

Embajada y Misión Permanente de la República Dominicana en Austria

<u>COMMENTS OF THE DOMINICAN REPUBLIC ON THE SCOPE, OBJECTIVES</u> <u>AND STRUCTURE OF A NEW INTERNATIONAL INSTRUMENT ON</u> <u>CYBERCRIME</u>

The Dominican Republic welcomes the opportunity to contribute to this collective exercise with all the Member States with a view to submitting comments on the scope, objectives, and structure of a new international instrument on cybercrime, in accordance with the United Nations General Assembly resolutions A/RES/74/247 and A/RES/75/282, dated December 27, 2019 and May 26, 2021, respectively.

Cybercrime is an emerging form of transnational crime, and one of the fastest growing worldwide, whose rise is closely linked to the evolution and exponential development of information and communication technologies (ICTs), impacting every year to millions of citizens and companies.

Our region, Latin America and the Caribbean, has been particularly affected by this phenomenon. Developing countries largely lack the necessary capacities to combat cybercrime, which has a direct impact on the high victimization rates recorded.

Likewise, the recent COVID-19 pandemic revealed the vulnerabilities of the international community in terms of cybercrime, which reaffirms the importance of a global response based on collaboration and coordination, not only between Member States, but also between governments and non-governmental organizations, civil society, academia and the private sector, since the complexity and scope of cybercrime implies that any type of response must be based on a multidisciplinary approach, if want it to be successful.

The Dominican Republic enthusiastically joins this effort of the international community within the framework of the United Nations and reiterates its willingness to work together with all Member States to achieve an international treaty that represents each and every one of us, guided, at all times, by the principles of transparency, impartiality and inclusion.

SCOPE

The Dominican Republic is of the opinion that the central purpose of a new international instrument on cybercrime is to have an effective tool for the prevention, detection, investigation and criminal prosecution of cybercrime, with total adherence to respect for personal privacy, data protection, civil liberties and human rights.

In particular, this new international instrument should complement other existing instruments, facilitating criminal investigation processes, allowing the timely obtention and



Embajada y Misión Permanente de la República Dominicana en Austria

subsequent use of digital evidence, thus reducing impunity for this type of crime, this being one of the main constraints faced by law enforcement officials on the ground.

Likewise, this new instrument should promote and facilitate international cooperation between Member States and technical assistance and capacity building in the States Parties that require it in the area of cybercrime.

Likewise, the Dominican Republic is of the opinion that it should be clearly established that this new international instrument should be limited to the field of cybercrime, without entering into considerations related to cybersecurity and Internet governance, the discussion of which belong to other fora.

On the other hand, we understand that the provisions of existing international and regional instruments must be taken into consideration, in order not to enter into unnecessary contradictions with the legal systems of the Member States that have made use of said instruments as the basis of their national legislation nor with the operation of these instruments. Likewise, the experiences acquired in their implementation should be taken into consideration, identifying the strengths and weaknesses that could be complemented by the new international instrument. In the same way, the efforts of specialized groups such as the Group of Experts in charge of Carrying out a Comprehensive Study on Cybercrime should be taken into consideration.

OBJECTIVES

The Dominican Republic believes that a new international instrument for the prevention and combat of cybercrime must, among other things:

- Promote and facilitate agile, practical, and effective international cooperation among Member States.
- Cover the prevention, detection, investigation and criminal prosecution of cybercrimes to which said international instrument applies, as well as the collection and processing of digital evidence of other crimes, providing the States Parties with the necessary tools to to face this type of transnational crime.
- Clearly delimit the types of crime to which the provisions of the new convention would apply and which should be considered illegal acts in the legal systems of all States Parties.
- Promote and facilitate the development of capacities in the Member States that require it, with a view to avoiding the creation of "cyber paradises".
- Promote the exchange of good practices and lessons learned.
- Define clear rules of the game for the establishment of the appropriate jurisdiction for the purpose of requesting digital evidence from "global" internet service



Embajada y Misión Permanente de la República Dominicana en Austria

providers, which currently constitutes one of the greatest challenges with a view to reducing impunity and giving responses to victims of cybercrime.

- Establish clear safeguards and a regime of consequences in the event of non-compliance with them.
- Establish sufficient powers to investigate the criminal offenses provided for therein, always taking into account the respect of personal privacy, data protection, civil liberties and human rights.
- Use a technologically neutral language to ensure that its validity over time is not affected by technological evolution.
- Given the rapid evolution of technological developments, the convention must have a broad and long-term vision. In this sense, a technologically neutral language should be used to ensure that its validity over time is not affected by technological evolution.
- Establish a multidisciplinary approach that allows active collaboration between the public and private sectors.

STRUCTURE

- Definitions
- Criminal types
- Procedural tools for investigation
- Safeguards
- International cooperation
- Access to digital evidence
- Technical assistance and development investigation capacities
- Standardized operating procedures
- Precautionary measures
- Implementation mechanism