application du paragraphe 1), **profilage** désigne n'importe quelle forme de traitement automatisé de données personnelles pour évaluer certains aspects personnels en rapport avec une personne physique;

3) Le paragraphe 1) ne s'applique pas si une décision :

a) est autorisée par une loi à laquelle le contrôleur de données est soumis ;

b) est nécessaire pour conclure ou mener à bien un contrat entre le sujet de données et le contrôleur de données ; ou

c) est basée sur le consentement du sujet de données et que des garanties appropriées ont été mises en place.

4) Lorsque l'alinéa 3)b) ou c) s'applique, le contrôleur de données doit :

a) mettre en œuvre des mesures qui conviennent pour protéger les droits et libertés fondamentaux du sujet de données et ses intérêts légitimes ; et

b) donner au sujet des données la possibilité d'obtenir une intervention humaine de la part du contrôleur.

5) Lorsqu'une décision selon le paragraphe 1) est basée sur des catégories particulières de données personnelles ou des données personnelles d'enfants ou des données personnelles relatives à des personnes vulnérables, le traitement ne doit être effectué que si :

a) les conditions énoncées aux articles 6 et 7 pour le traitement sont remplies ;

b) le traitement est nécessaire pour des raisons d'intérêt public ; et

c) . le traitement est exigé par une autre loi

14 Représentation du sujet de données

Un contrôleur de données doit s’assurer qu’un sujet de données peut autoriser une personne, un organisme, une organisation ou une association à but non lucratif de déposer et poursuivre une plainte pour le compte du sujet de données auprès du Commissaire adjoint ou du tribunal.

TITRE 4 MOUVEMENTS DE DONNEES TRANSFRONTALIERS

15 Conditions de transfert hors du Vanuatu

1) Des données personnelles générées ou recueillies au Vanuatu ne doivent pas être utilisées ailleurs sans l'autorisation préalable du Ministre sur recommandation du Commissaire adjoint.

2) Nonobstant le paragraphe 1), des données personnelles générées ou recueillies au Vanuatu peuvent être transférées à un autre pays ou à une organisation internationale sans l'autorisation préalable du Ministre si le pays ou l'organisation internationale en question a été prescrit par le Ministre conformément au paragraphe 3).

3) Le Ministre peut, par arrêté, sur recommandation du Commissaire adjoint, dresser une liste des pays et des organisations internationales qui apportent un niveau approprié de protection de données personnelles.

16 Protections préalablement au transfert hors du Vanuatu

En sus de l'article 15, le Ministre peut, sur avis du Commissaier adjoint, prescrire des procédures de protection à appliquer s'agissant de transférer des données personnelles en dehors du Vanuatu si :

a) l'information demandée est réputée de nature urgente et sensible par le Commissaire adjoint ; et

b) le pays ou l'organisation internationale auquel ou à laquelle les données personnelles seront transférées a été prescrit conformément au paragraphe 15.3).

17 Transfert transfrontalier dans des situations spécifiques

Nonobstant l'article 15, le Ministre peut, sur recommandation du Commissaire adjoint, autoriser le transfert transfrontalier de données personnelles à d'autres pays ou à des organisations internationales qui ne garantissent pas un degré de protection approprié si :

a) le sujet de données a donné son consentement librement et de façon explicite et spécifique, après avoir été informé de tous les risques résultant du transfert en l'absence de protections adéquates ;

b) les intérêts spécifiques du sujet de données nécessitent le transfert dans un cas particulier ;

c) le transfert est nécessaire pour tout objet approuvé par la Commission.

TITRE 5 EXECUTION

18 Communication de documents ou d'informations

1) Si le Commissaire adjoint est convaincu qu'un contrôleur de données détient en sa possession un document ou une information qui l'aidera à constater s'il y a eu une violation de la présente loi, il peut, par écrit, exiger que ledit contrôleur de données lui fournisse le document ou l'information en question.

2) Le contrôleur de données visé au paragraphe 1) doit se conformer à la demande sous les 14 jours de sa réception.

3) Le Commissaire adjoint ne doit pas communiquer un document ou une information quelconque reçu en vertu du présent article à moins :

   a) d'y être autorisé par le contrôleur de données ;

   b) d'y être tenu par une ordonnance d'un tribunal ;

   c) d'être convaincu que le document ou l'information n'identifie pas de contrôleur de données ou de sujet de données en particulier ; ou

   d) que la communication ne soit exigée par la présente ou toute autre loi.

19 Requête pour mandat de perquisition

1) Si le Commissaire adjoint est raisonnablement convaincu qu'un délit a été commis aux termes de la présente loi, il peut demander au Commissaire de Police de l'aider pour former une requête pour un mandat de perquisition.

2) Une requête pour un mandat de perquisition doit être formée par écrit et sous serment par le Commissaire de Police, et doit exposer :

   a) le délit auquel se rapporte la requête ;

   b) une description du centre de données ou d'un serveur de données ;

   c) l'information à l'appui du soupçon raisonnable de la perpétration du délit ; et

   d) la durée pour laquelle le mandat de perquisition est nécessaire.

20 Octroi de mandat de perquisition

1) La Cour peut octroyer un mandat de perquisition si elle est satisfaite de la requête du Commissaire de Police.

2) Sans limiter la portée du paragraphe 1), avant d'accorder un mandat de perquisition, la Cour doit prendre en considération ce qui suit :

a) la gravité du délit auquel se rapporte la requête ;

b) la fiabilité de l'information à l'appui de la requête, y compris la nature de la source de l'information ;

c) si l'intérêt public pour la production de données du centre de données ou d'un serveur de données l'emporte sur le droit au secret d'une personne dont la vie personnelle pourrait être affectée par suite de la production des données ;

d) s'il y a un lien suffisant entre les preuves recherchées et le délit auquel se rapporte la requête ;

e) si le mandat de perquisition doit être assorti d'une condition quelconque ;

f) la durée du mandat de perquisition telle que proposée ; et

g) toutes autres affaires que la Cour estime pertinentes.

21 Contenu d'un mandat de perquisition

Un mandat de perquisition doit contenir les informations suivantes :

a) une description du centre de données et du serveur de données qui doivent être perquisitionnés ;

b) le délit auquel la requête se rapporte ;

c) les types de preuves pertinentes qui peuvent être recherchés ;

d) le pouvoir du Commissaire adjoint de sécuriser un centre de données ou un serveur de données ou de le rendre inaccessible ;

e) la date et l'heure d'expiration du mandat de perquisition ; et

f) toutes conditions imposées eu égard à l'exécution du mandat de perquisition.

22 Prorogation d'un mandat de perquisition

1) La Cour doit préciser la date et l'heure d'expiration du mandat de perquisition dans le mandat de perquisition.

2) A la demande du Commissaire de Police, la Cour peut proroger la date et l'heure d'expiration d'un mandat de perquisition si elle est satisfaite que l'objet pour lequel le mandat de perquisition a été accordé ne peut être rempli avant son expiration.

23 Effets d'un mandat de perquisition

1) Aux termes d'un mandat de perquisition accordé en vertu de l'article 20, le Commissaire de Police est autorisé à :

a) saisir un article qu'il est fondé à croire être :

i) une preuve pertinente en rapport avec un délit objet du mandat de perquisition ; ou

ii) une preuve pertinente pour un autre délit à la présente ou toute autre loi ;

b) avoir accès à un centre de données ou un serveur de données aux fins d'obtenir des informations et des registres ;

c) saisir ou sécuriser un serveur de données ;

d) exiger qu'une personne ayant une connaissance du centre de données ou du serveur de données l'aide à y accéder ;

e) déplacer le serveur de données de l'endroit perquisitionné à un autre endroit pour l'examiner dans le but de constater s'il contient des données qui pourraient être accessibles, collationnées ou saisies en vertu du mandat de perquisition ; et

f) se faire aider par le Commissaire adjoint ou une autre personne selon que raisonnablement nécessaire pour exécuter le mandat de perquisition.

2) Si le Commissaire de Police saisit le serveur de données en application du paragraphe 1), il peut :

a) en prendre possession ; et

b) le garder pour la durée qu'il considère nécessaire aux fins d'application de la présente loi.

3) Le Commissaire de Police doit rendre le serveur de données visé au paragraphe 2) au contrôleur de données :

a) s'il n'est plus nécessaire de le saisir ; ou

b) s'il ne va pas servir au titre de preuve.

TITRE 6 DELITS

24 Infraction à une disposition de la présente loi

Quiconque enfreint une disposition de la présente loi commet un délit passible sur condamnation d'une amende ne dépassant pas VT 10.000.000.

25 Obtention et divulgation illicites de données à caractère personnel

1) Une personne autre que le contrôleur de données ne doit pas, sciemment ou imprudemment, obtenir, retenir ou divulguer ou faire divulguer des données personnelles :

   a) sans l'autorisation du contrôleur de données ; et

   b) dans l'intention d'obtenir un gain financier ou de causer du mal au sujet de données.

2) Une personne qui enfreint le paragraphe 1) commet un délit passible sur condamnation d'une amende ne dépassant pas VT 10.000.000.

26 Modification de données personnelles pour empêcher la divulgation à un sujet de données

Un contrôleur de données ou un processeur de données, ou une personne employée par l'un ou par l'autre, qui modifie, dégrade, bloque, efface, détruit ou dissimule des informations personnelles dans l'intention d'empêcher la divulgation de toutes les informations personnelles ou d'une partie d'entre elles à un sujet de données commet un délit passible sur condamnation d'une amende ne dépassant pas VT 10.000.000.

27 Entrave aux pouvoirs d'entrée dans des locaux

Quiconque entrave délibérément une personne dans l'exécution d'un mandat de perquisition délivré en application de la présente loi commet un délit passible sur condamnation d'une amende ne dépassant pas VT 10.000.000.

28 Destruction ou falsification d'informations demandées par le Commissaire adjoint

Une personne qui détruit, dissimule ou falsifie, entièrement ou partiellement, des informations personnelles, un document, un équipement ou un matériel, dans l'intention d'empêcher la communication d'informations personnelles au Commissaire adjoint en application de l'article 18, commet un délit passible sur condamnation d'une amende ne dépassant pas VT 10.000.000.

29 Entrave ou obstruction dans l'exercice légal de pouvoirs

1) Une personne ne doit pas gêner ou entraver le Commissaire adjoint, un policier ou une personne aidant un policier dans l'exercice de ses pouvoirs aux termes de la présente loi.

2) Une personne qui enfreint le paragraphe 1) commet un délit passible sur condamnation d'une amende ne dépassant pas VT 1.000.000.

30 Défense de communiquer des informations, des registres et des données

1) Une personne qui obtient des informations, des extraits, des registres ou des données en vertu d'une demande ou d'un mandat de perquisition en application de la présente loi ne doit pas sciemment les communiquer, entièrement ou partiellement.

2) Une personne qui enfreint le paragraphe 1) commet un délit passible sur condamnation d'une amende ne dépassant pas VT 2.000.000.

TITRE 7 DISPOSITIONS DIVERSES

31 Règlements

1) Le Ministre peut, après avis du Commissaire adjoint, établir des règlements qui ne soient pas incompatibles avec la présente loi dans le but de mieux appliquer ou donner effet aux dispositions de la présente loi.

2) Sans limiter la portée générale du paragraphe 1), les règlements peuvent disposer de ce qui suit :

   a) comment des données personnelles doivent être traitées en toute transparence ;

   b) comment des contrôleurs de données conjoints doivent travailler ensemble et les obligations qui doivent incomber à chacun d'entre eux ou aux deux ;

   c) les obligations des processeurs de données ;

   d) la sécurité du traitement ;

   e) l'enregistrement des opérations de traitement ;

   f) les obligations relativement à des violations de données personnelles ; et

   g) la notification de violation de données personnelles à des sujets de données.

32 Entrée en vigueur

La présente loi entre en vigueur le jour de sa publication au Journal Officiel.

REPUBLIC OF VANUATU

HARMFUL DIGITAL COMMUNICATIONS ACT NO. 14 OF 2024

Arrangement of Sections

PART 1 PRELIMINARY MATTERS 3
1 Interpretation 3
2 Communication Principles 5

PART 2 PROCEEDINGS FOR HARMFUL DIGITAL COMMUNICATIONS IN THE MAGISTRATES COURT 7

Division 1 Proceedings for harmful digital communications in the Magistrates Court 7
3 Proceedings 7
4 Requirements for the proceedings 7
5 Magistrates Court may refer matter back to the Deputy Commissioner 8
6 Magistrates Court may require Deputy Commissioner to provide information 8

Division 2 Applications 8
7 Applications 8
8 Mode of hearing and evidence 9

Division 3 Technical Advisers 10
9 Technical advisers 10

Division 4 Orders 10
10 Interim Order 10
11 Orders that may be made by the Magistrates Court 10
12 Magistrates Court may vary or discharge order 12

PART 3 OFFENCES 14
13 Offence of non-compliance with order 14
14 Causing harm by posting digital communication 14
15 Posting intimate visual recording without consent 15
16 Civil orders may be made during proceedings for offence under section 15 15

PART 4 LIABILITY OF ONLINE CONTENT HOST 17
17 Process for obtaining protection against liability for specific content 17
18 Further provisions related to section 17 18

PART 5 MISCELLANEOUS PROVISIONS 20
19 Report to the Authority 20
20 Regulations 20
21 Commencement 20

REPUBLIC OF VANUATU

Assent: **05/12/2024**
Commencement: **02/01/2025**

HARMFUL DIGITAL COMMUNICATIONS ACT NO. 14 OF 2024

An Act to regulate the use of harmful digital communications and for related matters.

Be it enacted by the President and Parliament as follows-

PART 1 PRELIMINARY MATTERS

1 Interpretation

(1) In this Act, unless the contrary intention appears:

applicant means a person who makes an application under section 3;

application means an application to the Magistrates Court under section 7;

Authority means the Digital Safety Authority established under the Digital Safety Authority Act No. 15 of 2024;

Commission means the Digital Safety Commission established under the Digital Safety Authority Act No. 15 of 2024;

Communication Principles means the Communication Principles under section 2;

court means the Magistrates Court or the Supreme Court;

Deputy Commissioner means the Deputy Commissioner of Harmful Digital Communications appointed under the Digital Safety Authority Act No. 15 of 2024;

digital communication means:

(a) any email, phone call, social media messaging, posts or comments related to posts, short message service or text message, web chat, blog, podcast or video; or

(b) any writing, photograph, picture, recording or other matter that is communicated electronically; or

(c) any other form of electronic communication;

harm means serious emotional distress;

internet protocol address provider means a person that operates a business that, other than as an incidental feature of its main business activities:

(a) offers the transmission, routing, and providing of connections for digital online communications, between or among points specified by a user, of material of the user's choosing; and

(b) allocates Internet Protocol addresses to its account holders; and

(c) charges its account holders for its services; and

(d) is not primarily operated to cater for transient users;

intimate visual recording has the meaning given by subsections (2) and (3);

Minister means the Minister responsible for harmful digital communications;

online content host, in relation to a digital communication, means the person who has control over the part of the electronic retrieval system, such as a website or an online application, on which the communication is posted and accessible by the user;

post, in relation to a digital communication, means:

(a) to transfer, send, publish, disseminate, or otherwise communicate by means of a digital communication:

(i) any information, whether truthful or untruthful, about a victim; or

(ii) an intimate visual recording of an individual; and

(b) to include an attempt to do anything referred to in paragraph (a);

victim means:

(a) in relation to section 14, an individual who is the target of a posted digital communication; and

(b) in relation to section 15, an individual who is the subject of an intimate visual recording.

(2) An intimate visual recording is a visual recording (for example, a photograph, videotape, or digital image) that is made in any medium using any device with or without the knowledge or consent of an individual who is the subject of the recording, and that is of:

(a) the individual who is in a place which, in the circumstances, would reasonably be expected to provide privacy, and the individual is:

(i) naked or has his or her genitals, pubic area, buttocks, or female breasts exposed, partially exposed, or wearing only undergarments; or

(ii) engaged in an intimate sexual activity; or

(iii) engaged in showering, toileting, or other personal bodily activity that involves dressing or undressing; or

(b) the individual's naked or partly covered genitals, pubic area, buttocks, or female breasts which is made:

(i) from beneath or under an individual's clothing; or

(ii) through an individual's outer clothing in circumstances where it is unreasonable to do so.

(3) An intimate visual recording includes a recording that is made and transmitted in real time without retention or storage in:

(a) a physical form; or

(b) an electronic form,

from which the recording is capable of being reproduced with or without the aid of any device or thing.

2 Communication Principles

(1) A person who performs any functions or exercises any powers under this Act must:

(a) consider the Communication Principles: and

(b) act consistently with the rights and freedoms under the Constitution of the Republic of Vanuatu.

(2) A digital communication must not do all or any of the following:

(a) disclose sensitive personal facts about an individual;

(b) be abusive, threatening, intimidating, or menacing;

(c) be offensive to a reasonable person in the position of the affected individual;

(d) be indecent or obscene;

(e) be used to harass an individual;

(f) make a false or misleading allegation;

(g) publish a matter that is in breach of confidence;

(h) incite or encourage anyone to send a message to an individual for the purpose of causing harm to the individual;

(i) incite or encourage an individual to commit suicide;

(j) denigrate an individual by reason of his or her colour, race, ethnic, island or national origins, political affiliation, religion, gender, sexual orientation, or disability.

PART 2 PROCEEDINGS FOR HARMFUL DIGITAL COMMUNICATIONS IN THE MAGISTRATES COURT

Division 1 Proceedings for harmful digital communications in the Magistrates Court

3 Proceedings

(1) A person may apply to the Magistrates Court for an order under section 10 or 11.

(2) An application may be made by:

(a) an individual (the affected individual) who alleges that he or she has suffered or will suffer harm as a result of a digital communication; or

(b) a parent or guardian on behalf of the affected individual; or

(c) the principal of a school if the affected individual is a student of that school and consents to the principal bringing the proceedings; or

(d) a police officer if the digital communication constitutes a threat to the safety of an individual; or

(e) any other person prescribed by the Regulations.

4 Requirements for the proceedings

(1) The Magistrates Court must not grant an application unless it is satisfied that:

(a) there has been a breach of the Communication Principles; and

(b) the breach has caused or is likely to cause harm to the individual.

(2) The Magistrates Court may dismiss an application under subsection 3(1):

(a) if it considers for a person under paragraph 3(2)(a), (b), (c) or (e) that the application is frivolous or vexatious, or for any other reason does not meet the requirements under this section; and

(b) if it is satisfied for a person under paragraph 3(2)(d), after having regard to all the circumstances of the case, that the application must be dismissed.

(3) The Magistrates Court may make an order that any proceeding under this Act is to be heard, in whole or in part, in closed court if the Court considers that it is in the interests of justice.

5 Magistrates Court may refer matter back to the Deputy Commissioner

The Magistrates Court, in considering an application under section 3:

(a) must consider whether an attempt has been made to resolve the complaint, whether through mediation or otherwise; and

(b) may adjourn the proceedings and refer the matter back to the Deputy Commissioner unless satisfied that attempts at resolution, or further attempts at resolution, of the matter by the parties and the Deputy Commissioner are likely:

(i) not to contribute constructively to resolving the matter; or

(ii) not in the circumstances to be in the public interest; or

(iii) to undermine the proceedings before the Court.

6 Magistrates Court may require Deputy Commissioner to provide information

(1) The Magistrates Court may require the Deputy Commissioner to provide information for the purposes of satisfying the Court of any matters referred to in sections 4 and 5.

(2) The Deputy Commissioner must provide the information in the form prescribed by the rules of court.

Division 2 Applications

7 Applications

(1) An application to the Magistrates Court for an order under section 10 or 11 must be filed in the Court and be in the prescribed form.

(2) The Magistrates Court may give directions as to service and, if the Court considers it appropriate to do so in the circumstances, consider an application made on a without notice basis.

(3) A filing fee is not payable for an application.

8 Mode of hearing and evidence

(1) The Magistrates Court may, having regard to the circumstances of a particular case, direct that an application be determined:

(a) on the basis only of written material provided to it; or

(b) by way of a hearing involving oral submissions; or

(c) in such other way as the Court determines.

(2) The Magistrates Court may deal with an application in any manner that it considers will preserve the anonymity of a party so that the party's identity is not released to any other party during the proceedings.

(3) The Magistrates Court may receive any evidence or information that may in its opinion, assist it in dealing effectively with any proceedings under this Act, whether or not the evidence or information would be otherwise admissible in a court of law.

(4) An applicant may appeal against a decision of the Magistrates Court in accordance with section 30 of the Judicial Services and Courts Act [CAP 270].

Division 3 Technical Advisers

9 Technical advisers

(1) The Commission must maintain a panel of persons who may be approved as technical advisers, and only persons named on the panel may be approved as technical advisers.

(2) A technical adviser may be appointed to the panel for up to 5 years, and the appointment continues until:

(a) the person is reappointed; or

(b) a successor to the person is appointed; or

(c) the person is informed in writing by the Commission that he or she is not to be reappointed and that a successor to that person is not to be appointed; or

(d) the person resigns by notice in writing to the Commission; or

(e) the person is removed from the panel by the Commission for incapacity that affects the person's performance of duty, for neglect of duty, or for misconduct, proved to the satisfaction of the Commission; or

(f) the person dies.

(3) The Commission is to determine the remuneration and allowances of the technical advisers.

Division 4 Orders

10 Interim Order

(1) The Magistrates Court may grant any interim orders pending the determination of the application for orders under section 11.

(2) An interim order under this section may do anything that may be done by order under section 11 and expires when the application under that section is determined.

11 Orders that may be made by the Magistrates Court

(1) The Magistrates Court may, on an application, make all or any of the following orders against a defendant:

(a) an order to remove or disable material;

(b) an order that the defendant cease or refrain from the conduct concerned;

(c) an order that the defendant must not encourage any other person to engage in similar communications towards the affected individual;

(d) an order that a correction be published;

(e) an order that a right of reply be given to the affected individual;

(f) an order that an apology be published;

(g) any other order that the Court considers appropriate.

(2) The Magistrates Court may, on an application, make all or any of the following orders against an online content host:

(a) an order to remove or disable public access to material that has been posted or sent;

(b) an order that the identity of the author of an anonymous or pseudonymous communication be released to the Court;

(c) an order that a correction be published in any manner that the Court specifies in the order;

(d) an order that a right of reply be given to the affected individual in any manner that the Court specifies in the order.

(3) The Magistrates Court may, on an application, make an order against an internet protocol address provider that the identity of an anonymous communicator be released to the Court.

(4) The Magistrates Court may do all or any of the following:

(a) make a direction applying an order provided for in subsection (1) or (2) to other persons specified in the direction, if there is evidence that those other persons have been encouraged to engage in harmful digital communications towards the affected individual;

(b) make a declaration that a communication breaches a Communication Principle;

(c) make an order that the names of any specified parties be suppressed.

(5) In deciding whether or not to make an order under this section, the Magistrates Court must take into account:

(a) the content of the communication and the level of harm caused or likely to be caused by it; and

(b) the purpose of the communication, in particular whether the communication was intended to cause harm; and

(c) the occasion, context, and subject matter of the communication; and

(d) the extent to which the communication has spread beyond the original parties to the communication; and

(e) the age and vulnerability of the affected individual; and

(f) the truth or falsity of the statement; and

(g) whether the communication is in the public interest; and

(h) the conduct of the defendant, including any attempt by the defendant to minimise the harm caused; and

(i) the conduct of the affected individual or complainant; and

(j) the technical and operational practicalities, and the costs, of an order; and

(k) the appropriate individual or other person who should be subject to the order.

12 Magistrates Court may vary or discharge order

(1) Any applicant who obtains an order under section 10, 11 or 16 or any other party to that order may apply for an order in subsection (2).

(2) The Magistrates Court may, by order, do all or any of the following things to an order made under section 10, 11 or 16:

(a) vary the duration of the order;

(b) vary any conditions of the order;

(c) discharge the order.

PART 3 OFFENCES

13 Offence of non-compliance with order

If a person, without reasonable excuse, fails to comply with an order made under section 10, 11 or 16, the person commits an offence punishable on conviction:

(a) in the case of an individual – to a fine not exceeding VT500,000 or by imprisonment to a term not exceeding 6 months, or to both; or

(b) in the case of a body corporate – to a fine not exceeding VT1,000,000.

14 Causing harm by posting digital communication

(1) If:

(a) a person posts a digital communication with the intention that it cause harm to a victim; and

(b) posting the communication causes harm to the victim,

the person commits an offence punishable on conviction by the penalty set out in subsection (2).

(2) The penalty is:

(a) in the case of an individual – to a fine not exceeding VT500,000 or by imprisonment to a term not exceeding 2 years, or to both; or

(b) in the case of a body corporate – to a fine not exceeding VT1,000,000.

(3) In determining whether a post causes harm, the court may take into account any factors it considers relevant, including:

(a) the extremity of the language used;

(b) the age and characteristics of the victim;

(c) whether the digital communication was anonymous;

(d) whether the digital communication was repeated;

(e) the extent of circulation of the digital communication;

(f) whether the digital communication is true or false;

(g) the context in which the digital communication appeared.

(4) This section does not apply if the posted digital communication is an intimate visual recording to which the offence in section 15 applies.

15 Posting intimate visual recording without consent

(1) If a person, without reasonable excuse, posts a digital communication that is an intimate visual recording of a victim:

(a) knowing that the victim has not consented to the posting; or

(b) being reckless as to whether the victim has consented to the posting,

the person commits an offence punishable on conviction by the penalty set out in subsection (2).

(2) The penalty is:

(a) in the case of an individual – to a fine not exceeding VT500,000 or by imprisonment to a term not exceeding 2 years, or to both; or

(b) in the case of a body corporate – to a fine not exceeding VT1,000,000.

(3) An individual under the age of 16 years cannot consent to the posting of an intimate visual recording of which he or she is the subject.

16 Civil orders may be made during proceedings for offence under section 15

(1) On application made under this section and if the court considers it desirable to do so, the court conducting the proceedings for an offence under section 15 may make:

(a) during the proceedings, all or any of the interim orders set out in subsection (2) against the defendant for the duration of the proceedings; and

(b) if the defendant is proven to have committed the offence, all or any of the orders set out in subsection (3) against the defendant.

(2) Without limiting paragraph (1)(a), the court may make all or any of the following interim orders:

(a) an order to remove or disable material;

(b) an order that the defendant cease or refrain from the conduct concerned;

(c) an order that the defendant not encourage any other persons to engage in similar communications towards the affected individual.

(3) Without limiting paragraph (1)(b), the court may make all or any of the following interim orders:

(a) an order to remove or disable material;

(b) an order that the defendant cease or refrain from the conduct concerned;

(c) an order that the defendant not encourage any other persons to engage in similar communications towards the affected individual;

(d) an order that a correction be published;

(e) an order that a right of reply be given to the affected individual;

(f) an order that an apology be published.

PART 4 LIABILITY OF ONLINE CONTENT HOST

17 Process for obtaining protection against liability for specific content

(1) Civil or criminal proceedings may not be brought against an online content host if the online content host:

(a) receives a notice of complaint about a specific content; and

(b) complies with the requirements in subsection (2).

(2) The requirements that the online content host must do, as soon as practicable but no later than 48 hours after receiving a notice of complaint:

(a) provide the author of the specific content with a copy of the notice of complaint, altered to conceal personal information that identifies the complainant if the host has received confirmation that the complainant does not consent to the host providing that information to the author; and

(b) notify the author that the author may submit a counter-notice to the host within 48 hours after receiving that notification.

(3) If the host is unable to contact the author after taking reasonable steps to do so, the host must remove or disable the specific content as soon as practicable after taking those steps but not later than 48 hours after receiving a notice of complaint.

(4) If the author submits a valid counter-notice in which the author consents to the removal of the specific content, the host must remove or disable the specific content as soon as practicable after receiving that counter-notice.

(5) If the author submits a valid counter-notice in which the author refuses to consent to the removal of the specific content, the host must:

(a) leave the specific content in place; and

(b) as soon as practicable after receiving that counter-notice, notify the complainant of the author's decision; and

(c) if the author consents, provide the complainant with personal information that identifies the author.

(6) If the author does not submit a valid counter-notice, the host must remove or disable the specific content as soon as practicable but no later than 48 hours after notifying the author under subsection (2).

(7) A notice of complaint must:

(a) state the complainant's name and a telephone number, a physical address, and an email address for the complainant; and

(b) state the specific content, and explain why the complainant considers that the specific content is unlawful or breaches 1 or more Communication Principles and has caused harm; and

(c) provide sufficient details to enable the specific content to be readily located; and

(d) state whether the complainant consents to personal information that identifies the complainant being released to the author; and

(e) contain any other information that the complainant considers relevant.

(8) A counter-notice must state:

(a) the author's name and a telephone number, a physical address, and an email address for the author; and

(b) whether the author consents to personal information that identifies the author being released to the complainant; and

(c) whether the author consents to the removal of the specific content.

(9) An online content host must not disclose any personal information about the complainant or author except by order of a Magistrate made on an application under this subsection.

18 Further provisions related to section 17

(1) The Deputy Commissioner may lodge a notice of complaint under section 17 on behalf of a complainant and provide advice and assistance to the complainant in relation to the complaint.

(2) The protection conferred on an online content host by section 17 does not apply if:

(a) the host does not provide an easily accessible mechanism that enables a user to contact the host about specific content in the manner provided in that section; or

(b) the person who provides the specific content does so on behalf, or at the direction, of the online content host.

(3) Nothing in this section limits the right of an individual to injunctive relief in relation to the content of a digital communication posted by another person and hosted by the online content host.

PART 5 MISCELLANEOUS PROVISIONS

19 Report to the Authority

(1) The Deputy Commissioner must, within 3 months after the end of each year , provide a report to the Authority on:

(a) the general administration of this Act; and

(b) the activities of the Deputy Commissioner for that year.

(2) The annual report must also include:

(a) the number of complaints made to the Deputy Commissioner and the nature of those complaints; and

(b) the number of complaints resolved, deferred, or refused.

20 Regulations

The Minister may, on the recommendation of the Commission after receiving advice from the Deputy Commissioner, make Regulations prescribing all matters:

(a) required or permitted by this Act to be prescribed; or

(b) that are necessary or convenient to be prescribed for the carrying out or giving effect to the provisions of this Act.

21 Commencement

This Act commences on the day on which it is published in the Gazette.

RÉPUBLIQUE DE VANUATU

LOI N°14 DE 2024 RELATIVE AUX COMMUNICATIONS NUMÉRIQUES PRÉJUDICIABLES

Sommaire

TITRE 1 DISPOSITIONS PRELIMINAIRES

1 Définitions 3
2 Principes de communication 6

TITRE 2 POURSUITES POUR COMMUNICATION NUMERIQUE DELETERE AU TRIBUNAL DE PREMIERE INSTANCE

Sous-titre 1 Poursuites pour communication numérique préjudiciable au tribunal de première instance

3 Poursuites 7
4 Conditions requises pour des poursuites 7
5 Tribunal de première instance peut renvoyer une affaire devant le Commissaire adjoint 8
6 Tribunal peut exiger des informations de la part du Commissaire adjoint 8

Sous-titre 2 Requêtes

7 Requêtes 9
8 Mode d'audience et preuves 9

Sous-titre 3 Conseillers techniques

9 Conseillers techniques 9

Sous-titre 4 Ordonnances

10 Ordonnance provisoire 10
11 Ordonnances pouvant être rendues par le tribunal de première instance 10

12 Tribunal de première instance peut varier ou lever une ordonnance 13

TITRE 3 DELITS

13 Délit de non respect d'une ordonnance.....14
14 Causer du mal en publiant une communication numérique.....14
15 Publier un enregistrement visuel intime sans consentement 15
16 Tribunal peut rendre une ordonnance au civil lors de poursuites pour un délit visé à l'artile 15 15

TITRE 4 RESPONSABILITE DE L'HOTE DU CONTENU EN LIGNE

17 Procédure pour obtenir une protection contre la responsabilité pour un contenu particulier 17
18 Autres dispositions relatives à l'article 17 19

TITRE 5 DISPOSITIONS DIVERSES

19 Rapport à l'Autorité 20
20 Règlements.....20
21 Entrée en vigueur 20

RÉPUBLIQUE DE VANUATU

Promulguée : **05/12/2024**
Entrée en vigueur : **02/01/2025**

LOI N°14 DE 2024 RELATIVE AUX COMMUNICATIONS NUMÉRIQUES PRÉJUDICIABLES

Portant règlementation de l'utilisation de communications numériques préjudiciables et des questions connexes.

Le Président de la République et le Parlement promulguent le texte qui suit.

TITRE 1 DISPOSITIONS PRELIMINAIRES

1 Définitions

1) Dans la présente loi, sous réserve du contexte :

requérant désigne une personne qui introduit une requête en application de l'article 3 ;

requête désigne une requête formée au tribunal de première instance en application de l'article 7 ;

Autorité désigne l'Autorité de sécurité numérique instituée en vertu de la loi No. de 2024 relative à l'Autorité de sécurité numérique ;

Commission désigne la Commission de sécurité numérique instituée en vertu de la loi No. de 2024 relative à l'Autorité de sécurité numérique ;

principes de communication désigne les principes de communication visés à l'article 2 ;

tribunal désigne le tribunal de première instance ou la Cour Suprême ;

Commissaire adjoint désigne le Commissaire adjoint des communications numériques préjudiciables nommé en vertu de la loi No. de 2024 relative à l'Autorité de sécurité numérique ;

communication numérique désigne :

a) un courriel, un appel téléphonique, une messagerie sur réseau social, des publications ou des commentaires associés à des publications, un service

de message court (short message service ou sms en anglais) ou un message texté, une causerie sur site internet, un blog, un podcast ou une vidéo ;

b) un écrit, une photographie, une image, un enregistrement ou autre contenu qui est communiqué électroniquement ; ou

c) toute autre forme de communication électronique ;

mal désigne une détresse émotionnelle grave ;

fournisseur d'adresse de protocole internet désigne une personne qui exploite une affaire qui, sauf si elle est accessoire à ses activités commerciales principales :

a) offre la transmission, le routage et l'accès à des connexions pour des communications en ligne numériques de contenu au choix de l'usager entre ou parmi des points stipulés par ce dernier ;

b) assigne des adresses de protocole internet à ses titulaires de compte ;

c) fait payer ses titulaires de compte pour ses services ; et

d) n'est pas exploitée principalement pour s'occuper d'utilisateurs de passage;

enregistrement visuel intime a le sens qui lui est attribué par les paragraphes 2) et 3) ;

Ministre désigne le Ministre responsable des communications numériques préjudiciables ;

hôte du contenu en ligne, en rapport avec une communication numérique, désigne la personne qui détient le contrôle de la partie du système électronique de recherche documentaire, tel qu'un site internet ou une application en ligne, où la communication est affichée et accessible par l'utilisateur ;

publier, en rapport avec une communication numérique, désigne :

a) transférer, envoyer, publier, diffuser ou communiquer autrement au moyen d'une communication numérique :

i) n'importe quelle information, qu'elle soit vraie ou non, au sujet d'une victime ; ou

ii) un enregistrement visuel intime d'une personne physique ; et

b) inclure une tentative de faire ce qui est visé à l'alinéa a) ;

victime désigne :

a) en rapport avec l'article 14, une personne physique qui est la cible d'une communication numérique qui a été publiée ;

b) en rapport avec l'article 15, une personne physique qui est le sujet d'un enregistrement visuel intime.

2) Un enregistrement visuel intime est un enregistrement visuel (par exemple une photographie, une vidéo ou une image numérique) qui est effectué sur n'importe quel support au moyen d'un appareil quel qu'il soit, avec ou sans la connaissance ou le consentement d'une personne physique qui est le sujet de l'enregistrement, et qui montre :

a) la personne dans un lieu qui, dans les circonstances, pourrait raisonnablement être considéré comme assurant son intimité et la personne :

i) est nue ou ses organes génitaux, sa zone pubienne, ses fesses ou ses seins de femme sont exposés, partiellement exposés, ou revêtus seulement de sous-vêtements ;

ii) se livre à une activité sexuelle intime ; ou

iii) est en train de se doucher, faire sa toilette ou se livre à une autre activité d'hygiène personnelle qui implique le fait de s'habiller ou de se déshabiller ;

b) les organes génitaux de la personne, à nu ou revêtus de sous-vêtement, sa zone pubienne, ses fesses ou ses seins de femme pris :

i) de par en-dessous ou sous ses vêtements ; ou

ii) à travers ses vêtements extérieurs dans des circonstances où il n'est pas raisonnable de le faire.

3) Un enregistrement visuel intime inclut un enregistrement qui est effectué et transmis en temps réel sans être conservé ou mémorisé :

a) sous une forme matérialisée ; ou

b) sous une forme électronique,

à partir de laquelle il peut être reproduit avec ou sans l'aide d'un appareil quelconque ou autre dispositif.

2 Principes de communication

1) Une personne qui s'acquitte de fonctions ou exerce des pouvoirs aux termes de la présente loi doit :

a) tenir compte des principes de communication ; et

b) toujours agir en conformité avec les droits et libertés énoncés dans la Constitution de la République de Vanuatu.

2) Une communication numérique ne doit pas consister, en tout ou en partie, à:

a) divulguer des faits personnels sensibles au sujet d'une personne physique ;

b) être injurieuse, menaçante ou intimidante ;

c) être choquante du point de vue d'une personne raisonnable dans la situation de l'individu concerné ;

d) être indécente ou obscène ;

e) servir à harceler un individu ;

f) porter une allégation fausse ou trompeuse ;

g) publier un contenu qui constitue un abus de confiance ;

h) inciter ou encourager quiconque à envoyer un message à un individu dans le but de lui faire du mal ;

i) inciter ou encourager un individu à se suicider ;

j) dénigrer un individu au motif de sa couleur, sa race, son origine ethnique, insulaire ou nationale, son affiliation politique, sa religion, son genre, son orientation sexuelle ou son handicap.

TITRE 2 POURSUITES POUR COMMUNICATION NUMERIQUE PRÉJUDICIABLE AU TRIBUNAL DE PREMIÈRE INSTANCE

Sous-titre 1 Poursuites pour communication numérique préjudiciable au tribunal de Première instance

3 Poursuites

1) Une personne peut saisir le tribunal de première instance pour une ordonnance en application de l'article 10 ou 11.

2) Une requête peut être formée par :

a) un individu (l'individu concerné) qui allègue qu'il a subi ou va subir du mal du fait d'une communication numérique ;

b) un parent ou tuteur pour le compte de l'individu concerné ;

c) le directeur d'une école si l'individu concerné y est élève et consent à ce que le directeur introduise des poursuites ;

d) un policier si la communication numérique constitue une menace pour la sécurité d'un individu ; ou

e) toute autre personne prescrite par les règlements.

4 Conditions requises pour des poursuites

1) Le tribunal de première instance ne doit pas rendre une ordonnance en application de l'article 10 ou 11 sans être convaincu :

a) qu'il y a eu atteinte aux principes de communication ; et

b) que l'atteinte a causé ou est susceptible de causer du mal à l'individu.

2) Le tribunal de première instance peut débouter une requête formée en vertu du paragraphe 3.1) s'il :

a) estime, pour une personne visée aux alinéas 3 2) a), b), c) ou e), que la requête est dérisoire ou vexatoire ou que, pour tout autre motif, elle ne remplit pas les conditions requises prévues au présent article ; et

b) est convaincu, pour une personne visée à l'alinéa 3 2) d), après avoir considéré toutes les circonstances de l'affaire, que la requête doit être déboutée.

3) Le tribunal de première instance peut rendre une ordonnance que des poursuites en application de la présente loi doivent être entendues, en totalité ou en partie, à huis clos s'il estime que tel est dans l'intérêt de la justice.

5 Tribunal de première instance peut renvoyer une affaire devant le Commissaire adjoint

En statuant sur une requête en application de l'article 3, le tribunal de première instance :

a) doit considérer la question de savoir si une tentative a été effectuée pour résoudre la plainte, que ce soit par médiation ou autrement ; et

b) peut remettre les poursuites et renvoyer l'affaire au Commissaire adjoint sauf s'il est convaincu que des tentatives de résolution ou de nouvelles tentatives de résolution de l'affaire par les parties et le Commissaire adjoint sont susceptibles de :

i) ne pas contribuer constructivement à la résolution de l'affaire ;

ii) ne pas être dans l'intérêt public dans les circonstances ; ou

iii) compromettre les poursuites par devant le tribunal.

6 Tribunal peut exiger des informations de la part du Commissaire adjoint

1) Le tribunal de première instance peut exiger que le Commissaire adjoint fournisse des informations dans le but de convaincre le tribunal de l'une quelconque des questions visées aux articles 4 et 5.

2) Le Commissaire doit fournir les informations sous la forme prescrite par les règles du tribunal.

Sous-titre 2 Requêtes

7 Requêtes

1) Une requête au tribunal de première instance pour une ordonnance en application de l'article 10 ou 11 doit être déposée au tribunal sous la forme prescrite.

2) Le tribunal peut donner des directives quant à la signification et, s'il estime approprié dans les circonstances, il peut prendre en considération une requête formée sur une base sans préavis.

3) Des frais de dépôt ne sont pas payables pour une requête.

8 Mode d'audience et preuves

1) Le tribunal de première instance peut, compte tenu des circonstances d'un cas particulier, ordonner qu'une requête soit tranchée :

   a) sur la seule base des preuves écrites qui lui sont fournies ;

   b) par le biais d'une audience faisant intervenir une argumentation orale; ou

   c) par tout autre moyen qu'il arrête.

2) Le tribunal de première instance peut traiter d'une requête de la manière qu'il considère préserver l'anonymat d'une partie de façon à ce que son identité ne soit pas révélée à une autre partie, quelle qu'elle soit, durant les poursuites.

3) Le tribunal peut recevoir toute preuve ou information qui pourrait, à son avis, l'aider à traiter efficacement de n'importe quelles poursuites en application de la présente loi, indépendamment de savoir si les preuves ou informations seraient par ailleurs recevables devant une cour de justice.

4) Un requérant peut interjeter appel d'une décision du tribunal de première instance conformément à l'article 30 de la loi sur le service judiciaire et les tribunaux [CAP 270].

Sous-titre 3 Conseillers techniques

9 Conseillers techniques

1) La Commission doit tenir une liste d'un jury de personnes qui peuvent être approuvées en tant que conseillers techniques et seules les personnes dont

le nom figure sur la liste peuvent être approuvées comme conseillers techniques.

2) Un conseiller technique peut être nommé au jury pendant une période allant jusqu'à 5 ans et la nomination est maintenue jusqu'à ce que :

a) la personne soit renommée ;

b) un successeur à la personne soit nommé ;

c) la personne soit informée par écrit par la Commission qu'elle n'est pas renommée et qu'un successeur à cette personne ne sera pas nommé ;

d) la personne démissionne par préavis écrit à la Commission ;

e) la personne est rayée de la liste du jury par la Commission pour une incapacité qui l'affecte dans l'accomplissement de son devoir, pour manquement à son devoir ou pour faute grave, prouvée de façon convaincante pour la Commission ; ou

f) la personne décède.

3) La Commission fixe la rémunération et les indemnités des conseillers techniques.

Sous-titre 4 Ordonnances

10 Ordonnance provisoire

1) Le tribunal de première instance peut rendre n'importe quelles ordonnances provisoires en attendant de statuer sur la requête pour des ordonnances en application de l'article 11.

2) Une ordonnance provisoire en application du présent article peut porter sur tout ce qui peut être ordonné en application de l'article 11 et cesse d'être en vigueur dès lors que la requête a été tranchée conformément à cet article.

11 Ordonnances pouvant être rendues par le tribunal de première instance

1) Saisi d'une requête, le tribunal de première instance peut rendre l'une quelconque des ordonnances suivantes ou toutes à l'encontre d'un défendeur :

a) une ordonnance pour supprimer ou désactiver un contenu ;

b) une ordonnance que le défendeur cesse ou s'abstienne de se livrer au comportement en question ;

c) une ordonnance que le défendeur ne doit pas encourager d'autres personnes à se livrer à des communications semblables à l'attention de la personne physique concernée ;

d) une ordonnance qu'un rectificatif doit être publié ;

e) une ordonnance qu'un droit de réponse doit être accordé à la personne concernée ;

f) une ordonnance que des excuses doivent être publiées ;

g) toute autre ordonnance qu'il estime appropriée.

2) Saisi d'une requête, le tribunal de première instance peut rendre l'une quelconque des ordonnances suivantes ou toutes à l'encontre de l'hôte d'un contenu en ligne :

a) une ordonnance de supprimer ou désactiver l'accès par le public à un contenu qui a été publié ou envoyé ;

b) une ordonnance que l'identité de l'auteur d'une communication anonyme ou sous un pseudonyme doit lui être révélée ;

c) une ordonnance qu'un rectificatif doit être publié d'une manière que le tribunal stipule dans l'ordonnance ;

d) une ordonnance qu'un droit de réponse doit être accordé à l'individu concerné d'une manière que le tribunal stipule dans l'ordonnance.

3) Saisi d'une requête, le tribunal de première instance peut rendre une ordonnance à l'encontre d'un fournisseur d'adresse de protocole internet comme quoi l'identité d'un communicateur anonyme doit lui être révélée.

4) Le tribunal de première instance peut faire l'une quelconque des choses suivantes ou toutes :

a) donner une instruction portant application d'une ordonnance visée au paragraphe 1) ou 2) à d'autres personnes stipulées dans

l'instruction s'il existe des preuves que ces autres personnes ont été incitées à se livrer à des communications numériques préjudiciables envers l'individu concerné ;

b) faire une déclaration comme quoi une communication porte atteinte à un principe de communication ;

c) rendre une ordonnance que le nom de n'importe quelles parties spécifiées doit être supprimé.

5) En décidant de rendre ou non une ordonnance en application du présent article, le tribunal de première instance doit prendre en considération :

a) le contenu de la communication et le degré de mal qu'il a causé ou qu'il est susceptible de causer ;

b) le but de la communication, en particulier à savoir si la communication était destinée à causer du mal ;

c) l'occasion, le contexte et le sujet de la communication ;

d) à quel point la communication s'est répandue au-delà des parties à la communication à l'origine ;

e) l'âge et la vulnérabilité de l'individu concerné ;

f) la véracité ou la fausseté de la déclaration ;

g) la question de savoir si la communication est dans l'intérêt public ;

h) la conduite du défendeur, y compris toute tentative de sa part de minimiser le mal causé ;

i) la conduite de l'individu concerné ou du plaignant ;

j) les aspects pratiques techniques et opérationnels et les coûts d'une ordonnance ; et

k) l'individu ou autre personne qu'il conviendrait de soumettre à l'ordonnance.

12 Tribunal de première instance peut varier ou lever une ordonnance

1) Tout requérant ayant obtenu une ordonnance en application de l'article 10, 11 ou 16 ou n'importe quelle autre partie à une telle ordonnance peut former une requête en ordonnance selon le paragraphe 2).

2) Le tribunal de première instance peut, par ordonnance, faire tout ou partie de ce qui suit en rapport avec une ordonnance rendue en application de l'article 10, 11 ou 16 :

a) en varier la durée ;

b) en varier l'une quelconque des conditions ;

c) la lever.

TITRE 3 DELITS

13 Délit de non respect d'une ordonnance

Une personne qui, sans excuse acceptable, manque de respecter une ordonnance rendue en application de l'article 10, 11 ou 16, commet un délit passible sur condamnation :

a) dans le cas d'une personne physique – d'une amende ne dépassant pas VT 500 000 ou d'une peine d'emprisonnement pour 6 mois au plus ou des deux peines à la fois ; ou

b) dans le cas d'une personne morale – d'une amende ne dépassant pas VT 1 000 000 .

14 Causer du mal en publiant une communication numérique

1) Si :

   a) une personne publie une communication numérique dans l'intention de causer du mal à une victime ; et

   b) le fait de publier la communication cause du mal à la victime,

   la personne commet un délit passible sur condamnation de la peine stipulée au paragraphe 2).

2) La peine est :

   a) dans le cas d'une personne physique – une amende ne dépassant pas VT 500 000 ou une peine d'emprisonnement pour 6 mois au plus ou les deux peines à la fois ; ou

   b) dans le cas d'une personne morale – une amende ne dépassant pas VT 1 000 000.

3) En décidant de la question de savoir si une publication cause du mal, le tribunal peut prendre en compte tous facteurs quels qu'ils soient qu'il considère pertinents, y compris :

   a) la nature extrême du langage employé ;

   b) l'âge et les caractéristiques de la victime ;

   c) si la communication numérique était anonyme ;

d) si la communication numérique s'est répétée ;

e) l'étendue de la circulation de la communication numérique ;

f) si la communication numérique est vraie ou fausse ;

g) le contexte dans lequel la communication numérique est apparue.

4) Le présent article ne s'applique pas si la communication numérique publiée est un enregistrement visuel intime auquel le délit visé à l'article 15 est applicable.

15 Publier un enregistrement visuel intime sans consentement

1) Une personne qui, sans excuse acceptable, publie une communication numérique qui est un enregistrement visuel intime d'une victime :

a) sachant que la victime n'y a pas consenti ; ou

b) sans se soucier de savoir si la victime y a consenti,

commet un délit passible sur condamnation de la peine stipulée au paragraphe 2).

2) La peine est :

a) dans le cas d'une personne physique – une amende ne dépassant pas VT 500 000 ou une peine d'emprisonnement pour 2 ans au plus ou les deux peines à la fois ; ou

b) dans le cas d'une personne morale – une amende ne dépassant pas VT 1 000 000.

3) Un individu de moins de 16 ans ne peut pas consentir à ce qu'un enregistrement visuel intime dont il est le sujet soit publié.

16 Tribunal peut rendre une ordonnance au civil lors de poursuites pour un délit visé à l'artile 15

1) Sur requête formée conformément au présent article et s'il estime souhaitable, le tribunal chargé du procès pour un délit selon l'article 15 peut rendre :

a) au cours du procès, l'une quelconque des ordonnances provisoires énoncées au paragraphe 2) ou toutes à l'encontre du défendeur pour toute la durée du procès ; et

b) l’une quelconque des ordonnances énoncées au paragraphe 3) ou toutes à l’encontre du défendeur s’il est prouvé qu’il a commis le délit.

2) Sans limiter la portée de l’alinéa 1)a), le tribunal peut rendre l’une quelconque des ordonnances provisoires suivantes ou toutes :

a) une ordonnance pour supprimer ou désactiver un contenu ;

b) une ordonnance que le défendeur cesse ou s’abstienne de se livrer au comportement en question ;

c) une ordonnance que le défendeur ne doit pas encourager d’autres personnes à se livrer à des communications semblables à l’attention de la personne concernée.

3) Sans limiter la portée de l’alinéa 1)b), le tribunal peut rendre l’une quelconque des ordonnances suivantes ou toutes :

a) une ordonnance pour supprimer ou désactiver un contenu ;

b) une ordonnance que le défendeur cesse ou s’abstienne de se livrer au comportement en question ;

c) une ordonnance que le défendeur ne doit pas encourager d’autres personnes à se livrer à des communications semblables à l’attention de la personne concernée ;

d) une ordonnance qu’un rectificatif soit publié ;

e) une ordonnance qu’un droit de réponse soit accordé à la personne concernée ;

f) une ordonnance que des excuses soient publiées.

TITRE 4 RESPONSABILITE DE L'HOTE DU CONTENU EN LIGNE

17 Procédure pour obtenir une protection contre la responsabilité pour un contenu particulier

1) Des poursuites au civil ou au pénal ne sauraient être introduites contre un hôte de contenu en ligne si celui-ci :

   a) reçoit un avis de plainte concernant un contenu particulier ; et

   b) se conforme aux conditions requises du paragraphe 2).

2) Les conditions requises auxquelles l'hôte du contenu en ligne doit se plier, dans les plus brefs délais, mais au plus tard dans les 48 heures de la réception d'un avis de plainte, sont les suivantes :

   a) fournir à l'auteur du contenu particulier une copie de l'avis de plainte, modifiée pour dissimuler les renseignements personnels qui identifient le plaignant si l'hôte a reçu confirmation de ce que le plaignant ne consent pas à ce qu'il fournisse ces renseignements à l'auteur ; et

   b) notifier l'auteur que celui-ci peut lui soumettre une contre-notification dans les 48 heures de la réception de l'avis en question.

3) Si l'hôte ne parvient pas à contacter l'auteur après avoir pris des dispositions raisonnables pour le faire, il doit supprimer ou désactiver le contenu particulier dès que possible après avoir pris de telles dispositions, mais au plus tard dans les 48 heures de la réception d'un avis de plainte.

4) Si l'auteur soumet une contre-notification en règle dans laquelle il consent à la suppression du contenu particulier, l'hôte doit supprimer ou désactiver le contenu particulier aussitôt que possible après avoir reçu ladite contre-notification.

5) Si l'auteur soumet une contre-notification en règle dans laquelle il refuse de consentir à la suppression du contenu particulier, l'hôte doit :

   a) laisser le contenu particulier en place ;

   b) notifier le plaignant de la décision de l'auteur aussitôt que possible après avoir reçu la contre-notification ; et

c) si l'auteur y consent, fournir au plaignant des renseignements personnels identifiant l'auteur.

6) Si l'auteur ne soumet pas une contre-notification en règle, l'hôte doit supprimer ou désactiver le contenu particulier aussitôt que possible, mais au plus dans les 48 heures après avoir notifié l'auteur conformément au paragraphe 2).

7) Un avis de plainte doit :

a) indiquer le nom du plaignant, un numéro de téléphone, une adresse physique et une adresse courriel pour le plaignant ;

b) indiquer le contenu particulier et expliquer pourquoi le plaignant estime qu'il est illégal ou porte atteinte à un ou plusieurs des principes de communication et a causé du mal ;

c) fournir suffisamment de détails pour permettre de localiser aisément le contenu particulier ;

d) indiquer si le plaignant consent à ce que des renseignements personnels l'identifiant soient révélés à l'auteur ; et

e) contenir tous autres renseignements que le plaignant considère pertinents.

8) Une contre-notification doit indiquer :

a) le nom de l'auteur, un numéro de téléphone, une adresse physique et une adresse courriel pour l'auteur ;

b) si l'auteur consent à ce que des renseignements personnels l'identifiant soient révélés au plaignant ; et

c) si l'auteur consent à ce que le contenu particulier soit supprimé.

9) Un hôte de contenu en ligne ne doit pas communiquer d'informations personnelles au sujet du plaignant ou de l'auteur sauf sur ordonnance d'un magistrat ou d'un juge rendue sur requête en application du présent paragraphe.

18 Autres dispositions relatives à l'article 17

1) Le Commissaire adjoint peut déposer un avis de plainte conformément à l'article 17 pour le compte d'un plaignant et lui apporter conseil et concours concernant la plainte.

2) La protection accordée à un hôte de contenu en ligne en vertu de l'article 17 ne s'applique pas si :

   a) l'hôte n'aménage pas un mécanisme aisément accessible pour permettre à un utilisateur de le contacter au sujet d'un contenu particulier de la manière prévue dans ledit article ; ou

   b) la personne qui fournit le contenu particulier le fait pour le compte ou sur instruction de l'hôte.

3) Aucune disposition du présent article ne limite le droit d'une personne physique à un remède par injonction relativement au contenu d'une communication numérique publiée par une autre personne et hébergée par l'hôte de contenu en ligne.

TITRE 5 DISPOSITIONS DIVERSES

19 Rapport à l'Autorité

1) Le Commissaire adjoint doit fournir à l'Autorité dans un délai de 3 mois après la fin de chaque année un rapport portant sur :

a) l'administration générale de la présente loi ; et

b) les activités du Commissaire adjoint durant l'année en question.

2) Le rapport annuel doit aussi inclure :

a) le nombre de plaintes portées auprès du Commissaire adjoint et la nature de telles plaintes ; et

b) le nombre de plaintes résolues, reportées ou rejetées.

20 Règlements

Le Ministre peut, sur recommandation de la Commission après avis du Commissaire adjoint, établir des règlements prescrivant tout ce qu'il est :

a) requis ou permis par la présente loi d'être prescrit ; ou

b) nécessaire ou opportun d'être prescrit pour appliquer ou donner effet aux dispositions de la présente loi.

21 Entrée en vigueur

La présente loi entre en vigueur le jour de sa publication au Journal Officiel.

REPUBLIC OF VANUATU

DIGITAL SAFETY AUTHORITY ACT NO. 15 OF 2024

Arrangement of Sections

PART 1 INTERPRETATION

1 Interpretation....3

PART 2 DIGITAL SAFETY AUTHORITY AND COMMISSIONER

Division 1 Establishment of the Digital Safety Authority

2 Establishment of Digital Safety Authority....5
3 Functions of the Authority....5
4 Powers of the Authority....5

Division 2 Commissioner of the Authority

5 Appointment of the Commissioner....6
6 Functions of the Commissioner....6
7 Powers of the Commissioner....7
8 Delegation of functions and powers....7
9 Resignation of the Commissioner....7
10 Disqualification of appointment as the Commissioner....7
11 Termination of the Commissioner....8

Division 3 Other Staff

12 Other Staff of the Authority....8

PART 3 DIGITAL SAFETY COMMISSION

13 Establishment of the Digital Safety Commission....9
14 Composition of the Commission....9
15 Function of the Commission....9
16 Powers of the Commission....9
17 Delegation of functions and powers....10
18 Chairperson and Deputy Chairperson of the Commission....10
19 Meetings of the Commission....10

20 Sitting allowances of the members of the Commission....11
21 Removal of a member of the Commission....11

PART 4 DEPUTY COMMISSIONER OF HARMFUL DIGITAL COMMUNICATIONS AND DEPUTY COMMISSIONER OF DATA PROTECTION AND PRIVACY

22 Appointment of Deputy Commissioners....12
23 Term of office....13
24 Functions of the Deputy Commissioners....13
25 Powers of a Deputy Commissioner....13
26 Resignation of a Deputy Commissioner....13
27 Removal of a Deputy Commissioner....13
28 Contractors to assist the Deputy Commissioners....14

PART 5 COMPLAINTS

29 Submission of complaints....15

PART 6 MISCELLANEOUS PROVISIONS

30 Funds of the Authority....16
31 Accounts of the Authority....16
32 Annual reports....16
33 Immunity....16
34 Regulation....16
35 Commencement....17

REPUBLIC OF VANUATU

Assent: **05/12/2024**
Commencement: **02/01/2025**

DIGITAL SAFETY AUTHORITY ACT NO. 15 OF 2024

An Act to provide for the establishment, operation and management of the Digital Safety Authority and related matters.

Be it enacted by the President and Parliament as follows-

PART 1 INTERPRETATION

1 Interpretation

In this Act, unless a contrary intention appears:

Authority means the Digital Safety Authority established under section 2;

Commission means the Digital Safety Commission established under section 13;

Commissioner means the Commissioner appointed under subsection 5(1);

Deputy Commissioner means the Deputy Commissioner of Harmful Digital Communications or the Deputy Commissioner of Data Protection and Privacy appointed under section 22;

digital means electronic technology that generates, stores, and processes data in terms of 2 states- positive and non-positive;

digital communication means:

(a) any email, phone call, social media messaging, sms or text message, web chat, blog, podcast or video; or

(b) any writing, photograph, picture, recording or other matter that is communicated electronically; or

(c) any other form of electronic communication;

digital content means information in the form of a digital communication;

digital safety means protecting electronic devices connecting to the internet from potential threats and intruders, so that the digital platform is safe to use;

government agency means:

(a) a Ministry; or

(b) an office or body established under the Constitution; or

(c) an office or body established under an Act of Parliament; or

(d) a prescribed agency;

Minister means the Minister responsible for Information and Communications Technology.

PART 2 DIGITAL SAFETY AUTHORITY AND COMMISSIONER

Division 1 Establishment of the Digital Safety Authority

2 Establishment of Digital Safety Authority

(1) The Digital Safety Authority is established.

(2) The Authority is:

(a) a body corporate with perpetual succession; and

(b) to have a common seal; and

(c) capable of suing and being sued.

3 Functions of the Authority

The Authority has the following functions:

(a) to promote digital safety, digital communication and digital content in Vanuatu; and

(b) to coordinate activities on digital safety, digital communication and digital content with a government agency; and

(c) to assist to protect the public against any digital safety issues and harm; and

(d) to represent Vanuatu internationally in matters relating to data protection and privacy and harmful digital communication; and

(e) such other functions that may be conferred on the Authority by this Act or any other Act.

4 Powers of the Authority

(1) The Authority has the power to do all things necessary or convenient to be done for or in connection with the performance of its functions under this Act.

(2) Without limiting subsection (1), the Authority has the power to do all or any of the following:

(a) to acquire, purchase, hold, manage and dispose of real or personal property;

(b) to develop any land or other property and to build and maintain buildings or other structures;

(c) to enter into agreements with any local authority, corporation, society, firm or person for the management and maintenance of any land, buildings or facilities.

Division 2 Commissioner of the Authority

5 Appointment of the Commissioner

(1) The Commission is to appoint the Commissioner.

(2) A person may be eligible for appointment as Commissioner if he or she meets the following criteria:

(a) is a Vanuatu citizen; and

(b) has a Master's Degree in Digital Safety or Cyber Security from a recognised university; and

(c) has 5 to 10 years of experience in dealing with Information and Communications Technology; and

(d) has at least 5 years of experience in managing an office.

(3) The Commission is to determine the terms and conditions of the employment of the Commissioner.

(4) The appointment of the Commissioner must follow a fair and transparent selection process and must be based on merit.

(5) The Commissioner is to hold office for a period of 5 years and is eligible for re-appointment for 1 term only.

6 Functions of the Commissioner

The Commissioner has the following functions:

(a) to advise the Commission and the Minister on matters relating to the administration of this Act; and

(b) to advise the Minister, after receiving advice from the Commission, on digital safety matters; and

(c) to manage and oversee the operations of the Authority; and

(d) to encourage and support a government agency to follow digital safety best practices and standards; and

(e) to, on the advice of the Commission, produce, publish, issue, circulate and distribute reports, papers, periodicals or any other information; and

(f) to supervise the Deputy Commissioners; and

(g) such other functions that may be conferred on the Commissioner by this Act or any other Act.

7 Powers of the Commissioner

The Commissioner has the power to do all things necessary or convenient to be done for or in connection with the performance of his or her functions under this Act.

8 Delegation of functions and powers

(1) Subject to this section, the Commissioner may delegate its functions and powers to a staff of the Authority.

(2) The Commissioner cannot delegate the power of delegation.

(3) A delegation made under subsection (1) is subject to instructions, guidelines or conditions imposed by the Commissioner.

(4) A delegation under this section does not prevent the exercise of any powers by the Commissioner.

(5) A delegation under this section may be revoked by the Commissioner at any time.

9 Resignation of the Commissioner

The Commissioner may resign by giving 3 months written notice to the Commission.

10 Disqualification of appointment as the Commissioner

A person is disqualified from his or her appointment as the Commissioner if he or she:

(a) is a member of Parliament, a Provincial Government Council or a Municipal Council; or

(b) has been convicted of an offence and sentenced to a term of imprisonment of 12 months or more, whether or not it is a suspended sentence; or

(c) is a director of company.

11 Termination of the Commissioner

The Commission is to terminate the Commissioner if he or she:

(a) becomes a member of Parliament, a Provincial Government Council or a Municipal Council; or

(b) is incapacitated and is unable to perform his or her functions; or

(c) is declared bankrupt; or

(d) is convicted of an offence and sentenced to a term of imprisonment of 12 months or more, whether or not it is a suspended sentence; or

(e) commits a serious misconduct; or

(f) breaches the terms and conditions of his or her employment; or

(g) misappropriates the funds of the Authority; or

(h) neglects to carry out his or her functions under this Act or any other Act.

Division 3 Other Staff

12 Other Staff of the Authority

(l) The Commissioner may, with the prior approval of the Commission, employ other staff of the Authority as he or she considers necessary for the proper and efficient performance of the functions of the Authority.

(2) The Commissioner is to determine the terms and conditions of the employment of the other staff of the Authority.

(3) The appointment of other staff must follow a fair and transparent selection process and must be based on merit.

PART 3 DIGITAL SAFETY COMMISSION

13 Establishment of the Digital Safety Commission

The Digital Safety Commission is established.

14 Composition of the Commission

(1) The Commission consists of the following persons:

(a) the Director General of the Office of the Prime Minister; and

(b) a person representing the National University of Vanuatu nominated by the Chancellor; and

(c) the Director of the Vanuatu Internet Governance Forum.

(2) Subject to subsection (3), the Minister is to appoint the member under paragraph (1)(b).

(3) The person nominated under paragraph (1)(b) must:

(a) have a tertiary qualification in cyber security and digital safety; and

(b) have no criminal convictions or records; and

(c) be a citizen of Vanuatu.

(4) The member appointed under paragraph (1)(b) is to be appointed for a term of 3 years and is to be reappointed for 1 term only.

15 Function of the Commission

The Commission has the function to determine the following standards:

(a) the standards for digital safety; and

(b) the standards for digital communication; and

(c) the standards for digital content.

16 Powers of the Commission

The Commission has the power to do all things necessary or convenient to be done for or in connection with the performance of its functions under this Act.

17 Delegation of functions and powers

(1) Subject to this section, the Commission may delegate its functions and powers to the Commissioner or to a member of the Commission.

(2) The Commission cannot delegate the power of delegation.

(3) A delegation made under subsection (1) is subject to instructions, guidelines or conditions imposed by the Commission.

(4) A delegation under this section does not prevent the exercise of any powers by the Commission.

(5) A delegation under this section may be revoked by the Commission at any time.

18 Chairperson and Deputy Chairperson of the Commission

(1) The Director General is the Chairperson of the Commission.

(2) The members of the Commission are to elect from amongst themselves a Deputy Chairperson.

(3) The Deputy Chairperson is to hold office for a period of 1 year and may be re-elected.

19 Meetings of the Commission

(1) The Commission is to meet at least once every quarter within a year and may hold such other meetings as are necessary for the proper performance of its functions under this Act.

(2) The Chairperson is to preside at all meetings of a Commission and if the Chairperson is absent, the Deputy Chairperson is to preside at these meetings.

(3) The quorum for a meeting is 2 members of the Commission present at the meeting.

(4) A member present at the meeting has 1 vote and questions arising at a meeting are to be decided by a majority of votes.

(5) If the voting at the meeting is equal, the Chairperson or the Deputy Chairperson (if he or she is presiding over the meeting) has a casting vote.

(6) The Commissioner is the Secretary of the Commission.

(7) The Commissioner after consultation with the Chairperson, is to notify the other members of the Commission of the venue, time and date of the meeting.

(8) Subject to this Act, the Commission may determine and regulate its own procedures.

20 Sitting allowances of the members of the Commission

The Minister may, by Order, prescribe the sitting allowances for the members of the Commission.

21 Removal of a member of the Commission

The member appointed under paragraph 13(1)(b) is to be removed as a member if he or she:

(a) fails to attend 3 consecutive meetings of the Commission without the permission of the Commission; or

(b) is suspended from his or her profession; or

(c) is incapable of performing his or her duties as a member.

PART 4 DEPUTY COMMISSIONER OF HARMFUL DIGITAL COMMUNICATIONS AND DEPUTY COMMISSIONER OF DATA PROTECTION AND PRIVACY

22 Appointment of Deputy Commissioners

(1) The Commissioner may, with the prior approval of the Commission, appoint:

(a) the Deputy Commissioner of Harmful Digital Communications; and

(b) the Deputy Commissioner of Data Protection and Privacy.

(2) The appointment of a Deputy Commissioner under paragraphs (1)(a) and (b) must be based on merit and must follow a fair and transparent selection process.

(3) A person may be eligible for appointment as the Deputy Commissioner of Harmful Digital Communications if he or she has reasonable experience and knowledge:

(a) in the operation of social media services; or

(b) in the operation of the internet industry; or

(c) in public policy relating to the communications sector.

(4) A person may be eligible for appointment as the Deputy Commissioner of Data Protection and Privacy if he or she has reasonable experience and knowledge:

(a) in the operation of data protection and privacy services; or

(b) in the operation of the internet and computer security industry; or

(c) in public policy relating to the communications sector.

(5) The Commissioner is to determine the terms and conditions of employment of a Deputy Commissioner.

23 Term of office

A Deputy Commissioner is to hold office for a period of 5 years and is eligible for re-appointment for 1 term only.

24 Functions of the Deputy Commissioners

(1) The Deputy Commissioners have the following functions:

(a) to establish and maintain relationships with domestic and foreign service providers, online content hosts, and agencies (as appropriate) to achieve the purpose of this Act; and

(b) to provide education and advice on policies for online safety and conduct on the Internet; and

(c) such other functions that may be conferred on the Deputy Commissioners by this Act or any other Act.

(2) In addition to subsection (1):

(a) for the Deputy Commissioner of Harmful Digital Communications - to receive and determine complaints about harm caused to individuals by digital communications; and

(b) for the Deputy Commissioner of Data Protection and Privacy - to receive and determine complaints related to data protection and privacy breaches.

25 Powers of a Deputy Commissioner

A Deputy Commissioner has the power to do all things necessary or convenient to be done for or in connection with the performance of his or her functions under this Act.

26 Resignation of a Deputy Commissioner

A Deputy Commissioner may resign by giving 3 months written notice to the Commissioner.

27 Removal of a Deputy Commissioner

The Commissioner may, on the approval of the Commission, remove a Deputy Commissioner if he or she is satisfied that the Deputy Commissioner:

(a) is incapacitated and is unable to perform his or her functions; or

(b) commits a serious misconduct; or

(c) breaches the terms and conditions of his or her employment; or

(d) engages in any activity in the course of his or her employment for personal financial gain; or

(e) neglects to carry out his or her functions under this Act or any other Act.

28 Contractors to assist the Deputy Commissioners

(1) The Commissioner may, on the advice of a Deputy Commissioner and on the approval of the Commission, engage persons as contractors to assist a Deputy Commissioner.

(2) A person engaged must have the appropriate qualifications, skills or experience to assist the Deputy Commissioner.

(3) The Commissioner is to determine, in writing, the terms and conditions of engagement of the person.

PART 5 COMPLAINTS

29 Submission of complaints

(1) The Commissioner is to establish a system for receiving complaints relating to:

(a) services provided; and

(b) decisions made by a Deputy Commissioner.

(2) The Commissioner has the following functions in relation to the complaints made under subsection (1):

(a) to receive complaints through any means of communication deemed appropriate; and

(b) to maintain a register of complaints; and

(c) in the case of where a complaint relates to a service of a Deputy Commissioner- to forward the complaint to the Commission to consider and make a decision.

(3) A decision must be made on a complaint within 21 working days after the Commissioner receives the complaint.

PART 6 MISCELLANEOUS PROVISIONS

30 Funds of the Authority

The funds of the Authority consist of the following:

(a) monies appropriated to the Authority by Parliament; and

(b) grants from aid donors or other international organisations; and

(c) monies received from any other source.

31 Accounts of the Authority

(1) The Authority is to keep proper accounts and other records in respect of its receipts and expenditures and is to prepare an annual statement of accounts in respect of each financial year.

(2) The accounts of the Authority are to be audited by the Auditor- General at the end of each financial year.

(3) The Authority must provide the Minister with a copy of the audited accounts referred to in subsection (2).

32 Annual reports

The Authority must within 3 months after the end of each financial year provide a report to the Minister relating to the operations of the Authority for the preceding year.

33 Immunity

(1) A civil or criminal proceedings must not be brought against any staff of the Authority, the Commissioner, a Deputy Commissioner or a member of the Commission for anything done or omitted to be done in good faith in performing his or her functions or exercising his or her powers under this Act.

(2) Subsection (1) does not apply if the staff of the Authority, the Commissioner, a Deputy Commissioner or a member of the Commission acted in bad faith in performing his or her functions or exercising his or her powers under this Act.

34 Regulation

The Minister may, on the advice of the Commission, make Regulations prescribing matters:

(a) required or permitted by this Act to be prescribed; or

(b) that are necessary or convenient to be prescribed for the better carrying out or giving effect to the provisions of this Act.

35 Commencement

This Act commences on the day on which it is published in the Gazette.

RÉPUBLIQUE DE VANUATU

LOI N^{O}15 DE 2024 RELATIVE À L'AUTORITÉ DE LA SÉCURITÉ NUMÉRIQUE

Sommaire

TITRE 1 DÉFINITIONS

1 Définitions 3

TITRE 2 AUTORITÉ DE LA SÉCURITÉ NUMÉRIQUE ET COMMISSAIRE

Sous-titre 1 Création de l'Autorité de la sécurité numérique

2 Création 5
4 Pouvoirs 5

Sous-titre 2 Commissaire de l'Autorité

5 Nomination du commissaire 6
6 Fonctions du commissaire 6
7 Pouvoirs du commissaire 7
8 Délégation de fonctions et de pouvoirs 7
9 Démission du commissaire 7
10 Déchéance du mandat du commissaire 7
11 Cessation des fonctions de Commissaire 8

Sous-titre 3 Autre personnel

12 Autre personnel de l'Autorité 8

TITRE 3 COMMISSION DE LA SÉCURITÉ NUMÉRIQUE

13 Création de la Commission 10
14 Composition 10
15 Fonctions 10
16 Pouvoirs 10
17 Délégation de fonctions et de pouvoirs 11
18 Président et vice-président de la Commission 11
19 Réunions de la Commission 11

20 Indemnités de séances des membres de la Commission....12
21 Révocation d'un membre de la Commission....12

TITRE 4 COMMISSAIRE ADJOINT AUX COMMUNICATIONS NUMÉRIQUES PRÉJUDICIABLES ET COMMISSAIRE ADJOINT À LA PROTECTION DES DONNÉES ET DE LA VIE PRIVÉE

22 Nomination des commissaires adjoints....13
23 Mandat....14
24 Fonctions des commissaires adjoints....14
25 Pouvoirs d'un commissaire adjoint....14
26 Démission d'un commissaire adjoint....14
27 Révocation d'un commissaire adjoint....15
28 Contractants chargés d'assister les commissaires adjoints....15

TITRE 5 PLAINTES

29 Dépôt des plaintes....16

TITRE 6 DISPOSITIONS DIVERSES

30 Fonds de l'Autorité....17
31 Comptes de l'Autorité....17
32 Rapports annuels....17
33 Immunité....17
34 Règlementation....17
35 Entrée en vigueur....18

RÉPUBLIQUE DE VANUATU

Promulguée : **05/12/2024**
Entrée en vigueur : **02/01/2025**

LOI N^{O} 15 DE 2024 RELATIVE À L'AUTORITÉ DE LA SÉCURITÉ NUMÉRIQUE

Loi qui prévoit l'établissement, le fonctionnement et la gestion de l'Autorité de sécurité numérique et d'autres questions connexes.

Le Président de la République et le Président du Parlement promulguent le texte suivant :

TITRE 1 DÉFINITIONS

1 Définitions

Dans la présente Loi, sauf intention contraire :

Autorité désigne l'Autorité de la sécurité numérique créée en vertu de l'article 2 ;

Commission désigne la Commission de la sécurité numérique créée en vertu de l'article 12 ;

commissaire désigne un commissaire nommé en vertu du paragraphe 5 1) ;

commissaire adjoint désigne le commissaire adjoint aux communications numériques préjudiciables ou le commissaire adjoint à la protection des données et de la vie privée en vertu de l'article 21 ;

numérique désigne la technologie électronique qui génère, stocke et traite des données en fonction de 2 états - positif et non positif ;

communication numérique signifie :

a) tout courriel, appel téléphonique, messagerie sur les réseaux sociaux, sms ou message texte, tchat sur le web, blog, podcast ou vidéo ;

b) tout écrit, photographie, image, enregistrement ou autre élément communiqué par voie électronique ; ou

c) toute autre forme de communication électronique ;

contenu numérique signifie toute information se présentant sous la forme d'une communication numérique ;

sécurité numérique signifie la protection des appareils électroniques connectés à l'internet contre les menaces potentielles et les intrus, afin que la plateforme numérique puisse être utilisée en toute sécurité ;

organisme public désigne :

a) un ministère ;

b) un bureau ou un organisme créé en vertu de la Constitution ;

c) un bureau ou un organisme créé en vertu d'une Loi votée par le Parlement ; ou

d) une agence prescrite.

Ministre désigne le ministre chargé des technologies de l'information et de la communication ;

TITRE 2 AUTORITÉ DE LA SÉCURITÉ NUMÉRIQUE ET COMMISSAIRE

Sous-titre 1 Création de l'Autorité de la sécurité numérique

2 Création

1) Est ainsi créé l'Autorité de la sécurité numérique.

2) L'Autorité est :

a) une personne morale avec une succession perpétuelle ;

b) dotée d'un sceau commun ; et

c) capable d'ester et d'être poursuivie en justice.

3 Fonctions

1) L'Autorité a les fonctions suivantes :

a) promouvoir la sécurité, la communication et le contenu numériques à Vanuatu ;

b) coordonner les activités relatives à la sécurité, à la communication et au contenu numériques avec un organisme public ;

c) aider à protéger le public contre tout problème de sécurité numérique et tout préjudice ;

d) représenter Vanuatu au niveau international sur les questions relatives à la protection des données et de la vie privée et à la communication numérique préjudiciable ; et

e) toute autre fonction pouvant être conférée à l'Autorité par la présente Loi ou toute autre Loi.

4 Pouvoirs

1) L'Autorité a le pouvoir de prendre toutes mesures nécessaires ou utiles à l'exercice de ses fonctions qui lui sont confiées par la présente Loi.

2) Sans limiter la portée du paragraphe 1), l'Autorité a le pouvoir de faire tout ou en partie ce qui suit :

a) acquérir, acheter, détenir, gérer et céder des biens immobiliers ou mobiliers ;

b) développer tout terrain ou autre propriété et construire et entretenir ces bâtiments ou autres structures ; et

c) conclure des accords avec toute autorité locale, corporation, société, entreprise ou personne pour la gestion et l'entretien de tout terrain, bâtiment ou installation.

Sous-titre 2 Commissaire de l'Autorité

5 Nomination du commissaire

1) La Commission nomme le commissaire.

2) Toute personne peut être nommée commissaire si elle répond aux critères suivants :

a) être citoyen de Vanuatu ;

b) avoir un master en sécurité numérique ou en cybersécurité délivré par une université reconnue ;

c) avoir 5 à 10 ans d'expérience dans le domaine des technologies de l'information et de la communication ;

d) avoir au moins 5 ans d'expérience en gestion de bureau.

3) Il appartient à la Commission de déterminer les conditions d'emploi du commissaire.

4) La nomination du commissaire doit suivre une procédure de sélection équitable et transparente et doit être fondée sur le mérite.

5) Le commissaire est nommé pour un mandat de 5 ans et n'est rééligible qu'une seule fois.

6 Fonctions du commissaire

Le commissaire a les fonctions suivantes :

a) conseiller la Commission et le Ministre sur toute question relative à son application ;

b) conseiller le Ministre, après avis de la Commission, sur les questions de sécurité numérique ;

c) gérer et superviser les opérations de l'Autorité ;

d) encourager et soutenir un organisme public à suivre les meilleures pratiques et normes en matière de sécurité numérique ;

e) produire, publier, émettre, diffuser et distribuer des rapports, des documents, des périodiques ou toute autre information, sur les conseils de la Commission ;

f) superviser les commissaires adjoints ; et

g) toute autre fonction qui peut lui être conférée par la présente Loi ou toute autre Loi.

7 Pouvoirs du commissaire

Le commissaire est habilité à prendre toutes mesures nécessaires ou utiles à l'exercice des fonctions qui lui sont confiées au titre de la présente Loi.

8 Délégation de fonctions et de pouvoirs

1) Sous réserve des dispositions du présent article, le commissaire peut déléguer ses fonctions et ses pouvoirs à un membre du personnel de l'Autorité.

2) Le pouvoir de délégation ne peut être délégué par le Commissaire.

3) Toute délégation effectuée en application du paragraphe 1) est soumise aux instructions, lignes directrices ou conditions imposées par le Commissaire.

4) La délégation visée au présent article n'empêche pas le commissaire d'exercer ses pouvoirs.

5) Une délégation peut être révoquée à tout moment par le commissaire conformément au présent article.

9 Démission du commissaire

Le commissaire peut démissionner en donnant un préavis de trois mois à la Commission.

10 Déchéance du mandat du commissaire

Une personne ne peut être nommée commissaire si elle :

a) est membre du Parlement, d'un conseil provincial ou d'un conseil municipal ;

b) a été reconnu coupable d'un délit et condamné à une peine d'emprisonnement de 12 mois ou plus, avec ou sans sursis ; ou

c) est directeur d'une société.

11 Cessation des fonctions de Commissaire

La Commission met fin aux fonctions du commissaire dans les cas suivants :

a) il devient membre du Parlement, d'un conseil provincial ou d'un conseil municipal ;

b) s'il est frappé d'incapacité et n'est pas en mesure d'exercer ses fonctions ;

c) est déclaré en faillite ;

d) est reconnu coupable d'un délit et condamné à une peine d'emprisonnement de 12 mois ou plus, qu'il s'agisse ou non d'une peine avec sursis ;

e) commet une faute grave ;

f) enfreint les conditions d'emploi ;

g) détourne des fonds de l'Autorité ; ou

h) omet de s'acquitter des fonctions qui lui sont dévolues par la présente Loi ou toute autre Loi.

Sous-titre 3 Autre personnel

12 Autre personnel de l'Autorité

l) Le commissaire peut, avec l'accord préalable de la Commission, employer tout autre personnel de l'Autorité qu'il juge nécessaire à l'exécution correcte et efficace des fonctions de cette dernière.

2) Le commissaire fixe les conditions d'emploi des autres membres du personnel de l'Autorité.

3) La nomination de tout autre membre du personnel doit suivre une procédure de sélection équitable et transparente et doit être fondée sur le mérite.

TITRE 3 COMMISSION DE LA SÉCURITÉ NUMÉRIQUE

13 Création de la Commission

Est créée la Commission de la sécurité numérique.

14 Composition

1) La Commission est composée des personnes suivantes :

   a) le Directeur général du Ministère du Premier ministre ;

   b) un représentant de l'Université nationale de Vanuatu nommée par le Chancelier ; et

   c) le directeur du Forum de gouvernance de l'internet.

2) Sous réserve du paragraphe 3), le Ministre devra nommer les membres visés à l'alinéa 1) b).

3) La personne nommée en vertu de l'alinéa 1) b) doit :

   a) avoir une qualification tertiaire dans le domaine de la cybersécurité et de la sécurité numérique ;

   b) ne doit avoir aucune condamnation pénale ni aucun casier judiciaire ; et

   c) être citoyen de Vanuatu.

4) Le membre nommé en vertu de l'alinéa 1) b), est nommé pour un mandat de trois ans et est renouvelable seulement une fois.

15 Fonctions

La Commission a pour fonction de déterminer les normes suivantes :

a) les normes de sécurité numérique ;

b) les normes de communication numérique ; et

c) les normes relatives au contenu numérique.

16 Pouvoirs

La Commission a le pouvoir de faire tout ce qui est nécessaire ou utile à l'exercice de ses fonctions en vertu de la présente Loi.

17 Délégation de fonctions et de pouvoirs

1) La Commission peut, sous réserve des dispositions du présent article, déléguer ses fonctions et ses pouvoirs au chef de direction ou à un de ses membres.

2) La Commission ne peut déléguer son pouvoir de délégation.

3) Toute délégation faite conformément au paragraphe 1) est soumise aux instructions, lignes directrices ou conditions imposées par la Commission.

4) La délégation visée au présent article n'empêche pas la Commission d'exercer ses pouvoirs.

5) Une délégation peut être révoquée à tout moment par la Commission conformément au présent article.

18 Président et vice-président de la Commission

1) Le directeur général est le président de la Commission.

2) Les membres de la Commission élisent parmi eux un vice-président.

3) Le vice-président est élu pour 1 an renouvelable.

19 Réunions de la Commission

1) La Commission se réunit au moins une fois par trimestre au cours d'une année et peut tenir toute autre réunion nécessaire à la bonne exécution de ses fonctions conformément à la présente Loi.

2) Le président préside toutes les réunions de la Commission et, en son absence le vice-président y préside.

3) Le quorum est atteint lorsque 2 membres de la Commission sont présents à la réunion.

4) Chaque membre présent dispose d'une voix et les questions soulevées lors de la réunion sont tranchées à la majorité des voix.

5) Lorsqu'il y a égalité des voix, le président ou le vice-président (s'il préside la réunion) dispose d'une voix prépondérante.

6) Le commissaire est le secrétaire de la Commission.

7) Le commissaire, après consultation du président, notifie aux autres membres de la Commission le lieu, l'heure et la date de la réunion.

8) Sous réserve des dispositions de la présente Loi, la Commission peut déterminer et réglementer ses propres procédures.

20 Indemnités de séances des membres de la Commission

Le ministre peut, par arrêté, fixer les indemnités de séance des membres de la Commission.

21 Révocation d'un membre de la Commission

Tout membre nommé conformément à l'alinéa 13 1) b) est révoqué s'il :

a) manque à trois réunions consécutives de la Commission sans autorisation de celle-ci ;

b) est suspendu de sa profession ; ou

c) est incapable d'exercer ses fonctions de membre.

TITRE 4 COMMISSAIRE ADJOINT AUX COMMUNICATIONS NUMÉRIQUES PRÉJUDICIABLES ET COMMISSAIRE ADJOINT À LA PROTECTION DES DONNÉES ET DE LA VIE PRIVÉE

22 Nomination des commissaires adjoints

1) Le commissaire peut, avec l'accord préalable de la Commission, nommer :

a) le commissaire adjoint aux communications numériques préjudiciables ; et

b) le commissaire adjoint chargé de la protection des données et de la vie privée.

2) La nomination d'un commissaire adjoint en vertu des alinéas 1) a) et b) doit être fondée sur le mérite et suivre une procédure de sélection équitable et transparente.

3) Pour être nommée commissaire adjoint aux communications numériques préjudiciables, la personne doit posséder une expérience et des connaissances suffisantes :

a) dans l'exploitation des services de médias sociaux ;

b) dans le fonctionnement de l'industrie de l'internet ; ou

c) dans la politique publique relative au secteur de la communication.

4) Pour être nommé commissaire adjoint à la protection des données et de la vie privée, la personne doit posséder une expérience et des connaissances suffisantes :

a) dans le fonctionnement des services de protection des données et de la vie privée ;

b) dans le fonctionnement de l'industrie de l'internet et de la sécurité informatique ; ou

c) dans la politique publique relative au secteur de la communication.

5) Le commissaire détermine les conditions d'emploi d'un commissaire adjoint.

23 Mandat

Le commissaire adjoint a un mandat de 5 ans renouvelable seulement une fois.

24 Fonctions des commissaires adjoints

1) Les commissaires adjoints ont les fonctions suivantes :

a) établir et maintenir des relations avec les fournisseurs de services locaux et étrangers, les hébergeurs de contenu en ligne et les agences (le cas échéant) afin d'atteindre l'objectif de la présente Loi ;

b) fournir une éducation et des conseils sur les politiques de sécurité en ligne et de conduite sur l'internet ; et

c) exercer toute autre fonction qui leur sont conférées par la présente Loi ou toute autre Loi.

2) Outre le paragraphe 1) :

a) le commissaire chargé des communications numériques préjudiciables reçoit et examine les plaintes concernant les dommages causés aux individus par les communications numériques ; et

b) le commissaire chargé de la protection des données et de la vie privée communications numériques préjudiciables reçoit et examine les plaintes relatives aux violations de la protection des données et de la vie privée

25 Pouvoirs d'un commissaire adjoint

Les commissaires ont le pouvoir de faire tout ce qui est nécessaire ou utile à l'exercice de leurs fonctions en vertu de la présente Loi.

26 Démission d'un commissaire adjoint

Le commissaire peut démissionner en donnant par écrit un préavis de trois mois à la Commission.

27 Révocation d'un commissaire adjoint

La Commission peut, sur approbation de la Commission, révoquer un commissaire adjoint si elle est convaincue que celui-ci :

a) est frappé d'incapacité et n'est pas en mesure d'exercer ses fonctions ;

b) a commis une faute grave ;

c) viole les conditions de son emploi ;

d) s'engage dans une activité dans le cadre de son emploi en vue d'un gain financier personnel ; ou

e) néglige de s'acquitter des fonctions qui lui incombent en vertu de la présente Loi ou de toute autre Loi.

28 Contractants chargés d'assister les commissaires adjoints

1) Le commissaire peut, sur avis d'un commissaire adjoint et avec l'approbation préalable de la Commission, engager des personnes en tant que contractants pour assister un commissaire adjoint.

2) Toute personne engagée doit avoir les qualifications, les compétences ou l'expérience nécessaires pour assister le commissaire adjoint.

3) Le commissaire fixe par écrit les conditions d'engagement de la personne.

TITRE 5 PLAINTES

29 Dépôt des plaintes

1) Le commissaire doit mettre en place un système de réception des plaintes pour :

   a) les services fournis ; et

   b) les décisions prises par un commissaire.

2) Pour les plaintes déposées conformément au paragraphe 1), le commissaire a les fonctions suivantes :

   a) recevoir les plaintes par tout moyen de communication jugé approprié ;

   b) tenir un registre des plaintes ;

   c) s'il s'agit d'une plainte relative à un service fourni par un commissaire, transmettre celle-ci à la Commission pour examen et prise de décision.

3) Le commissaire doit prendre une décision dans les 21 jours ouvrables suivant la réception de la plainte.

TITRE 6 DISPOSITIONS DIVERSES

30 Fonds de l'Autorité

Les fonds de l'Autorité de composent des éléments suivants :

a) les fonds alloués à l'Autorité par le Parlement ;

b) les subventions des donateurs ou d'autres organisations internationales ; et

c) les fonds reçus de toute autre source.

31 Comptes de l'Autorité

1) L'Autorité doit tenir une comptabilité appropriée et d'autres registres concernant ses recettes et ses dépenses et doit préparer un état annuel des comptes pour chaque exercice financier.

2) Les comptes de l'Autorité doivent être vérifiés par le contrôleur général à la fin de chaque exercice.

3) L'Autorité doit fournir au Ministre une copie des comptes vérifiés visés au paragraphe 2).

32 Rapports annuels

L'Autorité doit, dans les 3 mois suivant la fin de chaque exercice financier, fournir au Ministre un rapport sur ses activités de l'année précédente.

33 Immunité

1) Aucune procédure civile ou pénale ne peut être engagée contre un membre du personnel de l'Autorité, le commissaire, un commissaire adjoint ou un membre de la Commission pour un acte ou une omission commise de bonne foi dans l'exercice de ses fonctions ou de ses pouvoirs en vertu de la présente Loi.

2) Le paragraphe 1) ne s'applique pas lorsque le personnel de l'Autorité, le commissaire, un commissaire adjoint ou un membre de la Commission a agi de mauvaise foi dans l'exercice de ses fonctions ou des pouvoirs qui lui sont conférés en vertu de la présente Loi.

34 Règlementation

Le Ministre peut, sur avis de la Commission, prendre des règlements concernant les questions :

a) dont la prescription est requise ou permise par la présente Loi ; ou

b) dont la prescription est nécessaire ou opportune pour une meilleure application ou mise en œuvre des dispositions de la présente Loi.

35 Entrée en vigueur

La présente Loi entre en vigueur au jour de sa publication au Journal officiel.

REPUBLIC OF VANUATU

ANTI-MONEY LAUNDERING AND COUNTER-TERRORISM FINANCING (AMENDMENT) ACT NO. 16 OF 2024

Arrangement of Sections

1 Amendment 2

2 Transitional Provision 2

3 Commencement 2

REPUBLIC OF VANUATU

Assent: **05/12/2024**
Commencement: **02/01/2025**

ANTI-MONEY LAUNDERING AND COUNTER-TERRORISM FINANCING (AMENDMENT) ACT NO. 16 OF 2024

An Act to amend the Anti-Money Laundering and Counter-Terrorism Financing Act No. 13 of 2014.

Be it enacted by the President and Parliament as follows-

1 Amendment

The Anti-Money Laundering and Counter-Terrorism Financing Act No. 13 of 2014 is amended as set out in the Schedule.

2 Transitional Provision

A staff of the Unit who was employed before the commencement of this Act is to continue to be employed in the office as if he or she was employed by the Attorney General on the same terms and conditions of employment with accrued and accruing entitlements.

3 Commencement

This Act commences on the day on which it is published in the Gazette.

SCHEDULE

AMENDMENTS OF ANTI-MONEY LAUNDERING AND COUNTER-TERRORISM FINANCING ACT NO. 13 OF 2014

1 Section 4

After "established" insert "within the Office of the Attorney General"

2 After subsection 7(2)

Insert

"(2A) The Director must:

(a) provide an annual written report to the Attorney General on matters relating to the administration of this Act; and

(b) if requested by the Attorney General, provide a report on a particular matter under this Act or any other Act.

(2B) The Director has the power to do all things necessary or convenient to be done for or in connection with the performance of his or her functions under this Act."

3 After section 7

Insert

"7A Appointment of the Deputy Director

(1) The Attorney General is to appoint a Deputy Director of the Unit.

(2) The Attorney General is to determine the terms and conditions of employment of the Deputy Director."

4 Subsections 8(1) and (2)

Delete "Director", substitute "Attorney General"

RÉPUBLIQUE DE VANUATU

LOI N°16 DE 2024 SUR LA LUTTE CONTRE LE BLANCHIMENT D'ARGENT ET LE FINANCEMENT DU TERRORISME (MODIFICATION)

Sommaire

1 Modification 2

2 Disposition transitoire 2

3 Entrée en vigueur 2

RÉPUBLIQUE DE VANUATU

Promulguée: **05/12/2024**
Entrée en vigueur: **02/01/2025**

LOI N°16 DE 2024 SUR LA LUTTE CONTRE LE BLANCHIMENT D'ARGENT ET LE FINANCEMENT DU TERRORISME (MODIFICATION)

Loi modifiant la Loi N°13 de 2014 sur la Lutte contre le blanchiment d'argent et le financement du terrorisme.

Le Président de la République et le Parlement promulguent le texte suivant :

1 Modification

La Loi N°13 de 2014 sur la Lutte contre le blanchiment d'argent et le financement du terrorisme est modifiée tel que prévu à l'Annexe.

2 Disposition transitoire

Le personnel du Bureau qui était employé immédiatement avant l'entrée en vigueur de la présente Loi reste en fonction comme s'il était employé par l'Attorney général selon les mêmes conditions de service et avec les droits acquis.

3 Entrée en vigueur

La présente Loi entre en vigueur à la date de sa publication au Journal Officiel.

ANNEXE

MODIFICATION DE LA LOI N°13 DE 2014 SUR LA LUTTE CONTRE LE BLANCHIMENT D'ARGENT ET LE FINANCEMENT DU TERRORISME

1 Article 4

Insérer après "est établi", "au sein du Bureau de l'Attorney général"

2 Après le paragraphe 7 2)

Insérer

« 2A) Le Directeur doit :

a) présenter un rapport écrit annuel à l'Attorney général sur les questions relatives à l'application de la présente Loi ; et

b) présenter, à la demande de l'Attorney général, un rapport sur une question particulière relevant de la présente Loi ou de toute autre loi.

2B) Le Directeur est habilité à prendre toutes les mesures nécessaires ou utiles à l'exercice de ses fonctions en vertu de la Loi. »

3 Après l'article 7

Insérer

« 7A Nomination d'un Directeur adjoint

1) L'Attorney Général nomme un directeur adjoint du Bureau.

2) L'Attorney général détermine les conditions d'emploi du Directeur adjoint. »

4 Paragraphes 8 1) et 2)

Supprimer et remplacer « Directeur » par « Attorney général »

PUBLIC NOTICE UNDER SECTION 162 (1) OF THE COMPANIES ACT NO.25 OF 2012

NOTICE NO. 174 OF 2024

Neptune Pacific Direct Line Pte Limited, ("NPDL") currently registered to do business in Vanuatu as an Oversea Company, advises that it is about to cease carrying on business in Vanuatu.

The Company has traded under the business name of Transam, and its functions in Vanuatu will be carried on from 31st of December 2024 by Transam (Vanuatu) Limited, a local company wholly owned by NPDL.

Customers of NPDL will not notice any change in either service or personnel.

This notice placed by:- SFAI Barrett & Partners Vanuatu

PO Box 240

Port Vila

(on behalf of the Neptune Pacific Direct Line Pte. Limited)

UTILITIES REGULATORY AUTHORITY
ACT NO.11 OF 2007

MONTHLY ADJUSTED PRICE OF ELECTRICITY OF PORT VILA FOR DECEMBER 2024

Notice No. 175 of 2024

In the exercise of the powers conferred upon the Authority by subsection 13(1) and section 18 of the Utilities Regulatory Authority Act No.11 of 2007 (as amended) and in light of the Arbitration Panel Award of 5th June 2021 in the Matter of the 2020 Arbitration between *Union Electrique du Vanuatu Ltd and the Government of the Republic of Vanuatu* (Represented by the Utilities Regulatory Authority), the Authority makes the following approval of UNELCO's monthly adjusted electricity price for the concession of Port Vila.

1 **Monthly Adjusted Price of Electricity to be charged by UNELCO.**
The Authority approves UNELCO's monthly adjusted price of electricity of **60.16Vatu/kWh** to be charged to electricity consumers of the Port Vila electricity concession.

2 **Monthly Tariff Adjustment Formula and Parameters**
The monthly tariff adjustment formula and parameters used to adjust the price, as submitted to the Authority by UNELCO, are set out in the schedule.

3 **Application of the Monthly Adjusted Price**
The monthly adjusted price applies to electricity customers of the concessions of Port Vila for the month of December 2024.

4 **Commencement date**
This Approval is deemed to commence on 10th of December 2024.

Made at Port Vila this 10th day of December 2024.

Jesse Benjamin
Chief Executive Officer
Utilities Regulatory Authority

Utilities Regulatory Authority
PMB 9093, Port Vila, Vanuatu
Tel: (678) 23335; www.ura.gov.vu

SCHEDULE

The Monthly Electricity Price Adjustment Formula is set out below:

$$P = P_0 \times \left\{0.375 \times \frac{G}{G_0} \times \frac{N}{N_0} + 0.049 + \left[0.257 \times \frac{M}{M_0} + 0.019 \times \frac{IM}{IM_0} \times \left(0.6 + 0.4 \times \frac{C}{C_0}\right) + 0.300\right] \times \frac{V_0}{V}\right\} + PPA + \frac{Xo}{V}$$

Where:

Base Indexes:	**Definitions:**
P_0	Base Price determined by the 2020 Arbitration Panel by way of its Final Decision of 5th June 2021 as: **P_0 = 48.60 Vatu/kWh**
G_0	Is the marginal cost of fuel and lubricant oil used for the thermal generation as determined by the Panel to compute P_0, generated from thermal generation: **G_0 = 20.3593 Vatu/kWh**
M_0	Base index corresponding to the average of the first and second quarter of 2020 index of the Port Vila Consumer Price Index (CPI) published by the Vanuatu National Statistics Office (VNSO): **CPI_0 = 168.85**
IM_0	Is the base index of the indices "Materiel" (IM28), of July 2020, published by the institut des statistiques et des Etudes Economiques (ISEE) of New Caledonia: **IM_0 = 108.72**
N_0	Ratio resulting from dividing the quantity if electricity generated by UNELCO from thermal sources and total electricity generated by UNELCO, as per the panel determinations to compute P_0 : **N_0 = 0.8592**
C_0	Base value of the exchange rate between the Pacific Franc (XPF) and the Vatu (VUV); it is based on the average of daily exchange rates for the month of August 2020, as provided by ANZ Bank in Port Vila: **C_0 = 1.1569**
V_0	Base volume (Demand -in-P) determined by the Panel to compute P_0: **V_0 = 58,431,274**
X_0	Total amount of under-collection, in Vatu, determined by the Panel for the period between the effective date of the new P_0, September 2, 2020, and the eve of the implementation of the new P_0, May 31 202, divided by the period remaining for the recovery (51 Months) and multiplied by 12 months: **X_0 = 34,728,358**
Current Indexes:	
P	The Monthly Applicable Electricity Price is: **60.16 Vatu/kWh.**
G	The current weighted unit cost of diesel, copra oil, and lubricant oil used for thermal generation. It is calculated and updated once per month: **27.8529 Vatu/kWh.**
M	The current updated CPI for Quarter 3 in 2023 as determined by the VNSO[1] is set at: **217.50.** Latest available value of the Port Vila Consumer Price Index, as published by the Vanuatu National Statistics Office (VNSO), at the moment of calculation of the monthly Reference Price P.
IM	The 'Indice Materiel' (IM28), published by the institute de Statistiques et des Etudes Economiques (ISEE) of New Caledonia or the journal officiel (Gazette) of New Caledonia, index corresponding to the first of the two months preceding the calculation of the monthly reference price **P:126.61** Website: http://www.isee.nc/economie-entreprises/entreprises-secteurs-d-activites/immobilier-construction

[1] Vanuatu National Statistics Office

N	Is the average proportion of power generated from thermal generation (diesel and copra oil) and is calculated as a ratio of UNELCO thermal generation in UNELCO's overall generation. **N = 0.9268**
C	Is the selling exchange rate conversation for Pacific Franc (XPF) to Vatu (VUV); it is based on the average of daily exchange rates for the month preceding the tariff adjustment, as provided by ANZ bank in Port Vila: **C = 1.1470 XPF/VUV.**
V	Is the demand, expressed in units of P, updated every month based on the trailing twelve months. The trailing twelve months for this variable are calculated from (and including) the second month preceding the tariff adjustment. **V = 62,283,428**
PPA	Purchased power costs over the twelve months beginning from m-2 (m being the month of the reference price P being calculated) and the eventual benefit sharing; PPA is calculated and updated every month. PPA = **0.5448**

Applying the current indexes into the monthly electricity price adjustment formula as set-out above, the computed monthly electricity price effective for the month of **December 2024 is 60.16 Vatu/kWh.**

UTILITIES REGULATORY AUTHORITY
ACT NO.11 OF 2007

MONTHLY ADJUSTED PRICE OF ELECTRICITY FOR VANUATU UTILITIES AND INFRASTRUCTURE CONCESSION FOR DECEMBER 2024

Notice No. 176 of 2024

In the exercise of the powers conferred upon the Authority by subsection 13(1) and section 18 of the Utilities Regulatory Authority Act No.11 of 2007 (as amended), the Authority makes the following approval of VUI Ltd's monthly adjusted electricity price for the concession of Santo, Ambae, Maewo, and Vanua Lava.

1 Monthly Adjusted Price of Electricity to be charged by VUI.

(1) The Authority approves VUI Ltd's monthly adjusted price of electricity of **61.97 Vatu/kWh** to be charged to electricity consumers of the Santo, Ambae, Maewo and Vanua Lava electricity concessions.

(2) To avoid doubt, the tariff for the following as determined under Notice No.9 of 2024 remains unchanged:

(a) Consumption charge for Force Majeure;

(b) Consumption charge for NGEF;

(c) Solar Connection Charge.

3 Revised Monthly Tariff Adjustment Formula and Parameters

The revised monthly tariff adjustment formula and parameters was approved by the URA commission on 3rd July 2024 and used to adjust the price, as submitted to the Authority by VUI, are set out in the schedule.

4 Application of the Monthly Adjusted Price

The monthly adjusted price applies to electricity customers of the concessions of Santo, Ambae, Maewo, and Vanua Lava for the month of December 2024.

5 Commencement date

This Determination comes into force on 2nd December 2024.

Made at Port Vila this 2nd day of December 2024.



Jesse Benjamin
Chief Executive Officer
Utilities Regulatory Authority

SCHEDULE

The Monthly Electricity Price Adjustment Formula is set out below:

$$P_M = P_0 \times \left(0.26 \times \left(\frac{D_1}{D_0} \times \frac{R_1}{R_0}\right) + 0.16 \times \frac{CAPEX_1}{CAPEX_0} + \left[0.36 + 0.22 \times \left(\frac{CPI_1}{CPI_0} \times X\right)\right] \times V\right) + PPA$$

Where:

Parameter	Description of Parameter	Frequency of Adjustment
P_0	This is the base price set at 60.75 Vt/kWh	N/A
D_0	This is the weighted average cost of diesel oil per liter for VUI's concessions (except Maewo) set for the tariff period at 125.68 (2.d.p.)	N/A
D_1	This is the weighted average cost of diesel oil per liter for the prior month for VUI's concessions (except Maewo) computed as follows[1]. $$D_1 = \frac{D_{Luganville} + D_{Vanua\ Lava} + D_{Ambae}}{P_{Luganville} + P_{Vanua\ Lava} + P_{Ambae}}$$ Whereby: • D is the diesel cost (price per liter multiplied by quantity of litres used. • P is the liters used in generation.	Monthly
R_0	This is the portion of diesel oil output in the generation mix for VUI's concessions (except Maewo). This is set for the tariff period at 0.34 (2.d.p.)	N/A
R_1	This is the portion of diesel oil output in the generation mix for the prior month divided by the averaged total output over the trailing 12 months over VUI's concessions (except Maewo) computed as follows: $$R = \frac{Diesel\ Generation_{m-1}}{Total\ Generation_{m12}}$$ Whereby: • Diesel Generation is the kWh output utilizing diesel for the month prior. • Total Generation is the kWh output utilizing all generating sources averaged over the trailing 12 months.	Monthly
CPI_0	This is the Consumer Price Index for Luganville set at 153.3 (2.d.p.)	N/A
CPI_1	This is the most recent Consumer Price Index published for Luganville by the Vanuatu National Statistics Office.	Annually
X	This is a weighting applied to the CPI adjustment. The weighting is determined by the Authority on VUI's performance based on SAIDI and SAIFI indicators identified by the Authority.	Annually
$CAPEX_0$	This is the cost of investment for VUI's concessions which include recovery of and on investments set at 113,712,679.	Annually
$CAPEX_1$	This is the cost of investment for VUI's concessions for the prior year. This is computed as followings: $$CAPEX_1 = DEP_{n-1} + (NBV_{n-1} + DEP_{n-1} + WC_{n-1} - ZCC_{n-1}) \times RoR$$ Whereby: • DEP_{n-1} is depreciation expense for VUI's investment in the prior year. • NBV_{n-1} is net book value for VUI's investments in the prior year.	Annually

[1] The cost of diesel index may be updated to include Maewo concession area should at any point in time when installed hydro capacity is unable to meet demand and there is reliance on diesel oil to meet this excess demand.

	• WC_{n-1} is VUI's working capital is 10.81% of sales revenue for the prior year. • ZCC_{n-1} is VUI's zero cost capital identified as severance provision balance for the prior year. • RoR is VUI's reasonable rate of return set at 8.4%.	
V	This is the partial limited decoupling for VUI. This is computed as follows: $$V = 1 + V_A$$ Whereby: • V_A is the demand in P percentage change for the prior year of more than +/- 2% band on average forecasted demand in P set at 11,466,207. Annual demand P is the summation of sales and demand revenue for the year divided by the weighted average monthly adjusted base price for the year.	Annually
PPA	This is VUI's cost of IPP/PPAs approved by the Authority. This is computed as follows: $$PPA = \frac{PPA\ Cost_{m-1}}{Sales\ Revenue_{m3}}$$ Whereby: • PPA Cost is VUI's cost of purchased power from IPP/PPAs for the prior month. • Sales revenue is VUI's average sales revenue for the prior three months.	Monthly

Applying the current indexes into the monthly electricity price adjustment formula as set-out above, the computed monthly electricity price effective for the month of December 2024 is **61.97 Vatu/kWh.**