GHANA'S CONTRIBUTIONS FOR THE PROVISIONS ON CRIMINALISATION, GENERAL PROVISIONS AND PROVISIONS ON PROCEDURAL MEASURES AND LAW ENFORCEMENT FOR THE FUTURE UN CONVENTION ON COUNTERING THE USE OF ICTs FOR CRIMINAL PURPOSES

(Disclaimer) This contribution is without prejudice to any future contributions that Ghana may make during the course of future discussions, including on the present chapters.

Ghana welcomes the consideration of a global convention to counter the use of ICT for criminal purposes and note that when well elaborated it would complement existing national, regional and international instruments for addressing the cybersecurity challenges of our time and enhancing the safety and security of the cyberspace. To name a few such instruments include the UN Convention against Corruption (UNCAC) and the UN Convention against Transnational Organised Crime (UNTOC), the African Union Convention on Cyber Security and Personal Data Protection (Malabo) and the Convention on Cybercrime (Budapest Convention).

We identify that successful prosecution of cybercrime is a measure of mitigating threats to ICTs and their misuse thereof. Accordingly, the new draft Convention should harmonise national laws on cybercrime, improve investigatory powers and procedures, and promote and enhance international cooperation while protecting the privacy and other fundamental human rights as well as offering measures for sustainable capacity building and technical assistance.

Ghana is of the view that the Convention should criminalise cyber-dependent offences, together with cyber-enabled crimes where the use of a computer increases the scale, scope and speed of the offence.

The Convention should reinforce and enhance procedural law in existing instruments as well as include other innovative measures to strengthen investigations of cybercrime.

Additionally, we are of the view that the mandate of the Convention should extend into sustainable capacity building measures in order to enhance domestic capabilities and enable the sharing of good investigative practices and experiences.

As part of Ghana's contribution to shaping the discussion in the development of the convention we propose the following potential text for further deliberations at the second session of the Ad Hoc Committee.

CHAPTER I GENERAL PROVISIONS

Article 1 Statement of Purpose

The purpose of this convention is to promote and facilitate international cooperation as well as strengthen measures to prevent and counter the use of ICTs for criminal purposes.

Article 2 Use of Terms

For the purpose of this Convention

a. "Computer System" means any device or a group of interconnected or related devices, one or more of which, pursuant to a program, performs automatic processing of data;
b. "Computer data" means any representation of facts, information or concepts in a form suitable for processing in a computer system, including a program suitable to cause a computer system to perform a function;
c. "Content data" means the communication content of the communication, that is, the meaning or purport of the communication or the message or information being conveyed by the communication other than traffic data;
d. "Child" means a person under 18years of age. A Party may however, require a lower age-limit, which shall be not less than 16 years.
e. "Critical information Infrastructure" means a computer or computer system identified by a member state in its domestic legislation as essential for national security or the economic and social well-being of citizens.
f. "Prohibited intimate image and visual recording" includes
    I. Moving or still image that depicts
        i. The person engaged in an intimate sexual activity that is not ordinarily done in public; or
        ii. The genital or anal region of a person, when the genital or anal region is bare or covered only by underwear; and
    II. An image that has been altered to appear to show any of the things mentioned in paragraph (I) even if the thing has been digitally obscured, if the person is depicted in a sexual way;
g. Service Provider means:
    I. Any public or private entity that provides to users of its service the ability to communicate by means of a computer system, and
    II. Any other entity that processes or stores computer data on behalf of such communication service or users of such service;
h. "Subscriber" means a customer or a user of an electronic communications network, electronic communications service or broadcasting service;
i. "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 the services of a service provider other than traffic or content data and by which may be established;

I. The type of communication service used, the technical provision taken in respect of the communication service and the period of service;
II. The identity, postal or geographic address, telephone and other access number of the subscriber, billing and payment information available on the basis of the service agreement or arrangement; and
III. Any other information on the site of the installation of a communication equipment, available on the basis of the service agreement or arrangement

j. "Traffic data" means any computer data relating to a communication by means of a computer system, generated by a computer system that formed a part in the chain of communication, indicating the origin, destination, route, time, date, size or duration of the communication or the type of underlying service;

Article 3 Scope of application

This Convention shall apply, in accordance with its terms, to

1. the Prevention, investigation and prosecution of offences established in accordance with Articles 5 through 20 and
2. The collection of evidence in electronic form of a criminal offence;
3. The provision and conduct of technical assistance and capacity building on matters covered by this Convention
4. the freezing, seizure, confiscation and return of the proceeds of offences established in accordance with this Convention.

Article 4 Protection of Sovereignty

1. Member States shall carry out their obligations under this Convention in a manner consistent with the principles of sovereign equality and territorial integrity of States and that of non-intervention in domestic affairs of other States
2. Nothing in this Convention entitles a Member State to undertake in the territory of another State the exercise of jurisdiction and performance of functions that are reserved exclusively for the authorities of that other State by its domestic law.

CHAPTER II PROVISIONS ON CRIMINALISATION[1]

Cyber –dependent crimes: Offences against the confidentiality, integrity and availability of computer systems and data

Article 5: Unauthorised Access to a Computer System:

Each State Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences, when committed intentionally: the access to the whole or any

[1] The text for this section is adopted from primarily the Budapest Convention (BC), African Union Convention (AUC), Electronic Transactions Act, 2008 (Act 772) and Cybersecurity Act, 2020 (Act 1038). These Instruments forms Ghana's Cybercrime Legislative framework.

part of a computer system, without authorisation or exceeding authorised access. A Party may require that the offence be committed by infringing security measures, with the intent of obtaining computer data or other dishonest intent, or in relation to a computer system that is connected to another computer system.

Article 6: Unauthorised Access to a Critical Information Infrastructure:

Each State Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences, when committed intentionally: the access to the whole or any part of a critical information infrastructure without authorisation.

Article 7 – Unauthorised Interception:

Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, the interception without authorisation, made by technical means, of nonpublic transmissions of computer data to, from or within a computer system, including electromagnetic emissions from a computer system carrying such computer data.

A Party may require that the offence be committed with dishonest intent, or in relation to a computer system that is connected to another computer system.

Article 8 – Data Interference:

1. Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, the damaging, deletion, deterioration, alteration, copying or suppression of computer data without authorization.
2. A Party may reserve the right to require that the conduct described in paragraph 1 result in serious harm.

Article 9 – System Interference:

Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, the serious hindering without authorisation of the functioning of a computer system by inputting, transmitting, damaging, deleting, deteriorating, altering or suppressing computer data.

Article 10 – Misuse of Devices:

1. Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally and without right:
   a. the production, sale, procurement for use, import, distribution or otherwise making available of:

i. a device, including a computer program, designed or adapted primarily for the purpose of committing any of the offences established in accordance with Articles 5 through 9;
ii. a computer password, access code, or similar data by which the whole or any part of a computer system is capable of being accessed, with intent that it be used for the purpose of committing any of the offences established in Articles 5 through 9; and

b. The possession of an item referred to in paragraphs a.i or ii above, with intent that it be used for the purpose of committing any of the offences established in Articles 5 through 9. A Party may require by law that a number of such items be possessed before criminal liability attaches.

2. This article shall not be interpreted as imposing criminal liability where the production, sale, procurement for use, import, distribution or otherwise making available or possession referred to in paragraph 1 of this article is not for the purpose of committing an offence established in accordance with Articles 5 through 9 of this Convention, such as for the authorised testing or protection of a computer system.

3. Each Party may reserve the right not to apply paragraph 1 of this article, provided that the reservation does not concern the sale, distribution or otherwise making available of the items referred to in paragraph 1 a.ii of this article.

Cyber-enabled crimes: Offences whose scope, speed and impact have increased as a result of the advent of computer systems[2]

Article 11 – Computer-related forgery:

Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally and without right, the input, alteration, deletion, or suppression of computer data, resulting in inauthentic data with the intent that it be considered or acted upon for legal purposes as if it were authentic, regardless whether or not the data is directly readable and intelligible. A Party may require an intent to defraud, or similar dishonest intent, before criminal liability attaches.

Article 12 – Computer-related fraud:

Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally and without right, the causing of a loss of property to another person by:

a. any input, alteration, deletion or suppression of computer data,
b. any interference with the functioning of a computer system,

[2] Computer related fraud, forgery and crimes targeting children are consistent with BC, AUC and the Cybersecurity Act, 2020 (Act 1038)

With fraudulent or dishonest intent of procuring, without right, an economic benefit for oneself or for another person.

Crimes against children

Article 13 – Offences related to child sexual exploitation and abuse online:

1. Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally and without right, the following conduct
    a. Producing child sexual exploitation and abuse material for the purpose of publication and distribution through a computer system;
    b. Procuring child sexual exploitation and abuse material for oneself or for another person;
    c. Offering or making available child sexual exploitation and abuse material through a computer system or an electronic device;
    d. Publishing, distribution, streaming (including live streaming), transmitting child sexual exploitation and abuse material through a computer or an electronic device or;
    e. Possessing child sexual exploitation and abuse material in a computer system or on a computer or electronic record storage medium
2. For purpose of paragraph (c) of subsection (1), a person publishes child sexual exploitation and abuse material if that person,
    a. Parts with possession of the, child sexual exploitation and abuse material, to another person; or
    b. Exposes or offers the child sexual exploitation and abuse material for acquisition by another person
3. For the purpose of this section, child sexual exploitation and abuse material includes a material image, visual recording, video, audio, live streaming material, drawing or text, that depicts or describes
    a. A child engaged in sexually explicit or suggestive conduct;
    b. A person who appears to be a child engaged in sexually explicit or suggestive conduct;
    c. Images representing a child engaged in sexually explicit or suggestive conduct;
    d. Sexually explicit images of children;
    e. Process or material for viewing of child sexual exploitation and abuse in real-time often involving the offender directing the abuse;
    f. Any written material, visual representation or audio recording that advocates or counsels unlawful sexual activity with children;
    g. Any written material that has, as its dominant characteristics, the description, for a sexual purpose of unlawful sexual activity with a child;
    h. Any audio recording that has as its dominant characteristic, the description, for a sexual purpose, of unlawful sexual activity with a child.

Article 14: Dealing with a child for purposes of Sexual abuse

Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally the use of

a. a computer online service,
b. an internet service,
c. a local bulletin board service, or
d. any other device capable of electronic data storage or transmission

to seduce, solicit, lure, groom or entice, or attempt to seduce, solicit, lure, groom or entice, a child or another person believed by the person to be a child, for the purpose of facilitating, encouraging, offering, or soliciting, unlawful sexual conduct of or with any child, or the visual depiction of such conduct.

Article 15: Cyberstalking of a child

Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally the use of a computer online service, an internet service, or a local internet bulletin board service or any other electronic device to compile, transmit, publish, reproduce, buy, sell, receive, exchange, or disseminate the name, telephone number, electronic mail address, residence address, picture, physical description, characteristics or any other identifying information on a child in furtherance of an effort to arrange a meeting with the child for the purpose of engaging in sexual intercourse, sexually explicit conduct, or unlawful sexual activity.

Other online sexual offences[3]

Article 16: Sexual Extortion

1. Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally the threatening to distribute by post, email, text or transmit, by electronic means or otherwise, a private image or moving images of another person engaged in sexually explicit conduct, with the specific intent to
    a. harass, threaten, coerce, intimidate or exert any undue influence on the person especially to extort money or other consideration or to compel the victim to engage in unwanted sexual activity or
    b. actually extort money or other consideration or compel the victim to engage in unwanted sexual activity
2. Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally the threatening to distribute by post, email, text or transmit, by electronic means or

[3] Consistent with provisions of the Cybersecurity Act

otherwise, a private image or moving images of a child engaged in sexually explicit conduct, with the specific intent to

a. harass, threaten, coerce, intimidate or exert any undue influence on the child especially to extort money or other consideration or to compel the victim to engage in unwanted sexual activity or
b. actually extort money or other consideration or compel the victim to engage in unwanted sexual activity

3. For the purpose of sections (1) and (2), an intimate image may include a depiction in a way that the genital or anal region of another person is bare or covered only by underwear; or the breasts below the top of the areola, that is either uncovered or clearly visible through clothing.

Article 17: Non-consensual sharing of intimate image[4]

1. Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, the intentional distribution or intentionally causing another person to distribute the intimate image or prohibited visual recording of another identifiable person, without the consent of the person depicted in the intimate image, with the intent to cause serious emotional distress and in respect of which, there was a reasonable expectation of privacy either at the time of the creation of the image or visual recording and/or at the time the offence was committed.
2. For the purpose of this section, "serious emotional distress" includes any intentional conduct that results in mental reactions such as fright, nervousness, grief, anxiety, worry, mortification, shock, humiliation and indignity as well as physical pain.

Article 18 Threat to distribute prohibited intimate image or visual recording

1. Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally threatening to distribute a prohibited intimate image or visual recording of another person in a way that would cause that other person distress reasonably arising in all the circumstances and the threat is made in a way that would cause that other person fear, reasonably arising in all the circumstances, of the threat being carried out.

Article 19 – Offences related to infringements of copyright and related rights[5]

1. Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law the infringement of copyright, as defined under the law of that Party, pursuant to the obligations it has undertaken under the Paris Act of 24 July 1971 revising the Bern Convention for the Protection of Literary and Artistic Works, the Agreement on Trade-Related Aspects of Intellectual Property Rights and the WIPO Copyright Treaty, with the exception of any moral rights conferred by such conventions, where such acts are committed willfully, on a commercial scale and by means of a computer system.

2. Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law the infringement of related rights, as defined under the law of that Party, pursuant to the obligations it has undertaken under the International Convention for the Protection of Performers, Producers of Phonograms and Broadcasting Organisations (Rome Convention), the Agreement on Trade-Related Aspects of Intellectual Property Rights and the WIPO Performances and Phonograms Treaty, with the exception of any moral rights conferred by such conventions, where such acts are committed willfully, on a commercial scale and by means of a computer system.

3. A Party may reserve the right not to impose criminal liability under paragraphs 1 and 2 of this article in limited circumstances, provided that other effective remedies are available and that such reservation does not derogate from the Party's international obligations set forth in the international instruments referred to in paragraphs 1 and 2 of this article.

Article 20 – Attempt and aiding or abetting

1. Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, aiding or abetting the commission of any of the offences established in accordance with Articles 5 through 19 of the present Convention with intent that such offence be committed.
2. Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, an attempt to commit any of the offences established in accordance with Articles 7 through 9, 11, 12, 13.1.a,b, and e, 14, 15, 16, 17.

[5] Consistent with BC and AUC

Article 21 – Corporate liability

1. Each Party shall adopt such legislative and other measures as may be necessary to ensure that legal persons can be held liable for a criminal offence established in accordance with this Convention, committed for their benefit by any natural person, acting either individually or as part of an organ of the legal person, who has a leading position within it, based on:
    a. a power of representation of the legal person;
    b. an authority to take decisions on behalf of the legal person;
    c. an authority to exercise control within the legal person.

2. In addition to the cases already provided for in paragraph 1 of this article, each Party shall take the measures necessary to ensure that a legal person can be held liable where the lack of supervision or control by a natural person referred to in paragraph 1 has made possible the commission of a criminal offence established in accordance with this Convention for the benefit of that legal person by a natural person acting under its authority.

3. Subject to the legal principles of the Party, the liability of a legal person may be criminal, civil or administrative.

4. Such liability shall be without prejudice to the criminal liability of the natural persons who have committed the offence.

Article 22 – Sanctions and Measures

1. Each Party shall adopt such legislative and other measures as may be necessary to ensure that the criminal offences established in accordance with Articles 5 through 20 are punishable by effective, proportionate and dissuasive sanctions, which include deprivation of liberty.

2. Each Party shall ensure that legal persons held liable in accordance with Article 21 shall be subject to effective, proportionate and dissuasive criminal or non-criminal sanctions or measures, including monetary sanctions.

CHAPTER III PROCEDURAL MEASURES AND LAW ENFORCEMENT[6]

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.

Article 24 – Conditions and safeguards

[6] The text for this section is adopted from primarily the Budapest Convention (BC), African Union Convention (AUC), Electronic Transactions Act, 2008 (Act 772) and Cybersecurity Act, 2020 (Act 1038). These Instruments forms Ghana's Cybercrime Legislative framework.

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[7] including the 1948 Universal Declaration on Human Rights, the 1966 United Nations International Covenant on Civil and Political Rights, and other applicable international human rights instruments, and which shall incorporate the principle of proportionality 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 [8]

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

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

3. Each Party shall adopt such legislative and other measures as may be necessary to oblige the custodian or other person who is to preserve the computer data to keep confidential the undertaking of such procedures for the period of time provided for by its domestic law.

[7] https://www.ohchr.org/en/instruments-and-mechanisms/international-human-rights-law

[8] Consistent with the Budapest Convention, African Union Convention, Ghana's Electronic Transactions Act, 2008 (Act 772) and Ghana's Cybersecurity Act, 2020 (Act 1038)

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[9]

1. Each Party shall adopt, in respect of traffic data that is 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 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. person in its territory to submit specified computer data in that person's possession or control, which is stored in a computer system or a computer-data storage medium; and
    b. a service provider offering its services in the territory of the Party to submit subscriber information relating to such services in that service provider's possession or control.

2. 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 is reasonably required for the purposes of a specific criminal investigations.

3. For the purpose of paragraph 2, the Competent Authority shall

[9] Consistent with Budapest Convention

a. explain to the independent Supervisory Authority why the Competent Authority believes 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. Whilst 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 whilst 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 geographic address, telephone and other access number, billing and payment information, available on the basis of the service agreement or arrangement;
    c. any other information on the site of the installation of communication equipment, available on the basis of the service agreement or arrangement.

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

3. Each Party shall adopt such legislative and other measures as may be necessary to empower its competent authorities to seize or similarly secure computer data accessed according to paragraphs 1 or 2. These measures shall include the power to:
    a. seize or similarly secure a computer system or part of it or a computer-data storage medium;
    b. make and retain a copy of those computer data;
    c. maintain the integrity of the relevant stored computer data;
    d. Render inaccessible or remove those computer data in the accessed computer system.
4. Each Party shall adopt such legislative and other measures as may be necessary to empower its competent authorities to order any person who has knowledge about the functioning of the computer system or measures applied to protect the computer data therein to provide, as is reasonable, the necessary information, to enable the undertaking of the measures referred to in paragraphs 1 and 2.

5. 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 co-operate and assist the competent authorities in the collection or recording of, traffic data, in real-time, associated with specified communications in its territory transmitted by means of a computer system.
2. 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 is reasonably required for the purposes of a specific criminal investigations.
3. For the purpose of paragraph 2, the Competent Authority shall

    d. explain to the independent Supervisory Authority why the Competent Authority believes traffic data sought, will be available to
        i. the person in control or possession of the computer system or
        ii. a service provider
    e. Identify and explain with specificity the type of traffic data being sought;
    f. Identify and explain with specificity the offences in respect of which the power under this article is sought;
    g. Indicate what measures shall be taken to ensure that traffic data will be procured
        i. Whilst 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 whilst 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:
        1. to collect or record through the application of technical means on the territory of that Party, or
        2. to co-operate and assist the competent authorities in the collection or recording of, content data, in real-time, of specified communications in its territory transmitted by means of a computer system.

2. 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 requests

3. For the purpose of paragraph 2, the Competent Authority shall

    a. explain to the independent Supervisory Authority why the Competent Authority believes 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. Whilst 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 whilst 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 (6) years
    b. traffic data for a period of twelve (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.

CONFISCATION AND SEIZURE

Article 32 – Confiscation and Seizure

1. Each Party 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. 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. Member States 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 Member State.

JURISDICTION

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.