United Nations A/AC.291/9/Add.2

General Assembly

Distr.: General
21 April 2022
English
Original: Arabic/English/Spanish/
Russian

Ad Hoc Committee to Elaborate a Comprehensive International Convention on Countering the Use of Information and Communications Technologies for Criminal Purposes
Second session
Vienna, 30 May–10 June 2022

Compilation of proposals and contributions submitted by Member States on the provisions on criminalization, the general provisions and the provisions on procedural measures and law enforcement of a comprehensive international convention on countering the use of information and communications technologies for criminal purposes

Addendum

V.22-02335 (E) 120522 130522

Contents

IV. Procedural measures and law enforcement

Angola

[Original: English]
[8 April 2022]

Procedural provisions and law enforcement

Means of evidence: documentary evidence (electronic document, digital document), expert evidence (computer expertise).

Means of obtaining evidence: online searches, expeditious preservation of data, expeditious disclosure of data, injunction to submit or grant access to data, search of computer data, seizure of computer data, seizure of electronic mail and recording of communications of a similar nature, interception of communication, actions hidden (deepweb and darkweb).

Recovery of assets and loss of assets in favour of the State: seizure and confiscation of traditional assets and cryptoassets.

The provisions of this chapter should apply to the investigation and criminal prosecution of agents of traditional crimes and not just to the investigation of cybercrimes.

For the elaboration of the concepts related to this chapter, it is possible to resort to the regional and international legal instruments referred to above.[1]

Australia

[Original: English]
[13 April 2022]

The link between criminalization and procedural powers

Australia recognizes that States may wish to ensure that the Convention improves international cooperation for familiar crimes with or without a cyber dimension (such as trespass or murder), by providing a framework for requests and access to electronic evidence located in another jurisdiction, in relation to the commission of such crimes.

The procedural powers, investigative powers and international cooperation frameworks of the Convention to detect, investigate and prosecute cybercrime should apply to the offences listed in the Convention, but should not be restricted to apply only to those offences.

Procedural powers (expanded upon below) under the Convention should apply to other criminal offences committed by means of a computer system or digital technology, as well as the collection of electronic evidence required to detect, investigate and prosecute criminal offences that do not involve a computer system in their commission, that meets the required conditions and thresholds for those procedural powers.

Similarly, the framework for international cooperation under this Convention should apply not only to the criminal offences created by the convention, but, where appropriate, to other criminal offences committed by means of a computer, as well as the collection of electronic evidence required to detect, investigate and prosecute a kinetic criminal offence.

[1] Note by the Secretariat: this reference is to instruments included under a different subheading: African Union Convention on Cyber Security and Protection of Personal Data, Council of Europe Convention on Cybercrime, United Nations Convention against Transnational Organized Crime and United Nations Convention Against Corruption.

Therefore, the purpose of the criminalization chapter is not to restrict the operation of other chapters of the Convention, but, rather, to establish a common standard for a relatively new crime type – cybercrime – across all States.

Procedural measures to combat cybercrime

Procedural law is a critical element for investigating and prosecuting cybercrime. The Convention should provide a clear framework of procedural measures to ensure that law enforcement authorities can obtain the evidence needed to combat cybercrime, underpinned by robust procedural safeguards and limitations that uphold the rule of law, and protections for human rights and fundamental freedoms. The Convention's articles on procedural measures should also respect existing frameworks, and avoid fragmentation of existing international instruments.

Procedural measures should apply to the substantive criminal offences within the Convention, and, consistent with States' domestic legal frameworks, to other criminal offences committed by means of a computer system or digital technology, as well as the collection of electronic evidence required to detect, investigate and prosecute a kinetic criminal offence, that meets the required conditions and thresholds for those procedural powers.

Australia proposes the following procedural measures should be included in the new Convention:

- Orders for the preservation of electronic data (including stored content data, subscriber information, and traffic data)
- Orders for the production of electronic data
- Search and seizure of electronic data
- Real-time collection of electronic data (including traffic data and live interception of content data)
- Orders for emergency and expedited preservation and production of data.

Procedural measures should account for the nature of electronic data, ensuring that data are preserved quickly and effectively, and law enforcement and other relevant authorities can obtain such data quickly and effectively to ensure criminal methodologies and practices in cyberspace do not disrupt authorities' collection efforts.

Conditions, requirements and safeguards for procedural measures

Procedural measures for detecting, investigating and prosecuting cybercrime can engage obligations with respect to human rights and freedoms under relevant international human rights instruments, including the International Covenant on Civil and Political Rights. These may include:

Fair trial and fair hearing rights (International Covenant on Civil and Political Rights, article 14)

Article 14 of the Covenant contains fair trial and fair hearing rights, including procedural guarantees, the rule of law and the presumption of innocence. The Human Rights Committee has stated that "article 14 of the Covenant aims at ensuring the proper administration of justice, and to this end guarantees a series of specific rights".

Article 14 is not an absolute right, it is subject to permissible restrictions provided that those restrictions are prescribed by law and are reasonable, necessary and proportionate means for pursuit of a legitimate objective.

Freedom from interference with privacy (International Covenant on Civil and Political Rights, article 17)

Article 17 of the Covenant establishes the right to freedom from interference with privacy and provides that “no one shall be subjected to arbitrary or unlawful interference with his privacy, family, home or correspondence”.

The content of this right is outlined in greater detail in Human Rights Committee general comment No. 16. It states that such protections “are required to be guaranteed against all such interferences and attacks whether they emanate from State authorities or from natural or legal persons”. Paragraph 3 of general comment No. 16 states that “the term “unlawful” means that no interference can take place except in cases envisaged by the law. Interference authorized by States can only take place on the basis of law, which itself must comply with the provisions, aims and objectives of the Covenant.”

The right to freedom of expression (International Covenant on Civil and Political Rights, article 19, paragraph 2)

Article 19 of the Covenant provides for the right to freedom of expression. Article 19, paragraph 2, of the Covenant recognizes the right to seek, receive and impart information and ideas through any medium, including written and oral communication, the media, broadcasting and commercial advertising.

The right to freedom of expression is not an absolute right. Under article 19, paragraph 3, freedom of expression may be limited as provided for by law and when necessary to protect the rights or reputations of others, national security, public order or public health or morals. Limitations must be prescribed by legislation necessary to achieve the desired purpose and proportionate to the need on which the limitation is predicated.

The objective of the Convention and its procedural measures is to reduce the threat, impact and damage of cybercrime – which may provide a permissible basis for restricting human rights and freedoms when lawful, reasonable, necessary and proportionate.

It will be imperative for the procedural measures set out in the Convention to be established, implemented and applied subject to the conditions and safeguards provided for under the Covenant and other applicable human rights instruments.

Such conditions and safeguards should include, as appropriate for each procedural measure:

- Judicial or other independent supervision or oversight
- Grounds justifying the application of the procedural measure
- Limitations on the scope and duration of the procedural measure
- Consideration of the impact of procedural measures upon the rights, responsibilities and legitimate interests of third parties.

Brazil

[Original: English]
[8 April 2022]

Chapter III

Procedural measures and law enforcement

Article 18
Scope of procedural provisions[2]

1. Each Party shall adopt such legislative and other measures as are necessary to establish the powers and procedures envisaged in this chapter for the purposes of preventing, detecting, disrupting, investigating, prosecuting and adjudicating cybercrimes.

2. Except as otherwise provided, 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 chapter II of the Convention;

(b) Other criminal offences committed by means of information and communications technologies;

(c) The collection of evidence in electronic form relating to the commission of criminal offences.

Article 19
Conditions and safeguards[3]

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 International Covenant on Civil and Political Rights, and other applicable international human rights instruments, and which shall incorporate the principle of proportionality.

2. Such conditions and safeguards shall, as appropriate in view of the nature of the procedure or power concerned, inter alia, include judicial or other independent supervision, grounds justifying application, and limitation of the scope and the duration of such power or procedure.

3. To the extent that it is consistent with the public interest, in particular the sound administration of justice, each Party shall consider the impact of the powers and procedures in this section upon the rights, responsibilities and legitimate interests of third parties.

Article 20
Expedited preservation of stored computer data[4]

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 have been stored by means of a computer system, in particular where there are grounds to believe that the computer data are 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

[2] *Source*: proposal by China and the Russian Federation, with changes made by Brazil.
[3] *Sources*: Budapest Convention and proposal by China and the Russian Federation.
[4] *Source*: Budapest Convention.

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 90 days, to enable the competent authorities to seek their 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 18 and 19.

Article 21
Expedited preservation of accumulated electronic information[5]

1. Each Party shall adopt such legislative and other measures as may be necessary to enable its competent authorities to give adequate orders or instructions or similarly ensure the expeditious preservation of specified electronic information, including traffic data, in particular where there are grounds to believe that the data are particularly vulnerable to deletion, copying or modification, including due to expiry of the retention period provided for by its domestic legislation or by the provider's terms of service.

2. If a Party gives effect to the provisions of paragraph 1 of this article by means of an order to persons (including legal persons) to preserve specified stored information in the person's possession or control, the Party shall adopt such legislative and other legal measures as may be necessary to oblige that person to preserve such information and maintain its integrity for such period of time as is necessary, but no longer than the period determined by the domestic legislation of that Party, to enable the competent authorities to seek disclosure of the data. 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 person who is tasked with preserving the information to keep confidential the undertaking of such procedures for the period of time provided for by its domestic legislation.

4. The powers and procedures referred to in this article shall be established in accordance with the provisions of articles 18 and 19 of this Convention.

Article 22
Expedited preservation and partial disclosure of traffic data[6]

Each Party shall adopt, in respect of traffic data that are to be preserved, 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.

The powers and procedures referred to in this article shall be subject to articles 18 and 19.

[5] *Source*: proposal by China and the Russian Federation.
[6] *Sources*: Budapest Convention and proposal by China and the Russian Federation.

Article 23
Production order[7]

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 are 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 data 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 18 and 19.

Article 24
Search and seizure of information stored or processed electronically[8]

1. Each Party shall adopt such legislative and other measures as may be needed to empower its competent authorities to seek access in the territory or under the jurisdiction of that State party to:

(a) Information and communications technology devices and information stored therein; and

(b) Information storage media in which the electronic information sought may be stored.

2. Each Party shall adopt such legislative and other measures as may be necessary to ensure that where its competent authorities, conducting a search pursuant to the provisions of paragraph 1 (a) of this article, have grounds to believe that the information sought is stored on another information and communications technology device in the territory of that Party, such authorities shall be able to expeditiously conduct the search to obtain access to that other information and communications technology device or the data contained therein.

3. Each Party shall adopt such legislative and other measures as may be necessary to empower its competent authorities to seize electronic information in its territory or under its own jurisdiction, or similarly secure such information. These measures shall include the provision of the following powers:

(a) To seize an information and communications technology device used to store information or to secure it in another way;

(b) To make and retain copies of such information in electronic and digital form;

(c) To maintain the integrity of the relevant stored information;

(d) To remove information stored or processed electronically.

4. Each Party shall adopt such legislative and other measures as may be necessary to empower its competent authorities to order, under the procedure established by its domestic legislation, any person who has special knowledge about the functioning of the information system in question, information and telecommunications network, or their component parts, or measures applied to protect the information therein, to provide the necessary information and/or assistance in undertaking measures referred to in paragraphs 1 to 3 of this article.

[7] *Sources*: Budapest Convention and proposal by China and the Russian Federation, with changes made by Brazil.

[8] *Source*: proposal by China and the Russian Federation. Provision similar to article 19 of the Budapest Convention, with changes by China and the Russian Federation.

5. The powers and procedures referred to in this article shall be established in accordance with the provisions of articles 18 and 19 of the Convention.

Article 25
Real-time collection of traffic data[9]

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 cooperate with 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 18 and 19.

Article 26
Interception of content data[10]

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 cooperate with 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.

[9] *Source*: Budapest Convention.
[10] *Source*: Budapest Convention.

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 18 and 19.

Article 27
Jurisdiction[11]

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

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 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. If a State party exercising its jurisdiction under paragraph 1 or 2 of this article has been notified or has otherwise learned that any other States parties are investigating, prosecuting or conducting a judicial proceeding with respect to the same act, the competent authorities of those States parties shall, as appropriate, consult each other with a view to coordinating their actions.[12]

Canada

[Original: English]
[9 April 2022]

Procedural powers

Scope of procedural powers

1. Clarify that powers and procedures provided for in this section are for the purpose of specific criminal investigations or proceedings.

2. Except as specifically provided otherwise, a State Party shall apply the powers and procedures referred to in paragraph 1 to:

(a) The criminal offences established in accordance with 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.

[11] *Source*: Budapest Convention, with changes made by Brazil.
[12] *Source*: proposal by China and the Russian Federation.

Expedited preservation of stored computer data

1. Each State Party shall adopt the necessary legislative and other measures to enable its domestic competent authorities to order or similarly obtain the expeditious preservation of specified computer data, including traffic data, that have been stored by means of a computer system, in particular where there are grounds to believe that the computer data are particularly vulnerable to loss or modification.

2. If a State Party gives effect to paragraph 1 by means of an order to a person to preserve specified stored computer data in that person's possession or control, the State Party shall adopt the necessary legislative and other measures to oblige that person to preserve and maintain the integrity of that data for a period of time as long as necessary, up to a maximum of 90 days, to enable the competent authorities to seek their disclosure. A State Party may provide for such an order to be subsequently renewed.

3. Each State Party shall adopt the necessary legislative and other measures to oblige, where justified and authorized, 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.

Expedited preservation and partial disclosure of traffic data

In respect of traffic data that are to be preserved under the previous article:

(a) Ensure that the 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 State Party's competent authority, or a person designated by that authority, of a sufficient amount of traffic data to enable the State Party to identify the service providers and the path through which the communication was transmitted.

Production order

Each State Party shall adopt the necessary measures to empower its domestic competent authorities to order a person in its territory to submit specified computer data in that person's possession or control, which are stored in a computer system or a computer-data storage medium.

Search and seizure of stored computer data

1. Each State Party shall adopt the necessary measures to empower its domestic 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 State Party shall adopt the necessary measures to enable its domestic competent authorities to expeditiously extend the search or similar accessing to the other system where they have grounds to believe that the data sought are stored in another computer system or part of it in its territory, and such data are lawfully accessible from or available to the initial system, the authorities shall be able to expeditiously extend the search or similar accessing to the system.

3. Each State Party shall adopt the necessary measures to empower its domestic competent authorities to seize or similarly secure computer data accessed according to paragraphs 1 or 2. These measures 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; and

(d) Render inaccessible or remove those computer data in the accessed computer system.

4. Each State Party shall adopt the necessary measures to empower its domestic competent authorities to order any person who has knowledge about the functioning of the computer system or measures applied to protect the computer data to provide, as is reasonable, the necessary information to enable the undertaking of the measures referred to in paragraphs 1 and 2.

Jurisdiction

1. Each State Party shall adopt the necessary measures to establish its jurisdiction over the offences established in this convention when:

(a) The offence is committed in the territory of that State Party;

(b) The offence is committed on board a vessel that is flying the flag of that State Party or an aircraft that is registered under the domestic law of that State Party at the time that the offence is committed; or

(c) The offence is committed by a national of that State Party or a stateless person who has his or her habitual residence in its territory.

2. Enable a State Party to establish its jurisdiction over the offences established in accordance with this convention when the alleged offender is present in its territory and it does not extradite such person solely on the ground that he or she is one of its nationals.

3. Enable a State Party to establish its jurisdiction over the offences established in accordance with this convention when the alleged offender is present in its territory and it does not extradite him or her.

4. If a State Party exercising its jurisdiction under paragraph 1 or 2 has been notified, or has otherwise learned, that any other State Party is conducting an investigation, prosecution, or judicial proceeding in respect of the same conduct, the competent authorities of those State Parties shall, as appropriate, consult one another with a view to coordinating their actions.

5. Without prejudice to norms of general international law, this convention does not exclude the exercise of any criminal jurisdiction established by a State Party in accordance with its domestic law.

Colombia

[Original: Spanish]
[8 April 2022]

Procedural measures and law enforcement

Taking into account the provisions by which Colombia is bound with respect to the powers and procedures established in the United Nations Convention against Transnational Organized Crime, the United Nations against Corruption and the Budapest Convention on Cybercrime, the following are proposed in relation to procedural measures and law enforcement:

Measures	*Provision of existing international instrument*
Powers and procedures	Article 14 of the Budapest Convention
Conditions and safeguards	Article 15 of the Budapest Convention
Expedited preservation of stored computer data	Article 16 of the Budapest Convention

Measures	*Provision of existing international instrument*
Expedited preservation and partial disclosure of traffic data	Article 17 of the Budapest Convention
Production order	Article 18 of the Budapest Convention
Search and seizure of stored computer data	Article 19 of the Budapest Convention
Real-time collection of traffic data	Article 20 of the Budapest Convention
Interception of content data	Article 21 of the Budapest Convention
Jurisdiction	Article 22 of the Budapest Convention, article 15 of the Organized Crime Convention and article 42 of the Convention against Corruption
Freezing, seizure and confiscation	Article 31 of the Convention against Corruption

Egypt

[Original: Arabic]
[8 April 2022]

Chapter III. Criminal proceedings and law enforcement

It is proposed that this chapter include the following three main articles:

Article 31. Scope of procedural issues

1. Each State party shall adopt such legislative measures as are necessary to establish powers and procedures for the purposes of preventing, identifying, detecting and investigating offences and other illegal acts and conducting judicial proceedings relating thereto.

2. Each State party shall apply the aforementioned powers and procedures to:

(a) The criminal offences and other illegal acts set forth in this Convention;

(b) Other criminal offences and other illegal acts committed by means of information and communications technologies;

(c) The collection of electronic evidence.

Article 32. Criminal procedures

Criminal procedures shall include:

1. The expeditious preservation of data stored in information and communications technologies, including user tracking information that has been stored on information technology, particularly if it is believed that such information is subject to loss or modification, by issuing an order obliging the person concerned to preserve the integrity of such data in his or her possession or control to enable the competent authorities to search and investigate, while maintaining the confidentiality of any actions taken in this regard.

2. The expeditious preservation and partial disclosure of user tracking information regardless of how many service providers were involved in the transmission of such information, and assurance of the expeditious disclosure by the competent authorities of a fair amount of traffic data to enable the State party to identify the service providers and the transmission path of the communication.

3. Orders to provide information in the possession of a person in the territory of a State party and stored on an information technology or storage medium, or in the possession or control of a service provider that provides services in the territory of the State party.

4. Inspection of stored information or access to information stored on an information technology or storage medium.

5. Seizure, copying and retention of stored information in order to conduct procedures for searching and accessing it.

6. Real-time collection of user tracking information and the obliging of service providers within the jurisdiction of the State party to collect, record and maintain the confidentiality of such information.

7. Interception of content information by enabling the competent authorities to collect and record, in real time through technical means, the information transmitted by information and communications technologies.

8. Each State party shall take the necessary legislative and other measures to enable its competent authorities to stop the transmission and broadcast of any content that constitutes an offence set forth in this Convention.

Article 33. Admission of digital evidence

Digital evidence derived or extracted from devices, equipment, electronic media, information systems, computer programs or any information and communications technology shall have the probative value of material forensic evidence in criminal evidence when such digital evidence meets the technical conditions under the laws of the States parties.

El Salvador

[Original: Spanish
[12 April 2022]

Procedural measures and law enforcement

Scope of procedural measures

Each State 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.

Except as specifically provided otherwise, each State Party shall apply the powers and procedures referred to in the preceding paragraph of this article to:

(a) Offences established in accordance with the articles of this Convention;

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

(c) The collection of evidence in electronic form of a criminal offence.

Conditions and safeguards

Each State Party shall ensure that the establishment, implementation and application of the powers and procedures provided for in this section are subject to the conditions and safeguards provided for under its domestic law, which shall provide for the adequate protection of human rights and freedoms.

Such conditions and safeguards shall include, as appropriate in view of the nature of the procedure or power concerned, inter alia, judicial or independent supervision, the grounds justifying application, and limitation of the scope and duration of such power or procedure.

To the extent that it is consistent with the public interest, in particular the sound administration of justice, each State Party shall consider the impact of the powers and procedures provided for in this section on the rights, responsibilities and legitimate interests of third parties.

Powers to request information on offences

Each State Party shall adopt such legislative and other measures as may be necessary to empower its competent authorities to order or otherwise compel a natural or legal person in its territory to submit specified computer data in that person's possession or control that are stored in a computer system or on a computer data storage medium.

Preservation of data stored in computer systems

Each State 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 have been stored by means of a computer system, in particular where there are grounds to believe that the computer data are particularly vulnerable to loss or modification.

Where a State Party gives effect to the preceding paragraph by means of an order to a person to preserve specific stored computer data in the person's possession or control, the State Party shall adopt such legislative and other measures as may be necessary to oblige that person to preserve and maintain the integrity of those computer data for a period of time as long as necessary, up to a maximum of 90 days, to enable the competent authorities to seek their disclosure. The State Party may provide for such an order to be subsequently renewed.

Each State 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.

Search and seizure of data stored in computer systems

Each State 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.

Each State 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 are stored in another computer system or part of it in its territory, and such data are lawfully accessible from or available to the initial system, the authorities shall be able to expeditiously extend the search or similar access to the other system.

Each State 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 the preceding paragraphs. 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.

Each State 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 adoption of the measures referred to in the preceding paragraphs.

Real-time collection of traffic data

Each State 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 in the territory of that State Party; and

(b) Compel a service provider, within its existing technical capability, to: collect or record through the application of technical means in the territory of that State Party; or cooperate with and assist the competent authorities in the collection or recording of traffic data, in real time, associated with specific communications in its territory, transmitted by means of a computer system.

Where a State 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 in that territory.

Each State 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.

Interception of content data

Each State 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 in the territory of that State Party; and

(b) Compel a service provider, within its existing technical capability, to: collect or record through the application of technical means in the territory of that State Party; or cooperate with and assist the competent authorities in the collection or recording of content data, in real time, associated with specific communications in its territory transmitted by means of a computer system.

Where a State 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 in that territory.

Each State 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.

Confiscation and freezing

States Parties shall adopt, to the greatest extent possible within their domestic legal systems, such measures as may be necessary to enable confiscation of:

(a) Proceeds of crime derived from offences covered by this Convention or property the value of which corresponds to that of such proceeds;

(b) Property, equipment or other instrumentalities used in or destined for use in offences covered by this Convention.

States Parties shall adopt such measures as may be necessary to enable the identification, tracing, freezing or seizure of any of the items referred to in the preceding paragraph for the purpose of eventual confiscation.

If proceeds of crime have been transformed or converted, in full or in part, into other property, such property shall be liable to the measures referred to in this article instead of the proceeds.

If proceeds of crime have been intermingled with property acquired from legitimate sources, such property shall, without prejudice to any powers relating to freezing or seizure, be liable to confiscation up to the assessed value of the intermingled proceeds.

Income or other benefits derived from proceeds of crime, from property into which proceeds of crime have been transformed or converted or from property with which proceeds of crime have been intermingled shall also be liable to the measures referred to in this article, in the same way and to the same extent as proceeds of crime.

Each State Party shall empower its courts or other competent authorities to order that bank, financial or commercial records be made available or be seized. States Parties shall not decline to act under the provisions of this paragraph on the ground of bank secrecy.

States Parties may consider the possibility of requiring that an offender demonstrate the lawful origin of alleged proceeds of crime or other property liable to confiscation, to the extent that such a requirement is consistent with the principles of their domestic law and with the nature of the judicial and other proceedings.

The provisions of this article shall not be construed as prejudicing the rights of bona fide third parties.

Nothing contained in this article shall affect the principle that the measures to which it refers shall be defined and implemented in accordance with and subject to the provisions of the domestic law of a State Party.

Disposal of confiscated proceeds of crime or property

Proceeds of crime or property confiscated by a State Party pursuant to this Convention shall be disposed of by that State Party in accordance with its domestic laws and administrative procedures.

When acting on the request made by another State Party in accordance with this Convention, States Parties shall, to the extent permitted by domestic law and if so requested, give priority consideration to returning the confiscated proceeds of crime or property to the requesting State Party so that it can give compensation to the victims of the crime or return such proceeds of crime or property to their legitimate owners.

When acting upon a request made by another State Party in accordance with the provisions of this Convention, a State Party may give special consideration to concluding agreements or arrangements on:

(a) Contributing the value of the proceeds of crime or property or funds derived from the sale of such proceeds of crime or property or a part thereof to the account designated in accordance with the provisions of this Convention or as determined by intergovernmental bodies specializing in the fight against organized crime;

(b) Sharing with other States Parties, on a regular or case-by-case basis, such proceeds of crime or property, or funds derived from the sale of such proceeds of crime or property, in accordance with its domestic law or administrative procedures.

Establishment of criminal record

Each State Party may adopt such legislative or other measures as may be necessary to take into consideration, under such terms as and for the purpose that it deems appropriate, any previous conviction in another State of an alleged offender

for the purpose of using such information in criminal proceedings relating to an offence covered by this Convention.

Protection of witnesses

Each State Party shall take appropriate measures within its means to provide effective protection from potential retaliation or intimidation for witnesses in criminal proceedings who give testimony concerning offences covered by this Convention and, as appropriate, for their relatives and other persons close to them.

The measures envisaged in the preceding paragraph of this article may include, inter alia, without prejudice to the rights of the defendant, including the right to due process:

(a) Establishing procedures for the physical protection of such persons, such as, to the extent necessary and feasible, relocating them and permitting, where appropriate, non-disclosure or limitations on the disclosure of information concerning the identity and whereabouts of such persons;

(b) Providing evidentiary rules to permit witness testimony to be given in a manner that ensures the safety of the witness, such as permitting testimony to be given through the use of communications technology such as video links or other adequate means;

(c) States Parties shall consider entering into agreements or arrangements with other States for the relocation of persons referred to in the first paragraph of this article;

(d) The provisions of this article shall also apply to victims insofar as they are witnesses.

Assistance to and protection of victims

Each State Party shall take appropriate measures within its means to provide assistance and protection to victims of offences covered by this Convention, in particular in cases of threat of retaliation or intimidation.

Each State Party shall establish appropriate procedures to provide access to compensation and restitution for victims of offences covered by this Convention.

Each State Party shall, subject to its domestic law, enable views and concerns of victims to be presented and considered at appropriate stages of criminal proceedings against offenders in a manner not prejudicial to the rights of the defence.

Measures to improve cooperation with law enforcement authorities

Each State Party shall take appropriate measures to encourage persons who participate or who have participated in organized criminal groups:

(a) To supply information useful to competent authorities for investigative and evidentiary purposes on such matters as:

(i) The identity, nature, composition, structure, location or activities of criminal groups and organizations;

(ii) Links, including international links, with other organized criminal groups;

(iii) Offences that organized criminal groups have committed or may commit;

(b) To provide factual, concrete help to competent authorities that may contribute to depriving organized criminal groups of their resources or of the proceeds of crime.

Each State Party shall consider providing for the possibility, in appropriate cases, of mitigating punishment of an accused person who provides substantial cooperation in the investigation or prosecution of an offence covered by this Convention.

Each State Party shall consider providing for the possibility, in accordance with fundamental principles of its domestic law, of granting immunity from prosecution to a person who provides substantial cooperation in the investigation or prosecution of an offence covered by this Convention.

Protection of such persons shall be as provided for in the corresponding article of this Convention.

Where a person referred to in the first paragraph of this article located in one State Party can provide substantial cooperation to the competent authorities of another State Party, the States Parties concerned may consider entering into agreements or arrangements, in accordance with their domestic law, concerning the potential provision by the other State Party of the treatment set forth in paragraphs 2 and 3 of this article.

European Union and its member States

[Original: English]
[6 April 2022]

Chapter III
Criminal procedures and law enforcement

Article 13
Scope of procedural measures

1. Each State Party shall adopt such legislative and other measures as may be necessary to establish the powers and procedures provided for in this chapter for the purpose of specific criminal investigations or proceedings.

2. Each State 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 5 through 10 of this Convention; and

(b) The collection of evidence in electronic form of a criminal offence established in accordance with articles 5 through 10 of this Convention.

Article 14
Conditions and safeguards

1. Each State Party shall ensure that the establishment, implementation and application of the powers and procedures provided for in this chapter are subject to conditions and safeguards provided for under its domestic law, which shall provide for the adequate and full protection of human rights and fundamental freedoms, in line with international human rights standards including rights arising pursuant to obligations it has undertaken under the Universal Declaration of Human Rights, the International Covenant on Civil and Political Rights, the Convention against Torture and Other Cruel, Inhuman or Degrading Treatment or Punishment, the Convention on the Rights of the Child, the Optional Protocol to the Convention on the Rights of the Child on the sale of children, child prostitution and child pornography and other international human rights instruments, and which shall incorporate the principles of proportionality, legality and necessity and the protection of privacy and personal data.

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 State Party shall consider the impact of the powers and procedures in this chapter upon the rights, responsibilities and legitimate interests of third parties.

Article 15
Expedited preservation of stored computer data

1. Each State Party shall adopt 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 have been stored by means of a computer system, in particular where there are grounds to believe that the computer data are particularly vulnerable to loss or modification.

2. Where a State 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 90 days, to enable the competent authorities to seek their disclosure. A Party may provide for such an order to be subsequently renewed.

3. Each State 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 16
Production order

1. Each State Party shall adopt 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 are 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.

Article 17
Search and seizure of stored computer data

1. Each State Party shall adopt 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 State Party shall adopt 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 are stored in another computer system or part of it in its territory, and such data are 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 State 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 State 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.

Article 18
Jurisdiction

1. Each State Party shall adopt such measures as may be necessary to establish jurisdiction over the offence established in accordance with articles 5 to 10 of this Convention when:

(a) The offence is committed in the territory of that State Party;

(b) The offence is committed on board a vessel that is flying the flag of that State Party or an aircraft registered under the laws of that State Party at the time to offence is committed; or

(c) The offence is committed 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 State Party may also establish its jurisdiction over any such offence when:

(a) The offence is committed against a national of that State Party;

(b) The offence is committed by a national of that State Party or a stateless person who has his or her habitual residence in its territory.

3. Each State Party may also adopt such measures as may be necessary to establish its jurisdiction over the offences covered by this Convention when the alleged offender is present in its territory and it does not extradite him or her, solely on the basis of his or her nationality, after a request for extradition.

4. If a State Party exercising its jurisdiction under paragraph 1 or 2 of this article has been notified, or has otherwise learned, that one or more other States Parties are conducting an investigation, prosecution or judicial proceeding in respect of the same conduct, the competent authorities of those States Parties shall, as appropriate, consult one another with a view to coordinating their actions.

5. Without prejudice to norms of general international law, this Convention does not exclude the exercise of any criminal jurisdiction established by a State Party in accordance with its domestic law.

Article 19
Assistance to and protection of victims

1. Each State Party shall take appropriate measures within its means to provide assistance and protection to victims of offences established in accordance with articles 5 to 10 of this Convention.

2. Each State Party shall establish appropriate procedures to provide access to compensation for victims of offences established in accordance with articles 5 to 10 of this Convention.

3. Each State Party shall, subject to its domestic law, enable views and concerns of victims to be presented and considered at appropriate stages of criminal proceedings against offenders in a manner not prejudicial to the rights of the defence.

Ghana

[Original: English]
[12 April 2022]

Chapter III
Procedural measures and law enforcement[13]

Article 23. 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, 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 5 through 20 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. Each Party may reserve the right to apply the measures referred to in article 29 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 30. Each Party shall consider restricting such a reservation to enable the broadest application of the measure referred to in article 29.

4. 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 29 and 30 to communications being transmitted within a computer system of a service provider, which system:

(a) Is being operated for the benefit of a closed group of users; and

(b) 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 29 and 30.

5. 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 Article 31, that Party may reserve the right not to apply these measures. Each Party shall consider restricting such a reservation to enable the broadest application of the measures referred to in article 31.

[13] The text for this section is taken primarily from the Budapest Convention, the African Union Convention on Cyber Security and Protection of Personal Data, the Electronic Transactions Act, 2008 (Act 772) and the Cybersecurity Act, 2020 (Act 1038). These instruments form the cybercrime legislative framework of Ghana.

Article 24. 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 International Bill of Human Rights, [14] including the Universal Declaration on Human Rights and the International Covenant on Civil and Political Rights, and other applicable international human rights instruments, and which shall incorporate the principle of proportionality and necessity and ensuring judicial oversight.

2. Such conditions and safeguards shall, as appropriate in view of the nature of the procedure or power concerned, inter alia, include judicial or other independent supervision, grounds justifying application, and limitation of the scope and the duration of such power or procedure.

3. To the extent that it is consistent with the public interest, in particular the sound administration of justice, each Party shall consider the impact of the powers and procedures in this section upon the rights, responsibilities and legitimate interests of third parties.

Article 25. Expedited preservation of stored computer data[15]

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 have been stored by means of a computer system, in particular where there are grounds to believe that the computer data are 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 90 days, to enable the competent authorities to seek their 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 19 and 20.

Article 26. Expedited preservation and partial disclosure of traffic data[16]

1. Each Party shall adopt, in respect of traffic data that are to be preserved under article 21, 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

[14] Office of the United Nations High Commissioner for Human Rights, "International human rights law" (www.ohchr.org/en/instruments-and-mechanisms/international-human-rights-law).

[15] Consistent with the Budapest Convention, the African Union Convention on Cyber Security and Protection of Personal Data and the Electronic Transactions Act, 2008 (Act 772) and Cybersecurity Act, 2020 (Act 1038) of Ghana.

[16] Consistent with the Budapest Convention.

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 23 and 24.

Article 27. 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 are 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. Each Party shall adopt such legislative and other measures as may be necessary to ensure that the production order for the computer data or subscriber information shall only be obtained by a relevant competent authority under the supervision of an independent supervisory entity such as a judicial authority. Such measures shall ensure that it is a requirement for the competent authority to demonstrate to the satisfaction of the independent supervisory authority that there are reasonable grounds to believe that the computer data or subscriber information related to a person under investigation are reasonably required for the purposes of a specific criminal investigations.

3. For the purpose of paragraph 2, the competent authority shall:

(a) Explain to the independent supervisory authority why the competent authority believes that the computer data or subscriber information sought will be available to:

(i) The person in control or possession of the computer data or computer system; or

(ii) A relevant service provider;

(b) Identify and explain with specificity the type of computer data or subscriber information being sought;

(c) Indicate what measures shall be taken to ensure that the subscriber information or computer data will be procured;

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

(ii) Without the disclosure of the subscriber information or computer data of any party not part of the investigation.

4. Each Party shall adopt such legislative and other measures as may be necessary to ensure that the independent supervisory authority may grant a production order under paragraph 2 if it is satisfied that:

(a) The information requested is commensurate, proportionate and necessary for the purposes of a specific criminal investigation or prosecution;

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

(c) The investigation may be frustrated or seriously prejudiced unless the production of the information is permitted.

5. The powers and procedures referred to in this article shall be subject to articles 23 and 24.

6. 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 geographical 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 communications equipment, available on the basis of the service agreement or arrangement.

Article 28. 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 are stored in another computer system or part of it in its territory, and such data are 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. Each Party shall adopt such legislative and other measures as may be necessary to empower its competent authorities to be accompanied by an authorized person and is entitled, with the assistance of that person, to enable the undertaking of the measures referred to in paragraphs 1, 2 and 3.

6. Each Party shall adopt such legislative and other measures as may be necessary to empower its competent authorities to seize any computer, electronic record, program, information, document or thing in executing a warrant under its domestic laws if the competent authority has reasonable grounds to believe that any of the offences established in accordance with articles 1 through 16 of this Convention has been or is about to be committed.

7. The powers and procedures referred to in this article shall be subject to articles 23 and 24.

Article 29. 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 cooperate with 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. Each Party shall adopt such legislative and other measures as may be necessary to ensure that the power under this article shall only be obtained by a relevant competent authority under the supervision of an independent supervisory entity such as a judicial authority. Such measures shall ensure that it is a requirement for the competent authority to demonstrate to the satisfaction of the independent supervisory authority that there are reasonable grounds to believe that the traffic data related to a person under investigation are reasonably required for the purposes of a specific criminal investigation.

3. For the purpose of paragraph 2, the competent authority shall:

(a) Explain to the independent supervisory authority why the competent authority believes that traffic data sought will be available to:

(i) The person in control or possession of the computer system; or

(ii) A service provider;

(b) Identify and explain with specificity the type of traffic data being sought;

(c) Identify and explain with specificity the offences in respect of which the power under this article is sought;

(d) Indicate what measures shall be taken to ensure that traffic data will be procured:

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

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

4. Each Party shall adopt such legislative and other measures as may be necessary to ensure that the independent supervisory authority may grant the power of real-time collection of traffic data if the independent supervisory authority is satisfied that:

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

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

(c) The investigation may be frustrated or seriously prejudiced unless the power for real-time collection of traffic data is permitted.

5. 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.

6. 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.

7. The powers and procedures referred to in this article shall be subject to articles 23 and 24.

Article 30. 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 cooperate with 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. Each Party shall adopt such legislative and other measures as may be necessary to ensure that the power under this article shall only be obtained by a relevant competent authority under the supervision of an independent supervisory entity such as a judicial authority. Such measures shall ensure that it is a requirement for the competent authority to demonstrate to the satisfaction of the independent supervisory authority that there are reasonable grounds to authorize the interception of content data related to or connected with person or premises under criminal investigations for one of the following purposes:

(a) The interests of national security;

(b) The prevention or detection of a serious offence;

(c) In the interests of the economic well-being of the citizenry, so far as those interests are also relevant to the interests of national security; or

(d) To give effect to a mutual legal assistance request.

3. For the purpose of paragraph 2, the competent authority shall:

(a) Explain to the independent supervisory authority why the competent authority believes that the content sought will be available to:

(i) The person in control or possession of the computer system;

(ii) A service provider;

(b) Identify and explain the type of content data suspected to be found on the computer system or in the possession or control of the service provider;

(c) Identify and explain with specificity the offences in respect of which the power under this article is sought;

(d) Indicate what measures shall be taken to ensure that the content data will be procured:

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

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

4. Each Party shall adopt such legislative and other measures as may be necessary to ensure that the independent supervisory authority may grant the power of interception of content data if the independent supervisory authority is satisfied that:

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

(b) Measures shall be taken to ensure that the power of interception of the content data is executed while maintaining the privacy of other users, customers and third parties and without the disclosure of information and data of any party not part of the investigation; and

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

5. 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.

6. 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.

7. The powers and procedures referred to in this article shall be subject to articles 23 and 24.

Article 31. Retention of data

1. Each Party shall adopt such legislative and other measures as may be necessary to ensure that a service provider within its territory shall retain:

(a) Subscriber information for at least six years;

(b) Traffic data for a period of 12 months.

2. The powers and procedures referred to in this article shall be subject to articles 23 and 24.

3. 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 under this article, that Party may reserve the right not to apply these measures. Each Party shall consider restricting such a reservation to enable the broadest application of the measures referred to under this article.

Article 32. Confiscation and seizure

1. Each Party shall adopt, to the greatest extent possible within its domestic legal system, such measures as may be necessary to enable confiscation of:

(a) Proceeds of crime derived from offences covered by this Convention or property the value of which corresponds to that of such proceeds;

(b) Property, equipment or other instrumentalities used in or destined for use in offences covered by this Convention.

2. Each Party shall adopt such measures as may be necessary to enable the identification, tracing, freezing or seizure of any item referred to in paragraph 3 of this article for the purpose of eventual confiscation.

3. If proceeds of crime have been transformed or converted, in part or in full, into other property, such property shall be liable to the measures referred to in this article instead of the proceeds.

4. If proceeds of crime have been intermingled with property acquired from legitimate sources, such property shall, without prejudice to any powers relating to

freezing or seizure, be liable to confiscation up to the assessed value of the intermingled proceeds.

5. Income or other benefits derived from proceeds of crime, from property into which proceeds of crime have been transformed or converted or from property with which proceeds of crime have been intermingled shall also be liable to the measures referred to in this article, in the same manner and to the same extent as proceeds of crime.

6. For the purposes of this article, each Party shall empower its courts or other competent authorities to order that bank, financial or commercial records be made available or be seized. Parties shall not decline to act under the provisions of this paragraph on the ground of bank secrecy.

7. Each Party may consider the possibility of requiring that an offender demonstrate the lawful origin of alleged proceeds of crime or other property liable to confiscation, to the extent that such a requirement is consistent with the principles of their domestic law and with the nature of the judicial and other proceedings.

8. The provisions of this article shall not be construed to prejudice the rights of bona fide third parties.

9. Nothing contained in this article shall affect the principle that the measures to which it refers shall be defined and implemented in accordance with and subject to the provisions of the domestic law of a Party.

Article 33. 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 5 through 20 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. For the purpose of the extradition article of this Convention, each Party shall adopt such measures as may be necessary to establish jurisdiction over the offences established in accordance with 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.

Iran (Islamic Republic of)

[Original: English]
[8 April 2022]

3. Law enforcement and procedural measures

Criminals perpetually and increasingly misuse services provided by the private sector, including service providers and social media networking platforms. This poses a daunting challenge that requires concrete responses. Given the fundamental and crucial importance of the cooperation of these entities with law enforcement entities in the investigation and prosecution of such offences and in suppressing such misuses, the convention should specify and stipulate obligations and regulations as to the cooperation of the private sector, service providers and other similar entities with law enforcement, in particular sectors and providers with global or substantial outreach at the international level.

Effective measures for timely and effective cooperation on the part of these entities with law enforcement and judicial authorities should constitute an integral part of the convention. For this purpose, through specific sections within the convention, cooperation between national authorities and entities such as service providers and the private sector should be addressed and concrete measures, including for the expeditious preservation and disclosure of electronic data to law enforcement entities, should be delineated.

As electronic evidence constitutes a vital element for the investigation and prosecution of crimes committed via the use of information and communications technology, setting standardized processes for the obtaining, maintenance and disclosure of authentic electronic evidence needs to be among the procedures to stipulated in the convention. Standard procedures enable unified and harmonized responses to such crimes at the national level that could also ensure more efficient cooperation among law enforcement and judicial authorities at the international level in relation to the preservation and provision of electronic evidence.

Recovery and return of assets and proceeds of crime play an important role in depriving criminals of incentives for the perpetration of crime and reducing recidivism, as well as in providing compensation to victims. Therefore, the expedited seizure, recovery and return of proceeds of crime should constitute a key element of the convention. Relevant provisions of the convention on law enforcement and procedural measures should entrust national authorities with powers that ensure the smooth and expedited recovery of assets and proceeds of crimes, as well as the widest measures of assistance and cooperation in this area.

The fight against use of information and communications technology for criminal purposes requires that law enforcement entities be equipped with and use modern technologies in the course of the investigation and prosecution of offences in order to respond proportionately to such crimes. Hence, promoting and supporting the use of modern technology by law enforcement and judicial authorities, including throughout procedural measures in preventing and combating crimes committed via information and communications technology should be encouraged. This also necessitates the provision of the required equipment and technology to law enforcement and judicial authorities through politically neutral and reliable technical assistance.

Japan

[Original: English]
[8 April 2022]

3. Procedural measures and law enforcement

3.1 Regarding procedural measures for cybercrime investigations, consideration could be given to providing for the expedited preservation, search and seizure of stored computer data, production orders, and real-time collection of traffic data.

3.2 We could consider applying these procedural provisions to investigations and criminal proceedings for the criminal offences established in this convention and other criminal offences committed by means of a computer system, and to the collection of evidence in electronic form of a criminal offence.

3.3 In granting the above-mentioned authority to competent authorities of each Member State, it is necessary to establish provisions confirming that each Member State should ensure that the rights arising in accordance with obligations under human rights treaties and others, as well as other human rights and freedoms, are appropriately protected and that domestic legislation that include the principle of proportionality are followed. This convention should confirm this concept in the chapter on procedural measures and law enforcement.

Mexico

[Original: English]
[13 April 2022]

Procedural measures and law enforcement

Given the importance of digital evidence for investigation, prosecution and law enforcement purposes, it is so expected that States parties to the Convention agree upon general and minimally homologated procedural measures for obtaining, handling and preserving digital evidence. The following could be added: “States can consider and make use of all provisions contained in existing international instruments, such as the United Nations Convention against Transnational Organized Crime for investigative purposes or/and evidence-gathering and preservation of electronic evidence.”

With respect to private entities that provide information and communications technology services, Mexico recommends that the following articles be included:

> “States Parties commit to making private entities that provide information and communications technology services, constituted in their respective territory or operating under their national jurisdiction, to adopt and implement due diligence policies and procedures to avoid damages to third parties.”
>
> “States Parties also commit to taking appropriate measures to ensure that private entities constituted in their respective territory or operating under their national jurisdiction do not violate the laws of other States Parties.”

It would be also relevant to include a general call to the responsibility of private entities that provide information and communications technology services to effectively collaborate with national law enforcement and judicial authorities with regard to investigations and prosecution of cybercrimes, while respecting applicable privacy regulations.

New Zealand

[Original: English]
[8 April 2022]

Provisions on procedural and law enforcement measures

10. Contingent on the inclusion of comprehensive safeguards to ensure the protection of human rights and fundamental freedoms, respect for the rule of law and adherence to the principle of proportionality, New Zealand supports including in this convention provisions that would enable the swift preservation of and access to digital evidence. For example, provisions relating to:

- Search and seizure of targeted and relevant stored computer data
- Real-time collection of targeted and relevant computer data
- Interception of targeted and relevant computer data
- Preservation of targeted and relevant computer data
- Production orders for specified computer data in a person's possession or control, which are stored in a computer system or a computer-data storage medium.

11. New Zealand would also support the inclusion of provisions that ensure that criminals do not profit from their crimes, such as the seizure and confiscation of proceeds of crime, and provisions that would enhance cooperation with law enforcement authorities.

Norway

[Original: English]
[8 April 2022]

Procedural measures and law enforcement

9. The Ad Hoc Committee should draw on experiences from existing treaties, such as the United Nations Convention against Transnational Organized Crime and the United Nations Convention against Corruption. At the same time, bearing in mind that the new convention will deal with the challenges of modern cybercrime, it should require Member States to include domestic provisions specifically aimed at electronic evidence. Furthermore, the Ad Hoc Committee should be mindful that time and efficiency are of the essence when investigating or prosecuting cybercrime. The convention should allow for cooperation to collect and obtain electronic evidence for any type of crime, not only cybercrime.

10. To avoid unnecessary duplication of efforts, it should make good use of and strengthen existing and well-functioning channels of communication and networks.

11. The key role of the private sector must be addressed.

12. Assistance to and protection of victims as well as protection of witnesses should addressed.

13. The provisions on procedural measures must be consistent with due process and the protection of human rights and fundamental freedoms.

Russian Federation, also on behalf of Belarus, Burundi, China, Nicaragua and Tajikistan

[Original: Russian]
[7 April 2022]

Section 2

Criminal proceedings and law enforcement

Article 31. Scope of procedural provisions

1. Each State party shall adopt such legislative and other measures as are necessary to establish the powers and procedures envisaged in this section for the purposes of preventing, detecting, suppressing, exposing and prosecuting offences and other illegal acts, and conducting judicial proceedings relating to such offences and acts.

2. Except as otherwise provided in article 33 of this Convention, each State party shall apply the powers and procedures referred to in paragraph 1 of this article to:

(a) The criminal offences and other illegal acts established in accordance with articles 6–29 of this Convention;

(b) Other criminal offences and other illegal acts committed by means of information and communications technology;

(c) The collection of evidence, including electronic evidence, relating to the commission of criminal offences and other illegal acts.

3. (a) Each State party may make a reservation to the effect that it retains the right to apply the measures referred to in article 38 of this Convention only to criminal offences or categories of criminal offences specified in the reservation, provided that the range of such criminal offences or categories of criminal offences is not more restricted than the range of criminal offences to which it applies the measures referred to in the provisions of article 33 of this Convention. Each State party shall consider restricting the application of such a reservation to enable the broadest application of the measures provided for under article 38 of this Convention;

(b) If a State party, owing to limitations in its domestic legislation in force at the time of the adoption of this Convention, is not able to apply the measures referred to in articles 33 and 38 of this Convention to the information being transmitted within an information system of a service provider, and that system:

(i) Is being operated for the benefit of a closed group of users; and

(ii) Does not employ an information and telecommunications network and is not connected with other information systems,

that State party may reserve the right not to apply those measures to such information transmission.

Article 32. Conditions and safeguards

1. Each State 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 legislation, which shall ensure the adequate protection of human rights and freedoms, including rights arising from the obligations that the State party has undertaken under the International Covenant on Civil and Political Rights of 16 December 1966 and other applicable international human rights instruments.

2. In view of the nature of the powers and procedures concerned, such conditions and safeguards shall include, inter alia, judicial or other independent supervision, grounds justifying application, and limitation of the scope and the duration of such powers or procedures.

3. To the extent that it is consistent with the public interest, in particular as regards the administration of justice, the State party shall consider the impact of the powers and procedures provided for in this section on the rights, responsibility and legitimate interests of third parties.

Article 33. Collection of information transmitted by means of information and communications technology

1. In order to counter the offences covered by this Convention and established as such under its domestic legislation, each State party shall adopt such legislative and other measures as are necessary to empower its competent authorities to:

(a) Collect or record, through the application of technical means, in the territory of that State party, information transmitted by means of information and communications technology; and

(b) Oblige a service provider, to the extent that it possesses the technical capacity to do so:

(i) To collect or record, through the application of technical means in the territory of that State party, electronic information that includes data on content and is transmitted by means of information and communications technology; or

(ii) To cooperate with and assist the competent authorities of that State party in real-time collection or recording of electronic information that includes data on content and is transmitted by means of information and communications technology in the territory of that State party.

2. Where a State party, owing to the long-established principles of its domestic legal system, cannot adopt the measures referred to in paragraph 1 (a) of this article, it may instead adopt such legislative and other measures as may be necessary to ensure the real-time collection or recording of electronic information that includes data on content and is transmitted by means of information and communications technology in its territory through the application of technical means in that territory.

3. Each State party shall adopt such legislative and other measures as may be necessary to oblige a service provider to keep confidential the exercise 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 the provisions of articles 31 and 32 of this Convention.

Article 34. Expedited preservation of accumulated electronic information

1. Each State party shall adopt such legislative and other measures as may be necessary to enable its competent authorities to give adequate orders or instructions or similarly ensure the expeditious preservation of specified electronic information, including traffic data, in particular where there are grounds to believe that the data are particularly vulnerable to deletion, copying or modification, including due to expiry of the retention period provided for by its domestic legislation or by the provider’s terms of service.

2. If a State party gives effect to the provisions of paragraph 1 of this article by means of an order to persons (including legal persons) to preserve specified stored information in the person’s possession or control, the State party shall adopt such legislative and other legal measures as may be necessary to oblige that person to preserve such information and maintain its integrity for such period of time as is necessary, but no longer than the period determined by the domestic legislation of that State party, to enable the competent authorities to seek disclosure of the data. A State party may provide for such an order to be subsequently renewed.

3. Each State party shall also adopt such legislative and other measures as may be necessary to oblige the person who is tasked with preserving the information to keep

confidential the undertaking of such procedures for the period of time provided for by its domestic legislation.

4. The powers and procedures referred to in this article shall be established in accordance with the provisions of articles 31 and 32 of this Convention.

Article 35. Expedited preservation and partial disclosure of traffic data

1. Each State party shall adopt, in respect of traffic data that are to be preserved under the provisions of article 34 of this Convention, such legislative and other measures as may be necessary to:

(a) Ensure that such expeditious preservation of traffic data is possible, regardless of how many service providers were involved in the transmission of such information; and

(b) Ensure the expeditious disclosure to the competent authorities of that State party of a sufficient amount of traffic data to enable the respective State party to identify the service providers and the path through which the indicated information was transmitted.

2. The powers and procedures referred to in this article shall be subject to the provisions of articles 31 and 32 of this Convention.

Article 36. Production order

1. For the purposes set out in article 31, paragraph 1, of this Convention, each State 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 provide specified electronic information in that person's possession or control;

(b) A service provider offering its services in the territory of that State party to submit subscriber information in that service provider's possession or control.

2. The powers and procedures referred to in this article shall be established in accordance with the provisions of articles 31 and 32 of this Convention.

3. For the purposes of this article, the term "subscriber information" shall mean any information held by a service provider relating to subscribers to its services other than traffic data or content data, on the basis of which it is possible to establish:

(a) The type of information and communications service used, the technical provisions taken thereto and the period of service;

(b) The subscriber's identity, postal or other addresses, telephone and other access numbers, including Internet Protocol addresses and billing and payment information, available in the service agreement or arrangement;

(c) Information relating to the location of information and telecommunications equipment that has a bearing on the service agreement or arrangement.

Article 37. Search and seizure of information stored or processed electronically

1. Each State party shall adopt such legislative and other measures as may be necessary to empower its competent authorities to seek access in the territory or under the jurisdiction of that State party to:

(a) ICT devices and information stored therein; and

(b) Information storage media in which the electronic information sought may be stored.

2. Each State party shall adopt such legislative and other measures as may be necessary to ensure that where its competent authorities, conducting a search pursuant

to the provisions of paragraph 1 (a) of this article, have grounds to believe that the information sought is stored on another information and communications technology device in the territory of that State party, such authorities shall be able to expeditiously conduct the search to obtain access to that other information and communications technology device or the data contained therein.

3. Each State party shall adopt such legislative and other measures as may be necessary to empower its competent authorities to seize electronic information in the territory or under the jurisdiction of the State party, or similarly secure such information. These measures shall include the provision of the following powers:

(a) To seize an information and communications technology device used to store information or to secure it in another way;

(b) To make and retain copies of such information in electronic and digital form;

(c) To maintain the integrity of the relevant stored information;

(d) To remove from the information and communications technology device information stored or processed electronically.

4. Each State party shall adopt such legislative and other measures as may be necessary to empower its competent authorities to order, under the procedure established by its domestic legislation, any person who has special knowledge about the functioning of the information system in question, information and telecommunications network, or their component parts, or measures applied to protect the information therein, to provide the necessary information and/or assistance in undertaking measures referred to in paragraphs 1–3 of this article.

5. The powers and procedures referred to in this article shall be established in accordance with the provisions of articles 31 and 32 of this Convention.

Article 38. Real-time collection of traffic data

1. Each State party shall adopt such legislative and other measures as may be necessary to empower its competent authorities to:

(a) Collect or record, employing technical means for this purpose, the traffic data associated with information and communications technology use in the territory of that State party; and

(b) Oblige service providers, to the extent that they possess the technical capacity to do so:

(i) To collect or record traffic data in the territory of that State party, employing technical means for this purpose; or

(ii) To cooperate with and assist the competent authorities of that State party in collecting or recording in real time the traffic data associated with specified information in the territory of that State party.

2. Where a State party, owing to the long-standing principles of its domestic legal system, cannot adopt the measures provided for in paragraph 1 (a) of this article, it may instead adopt such legislative and other measures as may be necessary to ensure the real-time collection or recording of the traffic data in its territory through the application of technical means in that territory.

3. Each State party shall adopt such legislative and other measures as may be necessary to oblige a service provider to keep confidential the exercise 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 the provisions of articles 31 and 32 of this Convention.

Article 39. Jurisdiction

1. Each State party shall take all measures necessary to establish jurisdiction over criminal offences and other illegal acts established as such under this Convention, when they are committed:

(a) In the territory of that State party; or

(b) On board a vessel flying the flag of that State party when the offence was committed, or on board an aircraft registered under the law of that State party at that time.

2. Subject to article 3 of this Convention, a State party may also establish its jurisdiction over any such offence and other illegal act when:

(a) The offence is committed against a national of that State party, a stateless person permanently residing in its territory, a legal person established or having a permanent representation in its territory, a State or government facility, including the premises of a diplomatic mission or consular office of that State party; or

(b) The offence is committed by a national of that State party or a stateless person whose habitual residence is in its territory; or

(c) The offence is committed against that State party; or

(d) The offence is committed wholly or partly outside the territory of that State party but its effects in the territory of that State party constitute an offence or result in the commission of an offence.

3. For the purposes of article 47 of this Convention, each State party shall take all measures necessary to establish its jurisdiction over the offences established as such under this Convention when the alleged offender is present in its territory and the State party does not extradite such person solely on the grounds that he or she is a national of that State party or a person to which it has granted refugee status.

4. Each State party in whose territory an alleged perpetrator is present and which does not extradite such person shall, in cases provided for in paragraphs 1 and 2 of this article, without any exception and regardless of whether the offence was committed in the territory of that State party, submit the case without further delay to its competent authorities for the purpose of legal prosecution in accordance with the law of that State.

5. If a State party exercising its jurisdiction under paragraph 1 or 2 of this article has been notified or has otherwise learned that any other States parties are investigating, prosecuting or conducting a judicial proceeding with respect to the same act, the competent authorities of those States parties shall, as appropriate, consult each other with a view to coordinating their actions.

6. Without prejudice to general international law, this Convention shall not exclude the exercise of any criminal or administrative jurisdiction established by a State party in accordance with its domestic law.

Chapter III. Measures to prevent and combat offences and other illegal acts in cyberspace

[…]

Article 45. Measures for protecting witnesses

Each State party shall consider adopting such legislative measures as may be necessary to provide effective protection for the following:

(a) Persons who, in good faith and on reasonable grounds, provide information relating to illegal acts covered by articles 6–28 of this Convention or otherwise cooperate with investigating or judicial authorities;

(b) Witnesses who give testimony concerning illegal acts covered by articles 6–28 of this Convention, as well as victims;

(c) Where appropriate, family members of the persons referred to in subparagraphs (a) and (b) of this article.

South Africa

[Original: English]
[14 April 2022]

Chapter III. Procedural measures and law enforcement

Article 18: Procedural provisions

1. Each State Party shall adopt such legislative and other measures as may be necessary to establish the powers and procedures provided for in this article for the purpose of specific criminal investigations or proceedings.

2. Except as specifically provided otherwise in article 32, each Party shall apply the powers and procedures referred to in paragraph 1 of this article to:

(a) The criminal offences involving the use of information and communications technologies established in accordance with articles […] through […] of this Convention;

(b) Other criminal offences committed by means of information and communications technologies; and

(c) The collection of evidence in electronic form of a criminal offence involving the use of information and communications technologies.

3. Each State Party may reserve the right to apply the measures referred to in article 31 only to offences or categories of offences involving the use of information and communications technologies 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 32. Each Party shall consider restricting such a reservation to enable the broadest application of the measures referred to in article 31.

4. Where a State Party, due to limitations in its legislation in force at the time of the adoption of this Convention, is not able to apply the measures referred to in articles 31 and 32 to communications being transmitted using information and communications technologies of a service provider, which system:

(a) Is being operated for the benefit of a closed group of users, and

(b) Does not employ public communications networks and is not connected with other information and communications technologies, 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 31 and 32.

Article 19: Conditions and safeguards

1. Each State Party shall ensure that the establishment, implementation and application of the powers and procedures provided for in this article 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 and fundamental freedoms arising pursuant to obligations it has undertaken under agreements, treaties and applicable international human rights instruments, and which shall incorporate the principle of proportionality consistent with the sovereignty of the Party.

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 State Party shall consider the impact of the powers and procedures in this article upon the rights, responsibilities and legitimate interests of third parties.

Article 20: Expedited preservation of stored computer data

1. Each State 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 have been stored by means of information and communications technologies, in particular where there are grounds to believe that the computer data are particularly vulnerable to loss or modification.

2. Where a State 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 seven days, to enable the competent authorities to seek their disclosure. A Party may provide for such an order to be subsequently renewed.

3. Each State 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 27 and 28.

Article 21: Search and seizure of stored computer data

1. Each State Party shall adopt such legislative and other measures as may be necessary to empower its competent authorities to search or similarly access:

(a) Information and communications technologies, 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 State Party shall adopt such legislative and other measures as may be necessary to ensure that where its authorities search or similarly access any information and communications technologies or components which form part of such technologies, a specific computer system or part of it, pursuant to paragraph 1 (a), and have grounds to believe that the data sought are stored in other information and communications technologies or components forming part of such technologies, computer system or part of it in its territory, and such data are 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 State Party shall adopt such legislative and other measures as may be necessary to empower its competent authorities, where applicable with the assistance or in the presence of the authorized officers of the foreign/other Party 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 information and communications technologies or components forming part of such technologies, 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 or information and communications technologies.

4. Each State 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 information and communications technologies or components forming part of such technologies, a 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 27 and 28.

Article 22: Real-time collection of traffic data

1. Each State 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 cooperate with 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 information and communications technologies or a computer system.

Article 23: Interception of content data

1. Each State 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 cooperate with 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 information and communications technologies a computer system.

2. Where a State 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 State 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 27 and 28.

Article 24: Freezing, seizure and confiscation

1. Notwithstanding the fact that the provisions of this article it shall not be so construed as to prejudice the rights of bona fide third parties and that nothing contained in this article shall affect the principle that the measures to which it refers shall be defined and implemented in accordance with and subject to the provisions of the domestic law of a State Party.

2. The provisions of this article shall not be so construed as to prejudice the rights of bona fide third parties.

3. Nothing contained in this article shall affect the principle that the measures to which it refers shall be defined and implemented in accordance with and subject to the provisions of the domestic law of a State Party.

4. Each State Party shall take, to the greatest extent possible within its domestic legal system, such measures as may be necessary to enable confiscation of:

(a) Proceeds of crime derived from offences caused by the use of information and communications technologies established in accordance with this Convention or property the value of which corresponds to that of such proceeds and to the benefit of the affected State Party;

(b) Property, equipment or other instrumentalities, including the use of information and communications technologies used in or destined for use in offences established in accordance with this Convention.

4. Each State Party shall take such measures as may be necessary to enable the identification, tracing, freezing or seizure of any item referred to in paragraph 1 of this article for the purpose of eventual confiscation.

5. Each State Party shall adopt, in accordance with its domestic law, such legislative and other measures as may be necessary to regulate the administration by the competent authorities of frozen, seized or confiscated property covered in paragraphs 1 and 2 of this article.

6. If such proceeds of crime have been transformed or converted, in part or in full, into other property, such property shall be liable to the measures referred to in this article instead of the proceeds.

7. If such proceeds of crime have been intermingled with property acquired from legitimate sources, such property shall, without prejudice to any powers relating to freezing or seizure, be liable to confiscation up to the assessed value of the intermingled proceeds.

8. Income or other benefits derived from such proceeds of crime, from property into which such proceeds of crime have been transformed or converted or from property with which such proceeds of crime have been intermingled shall also be liable to the measures referred to in this article, in the same manner and to the same extent as proceeds of crime.

9. For the purpose of this article and article […] [on international cooperation] of this Convention, each State Party shall empower its courts or other competent authorities to order that bank, financial or commercial records be made available or seized. A State Party shall not decline to act under the provisions of this paragraph on the ground of bank secrecy.

10. States Parties may consider the possibility of requiring that an offender demonstrate the lawful origin of such alleged proceeds of crime or other property liable to confiscation, to the extent that such a requirement is consistent with the fundamental principles of their domestic law and with the nature of judicial and other proceedings.

Article 25: Disposal of confiscated proceeds of crime or property

1. Proceeds of crime or property confiscated by a State Party pursuant to article 33, paragraph 3, of this Convention shall be disposed of by that State Party in accordance with its domestic law and administrative procedures.

2. When acting on the request made by another State Party in accordance with article 39 of this Convention, States Parties shall, to the extent permitted by domestic law and if so requested, give priority consideration to returning the confiscated proceeds of crime or property to the requesting State Party so that it can give compensation to the victims of the crime or return such proceeds of crime or property to their legitimate owners.

3. When acting on the request made by another State Party in accordance with article 41 of this Convention, a State Party may give special consideration to concluding agreements or arrangements on:

(a) Contributing the value of such proceeds of crime or property or funds derived from the sale of such proceeds of crime or property or a part thereof to the account designated in accordance with article […] of this Convention and to intergovernmental bodies specializing in the fight against organized crime;

(b) Sharing with other States Parties, on a regular or case-by-case basis, such proceeds of crime or property, or funds derived from the sale of such proceeds of crime or property, in accordance with its domestic law or administrative procedures.

Article 26: Criminal record

Each State Party may adopt such legislative or other measures as may be necessary to take into consideration, under such terms as and for the purpose that it deems appropriate, any previous conviction in another State of an alleged offender for the purpose of using such information in criminal proceedings relating to an offence caused by the use of information and communications technologies established in accordance with this Convention.

Article 27: Measures to enhance cooperation with law enforcement authorities

1. Each State Party shall take appropriate measures to encourage persons who participate or who have participated in organized criminal groups:

(a) To supply information useful to competent authorities for investigative and evidentiary purposes on such matters as:

(i) The identity, nature, composition, structure, location or activities of organized criminal groups;

(ii) Links, including international links, with other organized criminal groups;

(iii) Offences that organized criminal groups have committed or may commit;

(b) To provide factual, concrete help to competent authorities that may contribute to depriving organized criminal groups of their resources or of the proceeds of crime.

2. Each State Party shall consider providing for the possibility, in appropriate cases, of mitigating punishment of an accused person who, in good faith, provides substantial cooperation in the investigation or prosecution of an offence covered by this Convention.

3. Each State Party shall consider providing for the possibility, in accordance with fundamental principles of its domestic law, of granting immunity from prosecution to a person who provides, in good faith, substantial cooperation in the investigation or prosecution of an offence involving the use of information and communications technologies covered by this Convention.

4. Protection of such persons shall be as provided for in article 34 of this Convention.

5. Where a person referred to in paragraph 1 of this article located in one State Party can, in good faith, provide substantial cooperation to the competent authorities of another State Party, the States Parties concerned may consider entering into agreements or arrangements, in accordance with their domestic law, concerning the potential provision by the other State Party of the treatment set forth in paragraphs 2 and 3 of this article.

Article 28: Law enforcement cooperation

1. States Parties shall cooperate closely with one another, consistent with their respective domestic legal and administrative systems, to enhance the effectiveness of law enforcement action to combat the offences involving the use of information and

communications technologies covered by this Convention. Each State Party shall, in particular, adopt effective measures:

(a) To enhance and, where necessary, to establish channels of communication between their competent authorities, agencies and Internet service providers in order to facilitate the secure and rapid exchange of information concerning all aspects of the offences involving the use of information and communications technologies covered by this Convention, including, if the States Parties concerned deem it appropriate, links with other criminal activities;

(b) To cooperate with other States Parties in conducting inquiries with respect to offences involving the use of information and communications technologies covered by this Convention concerning:

(i) The identity, whereabouts and activities of persons suspected of involvement in such offences or the location of other persons concerned;

(ii) The movement of proceeds of crime or property derived from the commission of such offences;

(iii) The movement of property, equipment or other instrumentalities used or intended for use in the commission of such offences;

(c) To provide, when appropriate, necessary items or quantities of substances for analytical or investigative purposes;

(d) To facilitate effective coordination between their competent authorities, agencies and Internet service providers and to promote the exchange of personnel and other experts, including, subject to bilateral agreements or arrangements between the States Parties concerned;

(e) To exchange information with other States Parties on specific means and methods used by organized criminal groups, including, where applicable, routes and conveyances and the use of false identities, altered or false documents or other means of concealing their activities through the use of information and communications technologies;

(f) To exchange information and coordinate administrative and other measures taken as appropriate for the purpose of early identification of the offences involving the use of information and communications technologies covered by this Convention.

2. With a view to giving effect to this Convention, States Parties shall consider entering into bilateral or multilateral agreements or arrangements on direct cooperation between their law enforcement agencies and, where such agreements or arrangements already exist, amending them. In the absence of such agreements or arrangements between the States Parties concerned, the Parties may consider this Convention as the basis for mutual law enforcement cooperation in respect of the offences covered by this Convention. Whenever appropriate, States Parties shall make full use of agreements or arrangements, including international or regional organizations, to enhance the cooperation between their law enforcement agencies.

3. States Parties shall endeavour to cooperate within their means to respond to transnational organized crime committed through the use of information and communications technologies.

Article 29: Joint investigations

States Parties shall consider concluding bilateral or multilateral agreements or arrangements whereby, in relation to matters that are the subject of investigations, prosecutions or judicial proceedings in one or more States, the competent authorities concerned may establish joint investigative bodies. In the absence of such agreements or arrangements, joint investigations may be undertaken by agreement on a case-by-case basis. The States Parties involved shall ensure that the sovereignty of the State Party in whose territory such investigation is to take place is fully respected.

Article 30: Special investigative techniques

1. In order to combat or counter the use of information and communications technologies for criminal purposes effectively, each State Party shall, to the extent permitted by the basic principles of its domestic legal system and in accordance with the conditions prescribed by its domestic law, take such measures as may be necessary, within its means, to allow for special investigative techniques, such as electronic or other forms of surveillance and undercover operations, within its territory, and to allow for the admissibility in court of evidence derived therefrom, without compromising the cybersecurity threat and confidentiality of the intelligence of each State Party.

2. For the purpose of investigating the offences involving the use of information and communications technologies covered by this Convention, States Parties are encouraged to conclude, when necessary, appropriate bilateral or multilateral agreements or arrangements for using such special investigative techniques in the context of cooperation at the international level. Such agreements or arrangements shall be concluded and implemented in full compliance with the principle of sovereign equality of States and respect for fundamental human rights and freedoms and shall be carried out strictly in accordance with the terms of those agreements or arrangements.

3. In the absence of an agreement or arrangement as set forth in paragraph 2 of this article, decisions to use such special investigative techniques at the international level shall be made on a case-by-case basis and may, when necessary, take into consideration financial arrangements and understandings with respect to the exercise of jurisdiction by the States Parties concerned.

Article 31: Return and disposal of assets

1. Property confiscated by a State Party pursuant to article 33 or 34 of this Convention shall be disposed of, including by return to its prior legitimate owners, pursuant to paragraph 3 of this article, by that State Party in accordance with the provisions of this Convention and its domestic law.

2. Each State Party shall adopt such legislative and other measures, in accordance with the fundamental principles of its domestic law, as may be necessary to enable its competent authorities to return confiscated property, when acting on the request made by another State Party, in accordance with this Convention, taking into account the rights of bona fide third parties.

3. In accordance with paragraphs 1 and 2 of this article, the requested State Party shall:

(a) In the case of countering the use of information and communications technologies as referred to in this Convention, when confiscation was executed in accordance with article […] and on the basis of a final judgment in the requesting State Party, a requirement that can be waived by the requested State Party, return the confiscated property to the requesting State Party;

(b) In the case of proceeds of any other offence involving the use of information and communications technologies covered by this Convention, when the confiscation was executed in accordance with article […] of this Convention and on the basis of a final judgment in the requesting State Party, a requirement that can be waived by the requested State Party, return the confiscated property to the requesting State Party, when the requesting State Party reasonably establishes its prior ownership of such confiscated property to the requested State Party or when the requested State Party recognizes damage to the requesting State Party as a basis for returning the confiscated property;

(c) In all other cases, give priority consideration to returning confiscated property to the requesting State Party, returning such property to its prior legitimate owners or compensating the victims of the crime.

4. Where appropriate, unless States Parties decide otherwise, the requested State Party may deduct reasonable expenses incurred in investigations, prosecutions or

judicial proceedings leading to the return or disposition of confiscated property pursuant to this article.

5. Where appropriate, States Parties may, in accordance with the domestic legislation, also give special consideration to concluding agreements or mutually acceptable arrangements, on a case-by-case basis, for the final disposal of confiscated property.

Switzerland

[Original: English]
[8 April 2022]

2.3 Provisions on procedural measures and law enforcement

Section 1

Common provisions

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. 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 the provisions on criminalization 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 measures on real-time collection of traffic data 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 measures on interception of content data. Each Party shall consider restricting such a reservation to enable the broadest application of measures on real-time collection of traffic data;

(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 measures on real-time collection of traffic data and on interception of content data 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 measures on real-time collection of traffic data and on interception of content data.

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 International Covenant on Civil and Political Rights and other applicable international and regional 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.

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 have been stored by means of a computer system, in particular where there are grounds to believe that the computer data are 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 90 days, to enable the competent authorities to seek their 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 the provisions on the scope of procedural provisions and on conditions and safeguards of this Convention.

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 are 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 the provisions on the scope of procedural provisions and on conditions and safeguards of this Convention.

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 geographical 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.

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 are stored in another computer system or part of it in its territory, and such data are 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 the provisions on the scope of procedural provisions and on conditions and safeguards of this Convention.

Section 2

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 the provisions on criminalization of this Convention, when the offence is committed:

(a) In its territory; or

(b) On board a vessel that is flying the flag of that Party or an aircraft that is registered under the laws of that Party; or

(c) By one of its nationals, if the offence is punishable under the law of the State in which 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 established in accordance with the provisions on criminalization 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, provided that the offences 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.

4. A Party may also establish its jurisdiction over any offence established in accordance with the provisions on criminalization of this Convention, when the offence is committed:

(a) Against a national of that Party;

(b) Against that Party.

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

6. 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.

United Kingdom of Great Britain and Northern Ireland

[Original: English]
[12 April 2022]

Chapter. Procedural measures and law enforcement

Article 16
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 International Covenant on Civil and Political Rights, and other applicable international human rights law, and which shall incorporate the principle of proportionality.

2. Such conditions and safeguards shall, as appropriate in view of the nature of the procedure or power concerned, inter alia, include judicial or other independent supervision, grounds justifying application, and limitation of the scope and the duration of such power or procedure.

3. To the extent that it is consistent with the public interest, in particular the sound administration of justice, each Party shall consider the impact of the powers and procedures in this section upon the rights, responsibilities and legitimate interests of third parties.

Article 17
Scope of procedural provisions, including the wider use of procedural law for all offences

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, 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 the offences defined in 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.

Article 18
Expedited preservation

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 have been stored by means of a computer system, in particular where there are grounds to believe that the computer data are 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 90 days, to enable the competent authorities to seek their 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 human rights safeguards.

Article 19
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 are 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;

(c) The powers and procedures referred to in this article shall be subject to human rights safeguards.

2. 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 geographical 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.

Article 20
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 are stored in another computer system or part of it in its territory, and such data are 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 human rights safeguards.

United Republic of Tanzania

[Original: English]
[8 April 2022]

5. Procedural measures

Cybercrime laws identify standards of acceptable behaviour for information and communications technology users, establish socio-legal sanctions for cybercrime and protect information and communications technology users, in general, and mitigate and/or prevent harm to people, data, systems, services, and infrastructure. The United Republic of Tanzania proposes that the Convention encompass the following aspects in the procedural measures section.-

Expedited preservation ad disclosure of electronic data

The Convention should have a provision for Member States to include measures in their domestic legislation, as may be necessary, to enable its competent authorities to order or similarly obtain the expeditious preservation of specified electronic data, including traffic data, which have been stored by means of a computer system. In particular, where there are grounds to believe that the electronic data are particularly vulnerable to loss or modification.

Where, by means of an order to a person to preserve specified stored electronic 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 electronic data for a period of time necessary to enable the competent authorities to seek their disclosure. A party may provide for such an order to be subsequently renewed.

The Convention should contain provisions for Member States to 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.

Production order

There should be a provision within the Convention for legislative and other measures as may be necessary to empower competent authorities to order a person in its territory to submit specified computer data in that person's possession or control, which are stored in a computer system or a computer-data storage medium.

Search and seizure of stored computer data

It is imperative for the Convention to set obligations for Member States to have provisions in their legislation and other measures as may be necessary to empower their competent authorities to search, access and seize a computer system or part of it, computer data stored therein and in which computer data may be stored in its territory.

Protection of whistle-blowers and witnesses

The Convention should provide for the obligation of parties to provide for the protection of whistle-blowers, witnesses and victims of cybercrimes, as the circumstance of the case may require.

It is further proposed that the Convention should direct Member States to take appropriate measures within their means to provide effective protection from potential retaliation or intimidation to whistle-blowers and witnesses in criminal proceedings who give information or testimony concerning offences covered by this Convention and, as appropriate, for their relatives and other persons close to them in accordance with their domestic laws. These measures should not prejudice the rights of the defendant, including the right to due process.

6. Law enforcement

The proper management of cybercrimes and related offences requires the involvement of different processes, which are prevention, detection and combating. Thus, these processes, mandated to law enforcement agencies, need to be acknowledged. Therefore, the United Republic of Tanzania is of the view that the Convention should cover the following aspects in relation to law enforcement.

Training, technical assistance and exchange of expertise

To effectively prevent and combat the use of information and communications technologies for criminal purposes, it is essential to provide technical assistance to developing countries and strengthen the exchange of information. Technical assistance and exchange of expertise should focus on the following:

(a) Detection, prevention, and combating of the offences covered by the Convention;

(b) Techniques used by persons suspected of involvement in offences covered by the Convention, and appropriate countermeasures;

(c) Monitoring of the movement of contraband;

(d) Detection and monitoring of the proceeds of crime, property, equipment or instrumentalities and methods used for the transfer, concealment or disguise of such proceeds and instrumentalities, as well as methods used in combating cybercrimes;

(e) Collection of evidence;

(f) Modern law enforcement equipment and techniques, including the use of new software and undercover operations;

(g) Methods used in combating cybercrimes committed through the use of computer systems, telecommunications networks or other forms of modern technology;

(h) Planning and implementing, research and training programmes designed to share expertise on the protection of cyberspace.

Joint investigations

Cybercrimes are borderless in nature and may involve more than one country. The Convention should provide for the obligation of States parties to make arrangements in relation to matters that are the subject of investigations, prosecutions or judicial proceedings in one or more States. The competent authorities concerned may establish joint investigative bodies. The States parties involved are urged to ensure that the sovereignty of the State party in whose territory such an investigation is to take place is fully respected.

Financial support

There should be a provision under the Convention that imposes an obligation for developed States and United Nations agencies to offer financial support to developing countries so as to implement strategies for detecting, preventing and combating cybercrimes.

United States of America

[Original: English]
[8 April 2022]

Procedural measures and law enforcement

Procedural provisions

Scope of procedural provisions

1. Each State 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 the article addressing interception of content data, each State Party shall apply the powers and procedures referred to in paragraph 1 of this article to:

(a) The criminal offences established in accordance with the criminalization chapter 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.

Expedited preservation of stored computer data

1. Each State 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 have been stored by means of a computer system, in particular where there are grounds to believe that the computer data are particularly vulnerable to loss or modification.

2. Where a State 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 State 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 90 days, to enable

the competent authorities to seek their disclosure. A State Party may provide for such an order to be subsequently renewed.

3. Each State 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.

Production order

1. Each State Party shall adopt such legislative and other measures as may be necessary to empower its competent authorities to order a person in its territory to submit specified computer data in that person's possession or control, which are stored in a computer system or a computer-data storage medium;

Search and seizure of stored computer data

1. Each State 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 State 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 are stored in another computer system or part of it in its territory, and such data are 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 State 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 State 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.

Real-time collection of traffic data

1. Each State 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 State 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 State Party; or

(ii) To cooperate with 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 State 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 State 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.

Interception of content data

1. Each State 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 State 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 State Party; or

(ii) To cooperate with 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 State 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 associated with specified communications transmitted in its territory, through the application of technical means on that territory.

3. Each State 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.

Jurisdiction[17]

1. Each State Party shall adopt such measures as may be necessary to establish its jurisdiction over offences established in accordance with this Convention when:

(a) The offence is committed in the territory of that State Party; or

(b) The offence is committed on board a vessel that is flying the flag of that State Party or an aircraft that is registered under the laws of that State Party at the time that the offence is committed.

2. Subject to the sovereignty article of this Convention, a State Party may also establish its jurisdiction over any such offence when:

(a) The offence is committed against a national of that State Party; or

(b) The offence is committed by a national of that State party or a stateless person who has his or her habitual residence in its territory; or

(c) The offence is one of those established in accordance with article [money-laundering article] of this Convention and is committed outside its territory with a

[17] United Nations Convention against Corruption, article 42, and United Nations Convention against Transnational Organized Crime, article 15.

view to the commission of an offence established in accordance with article [money-laundering article] of this Convention within its territory; or

(d) the offence is committed against the State Party.

3. For the purposes of the extradition article of this Convention, each State Party shall take such measures as may be necessary to establish its jurisdiction over the offences established in accordance with this Convention when the alleged offender is present in its territory and it does not extradite such person solely on the ground that he or she is one of its nationals.

4. Each State Party may also take such measures as may be necessary to establish its jurisdiction over offences established in accordance with this Convention when the alleged offender is present in its territory and it does not extradite him or her.

5. If a State Party exercising its jurisdiction under paragraph 1 or 2 of this article has been notified, or has otherwise learned, that any other States Parties are conducting an investigation, prosecution or judicial proceeding in respect of the same conduct, the competent authorities of those States Parties shall, as appropriate, consult one another with a view to coordinating their actions.

6. Without prejudice to norms of general international law, this Convention shall not exclude the exercise of any criminal jurisdiction established by a State Party in accordance with its domestic law.

Confiscation and seizure[18]

1. States Parties shall adopt, to the greatest extent possible within their domestic legal systems, such measures as may be necessary to enable confiscation of:

(a) Proceeds of crime derived from offences covered by this Convention or property the value of which corresponds to that of such proceeds;

(b) Property, equipment or other instrumentalities used in or destined for use in offences covered by this Convention.

2. States Parties shall adopt such measures as may be necessary to enable the identification, tracing, freezing or seizure of any item referred to in paragraph 1 of this article for the purpose of eventual confiscation.

3. If proceeds of crime have been transformed or converted, in part or in full, into other property, such property shall be liable to the measures referred to in this article instead of the proceeds.

4. If proceeds of crime have been intermingled with property acquired from legitimate sources, such property shall, without prejudice to any powers relating to freezing or seizure, be liable to confiscation up to the assessed value of the intermingled proceeds.

5. Income or other benefits derived from proceeds of crime, from property into which proceeds of crime have been transformed or converted or from property with which proceeds of crime have been intermingled shall also be liable to the measures referred to in this article, in the same manner and to the same extent as proceeds of crime.

6. For the purposes of this article and article [on international cooperation for purposes of confiscation] of this Convention, each State Party shall empower its courts or other competent authorities in order that bank, financial or commercial records be made available or be seized. States Parties shall not decline to act under the provisions of this paragraph on the ground of bank secrecy.

7. States Parties may consider the possibility of requiring that an offender demonstrate the lawful origin of alleged proceeds of crime or other property liable to

[18] Organized Crime Convention, article 12.

confiscation, to the extent that such a requirement is consistent with the principles of their domestic law and with the nature of the judicial and other proceedings.

8. The provisions of this article shall not be construed to prejudice the rights of bona fide third parties.

9. Nothing contained in this article shall affect the principle that the measures to which it refers shall be defined and implemented in accordance with and subject to the provisions of the domestic law of a State Party.

Disposal of confiscated proceeds of crime or property[19]

1. Proceeds of crime or property confiscated by a State Party pursuant to the article on confiscation and seizure and [any article on international cooperation for the purposes of confiscation] of this Convention shall be disposed of by that State Party in accordance with its domestic law and administrative procedures.

2. When acting on the request made by another State Party in accordance with article [any article on international cooperation for the purposes of confiscation] of this Convention, States Parties shall, to the extent permitted by domestic law and if so requested, give priority consideration to returning the confiscated proceeds of crime or property to the requesting State Party so that it can give compensation to the victims of the crime or return such proceeds of crime or property to their legitimate owners.

3. When acting on the request made by another State Party in accordance with the article on confiscation and seizure and [any international cooperation for the purposes of confiscation] of this Convention, a State Party may, after due consideration has been given to compensation to victims, give special consideration to concluding agreements on or arrangements on:

(a) Contributing the value of such proceeds of crime or property or funds derived from the sale of such proceeds of crime or property or a part thereof to the account designated in accordance with [any technical assistance article] of this Convention and to intergovernmental bodies specializing in the fight against cybercrime;

(b) Sharing with other States Parties, on a regular or case-by-case basis, such proceeds of crime or property, or funds derived from the sale of such proceeds of crime or property, in accordance with its domestic law or administrative procedures.

Establishment of criminal record[20]

Each State Party may adopt such legislative or other measures as may be necessary to take into consideration, under such terms as and for the purpose that it deems appropriate, any previous conviction in another State of an alleged offender for the purpose of using such information in criminal proceedings relating to an offence covered by this Convention.

Protection of witnesses[21]

1. Each State Party shall take appropriate measures within its means to provide effective protection from potential retaliation or intimidation for witnesses in criminal proceedings who give testimony concerning offences covered by this Convention and, as appropriate, for their relatives and other persons close to them.

2. The measures envisaged in paragraph 1 of this article may include, inter alia, without prejudice to the rights of the defendant, including the right to due process:

(a) Establishing procedures for the physical protection of such persons, such as, to the extent necessary and feasible, relocating them and permitting, where

[19] Organized Crime Convention, article 14.
[20] Organized Crime Convention, article 22.
[21] Organized Crime Convention, article 24 and Convention against Corruption, article 32.

appropriate, non-disclosure or limitations on the disclosure of information concerning the identity and whereabouts of such persons;

(b) Providing evidentiary rules to permit witness testimony to be given in a manner that ensures the safety of the witness, such as permitting testimony to be given through the use of communications technology such as video links or other adequate means.

3. States Parties shall consider entering into agreements or arrangements with other States for the relocation of persons referred to in paragraph 1 of this article.

4. The provisions of this article shall also apply to victims insofar as they are witnesses.

Assistance to and protection of victims[22]

1. Each State Party shall take appropriate measures within its means to provide assistance and protection to victims of offences covered by this Convention, in particular in cases of threat of retaliation or intimidation.

2. Each State Party shall establish appropriate procedures to provide access to compensation and restitution for victims of offences covered by this Convention.

3. Each State Party shall, subject to its domestic law, enable views and concerns of victims to be presented and considered at appropriate stages of criminal proceedings against offenders in a manner not prejudicial to the rights of the defence.

Measures to enhance cooperation with law enforcement authorities[23]

1. Each State Party shall take appropriate measures to encourage persons who participate or who have participated in offences established by this Convention:

(a) To supply information useful to competent authorities for investigative and evidentiary purposes on such matters as:

(i) The identity, nature, composition, structure, location or activities of persons participating in offences established by this Convention;

(ii) Links, including international links, with other persons participating in offences established by this Convention;

(iii) Offences that persons participating in offences established in this Convention have committed or may commit;

(b) To provide factual, concrete help to competent authorities that may contribute to depriving [persons participating in offences established by this Convention] of their resources or of the proceeds of crime.

2. Each State Party shall consider providing for the possibility, in appropriate cases, of mitigating punishment of an accused person who provides substantial cooperation in the investigation or prosecution of an offence covered by this Convention.

3. Each State Party shall consider providing for the possibility, in accordance with fundamental principles of its domestic law, of granting immunity from prosecution to a person who provides substantial cooperation in the investigation or prosecution of an offence covered by this Convention.

4. Protection of such persons shall be as provided for in the article on protection of witnesses of this Convention.

5. Where a person referred to in paragraph 1 of this article located in one State Party can provide substantial cooperation to the competent authorities of another State Party, the States Parties concerned may consider entering into agreements or

[22] Organized Crime Convention, article 25.
[23] Organized Crime Convention, article 26.

arrangements, in accordance with their domestic law, concerning the potential provision by the other State Party of the treatment set forth in paragraphs 2 and 3 of this article.

Venezuela (Bolivarian Republic of)

[Original: Spanish]
[13 April 2022]

6. Procedural measures and law enforcement

With regard to criminal procedures and law enforcement, in general terms it is proposed that the future convention establish mechanisms relating to:

- The determination of mechanisms for cooperation in identifying and sharing evidence and other phases of investigations
- The definition of mechanisms for determining the responsibilities of non-State actors and the establishment of regulatory frameworks delineating the scope of the obligations of such actors in processes relating to the enforcement of national and international law
- The establishment of jurisdiction with respect to the use of information and communications technology, promoting cooperation and without prejudice to the sovereignty of States in the context of criminal investigations.

Viet Nam

[Original: English]
[12 April 2022]

Chapter III
Procedural measures and law enforcement

8. Jurisdiction

1. Each Member State shall take such measures as may be necessary to establish its jurisdiction over the offences referred to in articles […] in the following cases:

(a) When the offences are committed in any territory under its jurisdiction or on board a ship or aircraft registered in that State;

(b) When the alleged offender is a national of that State;

(c) When the victim is a national of that State if that State considers it appropriate.

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

9. Powers of competent authorities

Member States shall:

(a) Undertake measures of prevention, identification, investigation, prosecution and judicial proceedings of commissions relating to criminal offences covered by this Convention;

(b) Collect evidence relating to offences covered by this Convention, including digital data in a manner of protection of sovereignty of other Member States.