Dominican Republic's submission for the Second session Ad Hoc Committee to Elaborate a Comprehensive International Convention on Countering the Use of Information and Communications Technologies for Criminal Purposes

Purpose

To promote international cooperation and technical assistance to prevent, investigate and prosecute cybercrime effectively, including the adoption and strengthening of substantive measures and procedural powers with adequate safeguards, balancing society and victim's rights with individual human and privacy rights.

Scope of application

This Convention shall apply to:

a) The prevention, investigation and prosecution of criminal offences established in this Convention,

b) The collection and sharing of evidence in electronic form of any criminal offence on a dual-criminality basis.

c) The provision and conduct of technical assistance and capacity building on matters covered by this Convention.

Conditions and safeguards

1. Each State Party shall ensure that the establishment, implementation and application of the provisions of this convention are subject to conditions and safeguards provided for under its domestic law, which shall provide for the full protection of human rights and liberties, incorporating the principles of the rule of law, legality, necessity and proportionality.

2. Such conditions and safeguards shall include judicial or other independent supervision, grounds justifying application, and limitation of the scope and the duration of the power or procedure.

Terms

Computer system:

Any device or group of interconnected or related devices, one or more of which, pursuant to a program, performs automatic processing of data or telecommunications functions.

Computer data:

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

Subscriber information:

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:

- the type of communication service used, the technical provisions taken thereto and the period of service;

- 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;

- any other information on the communication equipment and the site of its installation, available on the basis of the service agreement or arrangement

Traffic data:

Any computer data relating to a communication by means of a computer system, generated by a computer system that formed a part in the chain of communication, indicating the communication's origin, destination, route, time, date, size, duration, or type of underlying service.

Content data:

Any computer data or any other information other than traffic or subscriber data, such as text, voice, videos, images and sound, or the communication content of a communication.

Service provider:

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.

Central authority:

The authority or authorities designated for sending and answering requests for mutual assistance, the execution of such requests or the transmission to the authorities competent for their execution.

Competent authority:

A Judicial, administrative or law enforcement authority empowered by domestic law to order, authorize or undertake the execution of measures with respect to specific criminal investigations of proceedings.

Emergency:

A situation in which there is a significant and imminent risk to the life or safety of any natural person;

Criminalization

Illegal access

Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, the access to the whole or any part of a computer system without right. A Party may require that the offence be committed by infringing security measures, with the intent of obtaining computer data or other dishonest intent, or in relation to a computer system that is connected to another computer system.

Illegal interception

Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, the interception without right, made by technical means, of non-public transmissions of computer data to, from or within a computer system, including electromagnetic emissions from a computer system carrying such computer data. A Party may require that the offence be committed with dishonest intent, or in relation to a computer system that is connected to another computer system.

Data interference

1. Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, the damaging, deletion, deterioration, alteration or suppression of computer data without right.

2. A Party may reserve the right to require that the conduct described in paragraph 1 result in serious harm.

System interference

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

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 this convention;

      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 this convention; 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 this convention. 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 (the previous substantive Articles) of this Convention, such as for the authorized 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.

Computer-related forgery

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

Computer-related fraud

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

a. any input, alteration, deletion or suppression of computer data;

b. any interference with the functioning of a computer system,

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

Offences related to child sexual exploitation

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 material* for the purpose of its distribution through a computer system;

    b. offering or making available child *sexual exploitation material* through a computer system;

    c. distributing or transmitting child *sexual exploitation material* through a computer system;

    d. procuring child *sexual exploitation material* through a computer system for oneself or for another person;

    e. possessing child *sexual exploitation material* in a computer system or on a computer-data storage medium.

2. For the purpose of paragraph 1 above, the term "child *sexual exploitation material*" shall include pornographic material that visually depicts:

    a. a minor engaged in sexually explicit conduct;

    c. a person appearing to be a minor engaged in sexually explicit conduct;

    d. realistic images representing a minor engaged in sexually explicit conduct.

3. For the purpose of paragraph 2 above, the term "minor" shall include all persons under 18 years of age. A Party may, however, require a lower age-limit, which shall be not less than 16 years.

4. Each Party may reserve the right not to apply, in whole or in part, paragraphs 1, sub-paragraphs d. and e, and 2, sub-paragraphs b. and c.

Child sexual exploitation material

a) visual material, including photographic, video and live-streaming media, that depicts:

i) a child engaged in or in the presence of sexual activity,
ii) a person appearing to be a child engaged in or in the presence of sexual activity,
iii) realistic images representing a child engaged in or in the presence of sexual activity;

b) written material that:

i) advocates sexual activity with a child,
ii) is written for a sexual purpose and has as a dominant characteristic the description of sexual activity with a child; and

c) audio recordings that:

i) advocates sexual activity with a child,
ii) is recorded for a sexual purpose and has as a dominant characteristic the description of sexual activity with a child.

Grooming

Each State Party shall take the necessary legislative or other measures to criminalize the knowing persuasion, inducement, enticement, or coercion, through information and communication technologies, of a child, or an

individual believed to be a child, to engage in any illegal sexual activity. Each State Party shall take such necessary legislative or other measures to assure that its national law does not require a meeting in person between the individual and a child.

Nonconsensual dissemination of intimate images

1. Establish as criminal offences, when committed intentionally and without right, publishing, distributing, transmitting, selling, making available, or advertising an intimate image of a person by any means of a computer system, knowing that the person depicted in the image did not give their consent to that conduct, or being reckless as to whether or not that person gave their consent to that conduct.

2. For the purpose of paragraph 1, intimate image means a visual recording of a person made by any means including a photographic, film, or video recording:

    a) in which the person is nude, is exposing their genital organs, anal region or breasts, or is engaged in explicit sexual activity;

    b) in respect of which, at the time of the recording, there were circumstances that gave rise to a reasonable expectation of privacy; and

    c) in respect of which the person depicted retains a reasonable expectation of privacy at the time the offence is committed.

Cyber-extortion / Threat to distribute prohibited intimate image or visual recording

Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offence under its domestic law, when committed intentionally the threatening to expose, distribute or transmit, by electronic means or otherwise, private intimate images of another person with the specific intent of harassing, threatening, coercing, intimidating or

exerting any undue influence on the person especially to extort money or other consideration or to compel the victim to engage in unwanted sexual activity.

"Revenge porn"

Knowingly disclosing one or more sexual images of another identifiable person when:

1. The person depicted did not consent to the disclosure of the sexual image;
2. There was an agreement or understanding between the person depicted and the person disclosing that the sexual image would not be disclosed; and
3. The person disclosed the sexual image with the intent to harm the person depicted or to receive financial gain.

Attempt, participation, aiding and 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 (the previous substantive articles) 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 (the previous substantive articles) of this Convention.

3. Each Party may reserve the right not to apply, in whole or in part, paragraph 2 of this article.

Liability of a legal person

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.

Procedural measures

Scope of procedural provisions

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

2. Except as specifically provided otherwise in Article [X], 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 [A] through [Z] 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.

Request for domain name registration information

1. Each Party shall adopt such legislative and other measures as may be necessary to empower its competent authorities, for the purposes of specific criminal investigations or proceedings, to issue a request to an entity providing domain name registration services in the territory of another Party for information in the entity's possession or control, for identifying or contacting the registrant of a domain name.

2. Each Party shall adopt such legislative and other measures as may be necessary to permit an entity in its territory to disclose such information in response to a request under paragraph 1, subject to reasonable conditions provided by domestic law.

Disclosure of subscriber information

1. Each Party shall adopt such legislative and other measures as may be necessary to empower its competent authorities to issue an order to be submitted directly to a service provider in the territory of another Party, in order to obtain the disclosure of specified, stored subscriber information in that service provider's possession or control, where the subscriber information is needed for the issuing Party's specific criminal investigations or proceedings.

2. Each Party shall adopt such legislative and other measures as may be necessary for a service provider in its territory to disclose subscriber information in response to an order under paragraph 1.

Expedited preservation of stored computer data

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

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

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

Expedited preservation and partial disclosure of traffic data

Each Party shall adopt, in respect of traffic data that is to be preserved under Article 16, such legislative and other measures as may be necessary to:

a. ensure that such expeditious preservation of traffic data is available regardless of whether one or more service providers were involved in the transmission of that communication; and

b. ensure the expeditious disclosure to the Party's competent authority, or a person designated by that authority, of a sufficient amount of traffic data to enable the Party to identify the service providers and the path through which the communication was transmitted.

Production order

Each Party shall adopt such legislative and other measures as may be necessary to empower its competent authorities to order:

a. a person in its territory to submit specified computer data in that person's possession or control, which is stored in a computer system or a computer-data storage medium; and

b. a service provider offering its services in the territory of the Party to submit subscriber information relating to such services in that service provider's possession or control.

Giving effect to orders from another Party for expedited production of subscriber information and traffic data

1. Each Party shall adopt such legislative and other measures as may be necessary to empower its competent authorities to issue an order to be submitted as part of a request to another Party for the purpose of compelling a service provider in the requested Party's territory to produce specified and stored

    a. subscriber information, and
    b. traffic data

    in that service provider's possession or control which is needed for the Party's specific criminal investigations or proceedings.

2. Each Party shall adopt such legislative and other measures as may be necessary to give effect to an order under paragraph 1 submitted by a requesting Party.

3. In its request, the requesting Party shall submit the order under paragraph 1, the supporting information and any special procedural instructions to the requested Party.

Expedited disclosure of stored computer data in an emergency

Each Party shall adopt such legislative and other measures as may be necessary, in an emergency, for its point of contact for the 24/7 Network to transmit a request to and receive a request from a point of contact in another Party seeking immediate assistance in obtaining from a service provider in the territory of that Party the expedited disclosure of specified, stored computer data in that service provider's possession or control, without a request for mutual assistance.

Emergency mutual assistance

Each Party may seek mutual assistance on a rapidly expedited basis where it is of the view that an emergency exists. A request under this article shall include, in addition to the other contents required, a description of the facts that demonstrate that there is an emergency and how the assistance sought relates to it.

Joint investigation teams and joint investigations

By mutual agreement, the competent authorities of two or more Parties may establish and operate a joint investigation team in their territories to facilitate criminal investigations or proceedings, where enhanced coordination is deemed to be of particular utility. The competent authorities shall be determined by the respective Parties concerned.

The procedures and conditions governing the operation of joint investigation teams, such as their specific purposes; composition; functions; duration and any extension periods; location; organisation; terms of gathering, transmitting and using information or evidence; terms of confidentiality; and terms for the involvement of the participating authorities of a Party in investigative activities taking place in another Party's territory, shall be as agreed between those competent authorities.

Where investigative measures need to be taken in the territory of one of the Parties concerned, participating authorities from that Party may request their own authorities to take those measures without the other Parties having to submit a request for mutual assistance. Those measures shall be carried out by that Party's authorities in its territory under the conditions that apply under domestic law in a national investigation.

24/7 Point of contact

Each Party shall designate a point of contact that can be reached 24 hours a day, seven days a week, in order to ensure immediate assistance for investigations relating to offences related to this convention, and to obtain evidence in electronic format of an offence. This assistance shall include any action that facilitates the following measures, or their direct application if permitted by domestic law and practice:

- technical advice;
- preservation and exchange of data; and
- collection of evidence, provision of legal information and tracing of suspects.