Proposals of the Government of the Republic of Colombia concerning the provisions on international cooperation, technical assistance, preventive measures, the mechanism of implementation, the final provisions, and the preamble of a comprehensive international convention on cybercrime

---

The Republic of Colombia presents below its views on the elements that it considers should be present in the sections on international cooperation, technical assistance, preventive measures, implementation mechanisms, final provisions, and preamble of the Convention on Cybercrime under negotiation.

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

For the preparation of this text, the Colombian inter-institutional team analyzed the impact that the Budapest Convention has had on our country. This text calls to include, in our opinion, what should be improved in the field of cybercrime and thus have more instruments for the law enforcement agencies.

PREAMBULE

The member States of the United Nations recognising the value of fostering co-operation, the need to pursue, as a matter of priority, a common criminal policy aimed at the protection of society against cybercrime, inter alia, by adopting appropriate legislation, all in accordance with the Protection of Human Rights and Fundamental Freedoms.

Recalling the Security Council resolutions 2322 (2016), 2331 (2016)2341 (2017), 2396 (2017), the General Assembly resolutions 69-193 (2014), 1-S30(2016), the United Nations Convention against Transnational Organized Crime (UNTOC) 8/1(2016), 9/3(2018), 10/4 (2020), The Commission on Crime Prevention and Criminal Justice 26/4 (2017) and the Economic and Social Council 19 (2019), 21 (2019) that encourage to collect and preserve digital evidence.

INTERNATIONAL COOPERATION:

General principles relating to international co-operation. (Budapest Convention on Cybercrime. Art 23)

Principles relating to extradition:

Extradition

1. This article applies to extradition between Parties for the criminal offences established in accordance with Articles defining cyberdependant crimes and cyber dependants such as child sexual abuse, computer fraud, and personal data breach, provided that they are punishable under the laws of both Parties concerned by deprivation of liberty for a

maximum period of at least one year, or by a more severe penalty. (Budapest Convention on Cybercrime. Art 24, Num 1A)

2. The criminal offences described in paragraph 1 of this article shall be deemed to be included as extraditable offences in any extradition treaty existing between or among the Parties. The Parties undertake to include such offences as extraditable offences in any extradition treaty to be concluded between or among them. (Budapest Convention on Cybercrime. Art 24, Num 2)

3. If a Party that makes extradition conditional on the existence of a treaty receives a request for extradition from another Party with which it does not have an extradition treaty, it may consider this Convention as the legal basis for extradition with respect to any criminal offence referred to in paragraph 1 of this article. (Budapest Convention on Cybercrime. Art 24, Num 3)

4. Parties that do not make extradition conditional on the existence of a treaty shall recognize the criminal offences referred to in paragraph 1 of this article as extraditable offences between themselves. (Budapest Convention on Cybercrime. Art 24, Num 4)

5. Extradition shall be subject to the conditions provided for by the law of the requested Party or by applicable extradition treaties, including the grounds on which the requested Party may refuse extradition. (Budapest Convention on Cybercrime. Art 24, Num 5)

General principles relating to mutual assistance (Budapest Convention on Cybercrime. Art 25, Num 1 - 5)

1. The Parties shall afford one another mutual assistance to the widest extent possible for the purpose of investigations or proceedings concerning criminal offences related to computer systems and data, or for the collection of evidence in electronic form of a criminal offence.
2. Each Party shall also adopt such legislative and other measures as may be necessary to carry out the obligations set forth in the section related to the *procedures pertaining to mutual assistance requests* in the absence of applicable international agreements.

3. Each Party may, in urgent circumstances, make requests for mutual assistance or communications related thereto by expedited means of communication, via INTERPOL´S I 24/7 system, including or email, to the extent that such means provide appropriate levels of security and authentication (including the use of encryption, where necessary), with formal confirmation to follow, where required by the requested Party. The requested Party shall accept and respond to the request by any such expedited means of communication.

4. Except as otherwise specifically provided in articles in this chapter, mutual assistance shall be subject to the conditions provided for by the law of the requested Party or by applicable mutual assistance treaties, including the grounds on which the requested Party may refuse co-operation. The requested Party shall not exercise the right to refuse mutual assistance in relation to the offences referred defining cyberdependant crimes and cyber dependants such as child sexual abuse, computer fraud, and personal data breach solely on the ground that the request concerns an offence which it considers a fiscal offence.

5. Where, in accordance with the provisions of this chapter, the requested Party is permitted to make mutual assistance conditional upon the existence of dual criminality, that condition shall be deemed fulfilled, irrespective of whether its laws place the offence within the same category of offence or denominate the offence by the same terminology as the requesting Party, if the conduct underlying the offence for which assistance is sought is a criminal offence under its laws.

Spontaneous information (Budapest Convention on Cybercrime. Art 26, Num 1 - 2)

Procedures pertaining to mutual assistance requests in the absence of applicable international agreements:

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

1. Application in absence of treaty or arrangement (Budapest Convention on Cybercrime. Art 27, Num 1).

2. Central authority (Budapest Convention on Cybercrime. Art 27, Num 2a and 2b)

   2c. Each Party shall, at the time of signature or when depositing its instrument of ratification, acceptance, approval or accession, communicate to the Secretariat of the Convention the names and addresses of the authorities designated in pursuance of this paragraph; (Budapest Convention on Cybercrime. Art 27, Num 2c)

   2d. The Secretariat of the Convention shall set up and keep updated a register of central authorities designated by the Parties. Each Party shall ensure that the details held on the register are correct at all times. (Budapest Convention on Cybercrime. Art 27, Num 2d)

3. Mutual assistance (Budapest Convention on Cybercrime. Art 27, Num 3)

4. Refusal of assistance (Budapest Convention on Cybercrime. Art 27, Num 4a and 4b)

5. Postponement of action (Budapest Convention on Cybercrime. Art 27, Num 5)

6. Considerations before postponing assistance (Budapest Convention on Cybercrime. Art 27, Num 6)

7. Outcome of the execution of a request for assistance (Budapest Convention on Cybercrime. Art 27, Num 7)

8. Confidentiality of the request for assistance (Budapest Convention on Cybercrime. Art 27, Num 8)

9. Budapest Convention on Cybercrime. Art 27, Num 9a, 9b, 9c, 9d, and 9e

10. Confidentiality and limitation on use (Budapest Convention on Cybercrime. Art 28, Num 1, 2a, 2b, 3, 4)

Specific provisions

Mutual assistance regarding provisional measures

1. Expedited disclosure of preserved traffic data:

   Where, in the course of the execution of a request made pursuant to expedited disclosure of preserved traffic data to preserve traffic data concerning a specific communication, the requested Party discovers that a service provider in another State was involved in the transmission of the communication, the requested Party shall expeditiously disclose to the requesting Party a sufficient amount of traffic data to identify that service provider and the path through which the communication was transmitted. (Budapest Convention on Cybercrime. Art 30, Num 1).

2. Disclosure of traffic data under paragraph 1 (Budapest Convention on Cybercrime. Art 30, Num 2a, 2b)

3. Mutual assistance regarding accessing of stored computer data:

   1. A Party may request another Party to search or similarly access, seize or similarly secure, and disclose data stored by means of a computer system located within the territory of the requested Party, including data that has been preserved pursuant to the Expedited preservation of stored computer data. (Budapest Convention on Cybercrime. Art 31, Num 1).

   2. The requested Party shall respond to the request through the application of international instruments, arrangements and laws referred to in Article on General principles relating to international co-operation, and in accordance with other relevant provisions of this chapter. (Budapest Convention on Cybercrime. Art 31, Num 2).

   3. Answer to the request (Budapest Convention on Cybercrime. Art 32, Num 3a, 3b).

4. Mutual assistance regarding the real-time collection of traffic data (Budapest Convention on Cybercrime. Art 33, Num 1, 2).

5. Mutual assistance regarding the interception of content data (Budapest Convention on Cybercrime. Art 34).

Mechanism for implementation (Budapest Convention on Cybercrime. Art. 35)

1. Each Party shall designate a point of contact (Poc), to ensure the provision of immediate assistance for the purpose of investigations or proceedings concerning criminal offences related to the Use of Information and Communications Technologies for Criminal Purposes.

Such assistance shall include facilitating, or, if permitted by its domestic law and practice, directly carrying out the following measures:

a) the provision of technical advice;

b) b the preservation of data pursuant to Articles 29 and 30;

c) c the collection of evidence, the provision of legal information, and locating of suspects.

2. The Points of contact shall coordinate meetings (at least twice a year) to review and suggest updates of the convention and follow up on the development of cybercrime.

3. a. A Party's point of contact shall have the capacity to carry out communications with the point of contact of another Party on an expedited basis.
b If the point of contact designated by a Party is not part of that Party's authority or authorities responsible for international mutual assistance or extradition, the point of contact shall ensure that it is able to co-ordinate with such authority or authorities on an expedited basis.

4. Each Party shall ensure that trained and equipped personnel are available, in order to facilitate the operation of the network.

New language Proposals:

The Parties shall implement mechanisms to foster software design among developing countries to promote local development and computer security in public and private sectors to prevent cybercrime.

The Parties shall facilitate the dissemination of technologies necessary to improve the local capabilities of less developed countries in the fight against cybercrime. Building administrative

and technical capacities to preserve the technological developments achieved and promote new advances will be part of the cooperation programs with developing countries.

The prevention of cybercrime shall be a central element of programs to combat crime in cyberspace. The Parties shall promote the development of educational mechanisms for the public and support the development of affordable technologies capable of addressing the threats posed by cybercrime.