Permanent Mission of the Federative Republic of Brazil

Brazilian Government's position regarding the objectives, scope and structure of an international convention on countering the use of information and communications technologies for criminal purposes

As many countries, Brazil has been dealing with cybercrime, a phenomenon which is increasing in number and sophistication. The migration of various criminal offenses to digital platforms demands decisive efforts towards updating a proper normative and law-enforcement response to the threats, including internationally. Their geographical amplitude and operational speed challenge traditional mechanisms of law enforcement and legal cooperation worldwide.

Challenges are tremendous. Internet service providers, which hold important information needed to investigate cybercrime and collect electronic evidence, frequently have physical headquarters in one country, provide services in different continents and store their information on servers anywhere else on the planet. In this scenario, law enforcement strives to identify and duly address whoever has jurisdiction over the data and direct access to it.

A cohesive international coordination of jurisdictions is a necessary step forward in persecuting cybercrime. More and better cooperation is needed. Effective disruption requires agile and direct means of cooperation by which law enforcement agencies can timely share evidence from different cases involving the same criminal group.

Brazil is fully engaged in the negotiation of a comprehensive convention on countering the use of information and communication technologies for criminal purposes. It is a singular opportunity to establish common standards for cooperation in tackling such an essentially transnational issue, building on the best traditions and practice in its respect.

From the Brazilian perspective, a future Convention, in order to be capable of responding to the aforementioned challenges, shall address the following elements in terms of objectives, scope and structure.

OBJECTIVES

The main objective of the Convention should be to provide specific tools for international cooperation, so that States Parties have timely access to evidence and other information that contributes to the investigation and prosecution of cybercrime. In spite of the merit that this primary objective enjoys autonomously, the instrument should, ideally, also contemplate two other objectives: i) to establish minimum criminalization obligations (substantive criminal law) in each jurisdiction of the States Parties; and ii) to establish minimum obligations to enable timely response, investigation and prosecution (procedural criminal law) in each jurisdiction of the States Parties.

Brazil is fully committed to the idea of a universal convention. We are sensitive to the challenges of negotiating an instrument that contains minimum standards of criminalization, particularly in view of such a modern and volatile phenomenon. There are successful precedents in this direction, however. In other criminal areas, such as the existing universal criminal conventions, effective negotiations have allowed most of the world to commit to minimum substantive standards. The debate should not start from a presupposed antithesis between geographic scope and the scope of criminalization, but from the understanding that the negotiations themselves will be the safest method to obtain the best measure of the minimum possible consensus on substantive criminal law on cybercrime. As restricted as it may be, a minimum consensus on criminalization - well founded on neutral and generic concepts - could limit cybercriminals' choice of jurisdiction, facilitate the exchange of experiences and reduce normative dissensions between countries that demand application of the dual criminality principle to cooperate.

The timeliness of international cooperation will always depend on the procedural instruments available to investigators, prosecutors and judges in the most diverse jurisdictions. Nowhere can traditional instruments of legal cooperation, such as the letter rogatory and the recognition of foreign judgments, be able, by themselves, to assure an adequate reaction to cybercrime. The transnationality and extreme volatility inherent to the phenomenon demand procedural

standardization, even if it is as flexible and generic as necessary to contemplate all the specificities of the domestic legal systems involved. The core of this procedural standardization, however, should address some minimum standards in order to enable the expeditious preservation of electronic evidence, activated by an agile and direct international channel, or it will not allow the identification of criminals, especially in cases of organized crime.

SCOPE

The Convention should provide a basis for exchange of evidence and data relating to: i) crimes against computer systems; and ii) any crimes that are committed through electronic means. Ideally, electronic data related to connections, content and subscribers should be addressed.

The Convention should also allow Parties to make requests of international cooperation (for an expedited preservation of electronic data and for mutual legal assistance) and to transmit spontaneous information to other jurisdictions. A chapter would have to dedicate itself to building an international network of practitioners who would be responsible for responding to urgent cases. So operational a mechanism reinforces the understanding that such a convention requires establishing a decision-making body for monitoring and reviewing its implementation.

As a framework instrument, the treaty could establish the possibility of negotiating protocols as additional tools, which would deepen cooperation on specific cybercrime typologies.

The Convention should therefore constitute an instrument of practical criminal-law application, not delving into policy on international peace and security, cyber defense or issues relating to the structure or governance of the internet at domestic, regional or global levels.

STRUCTURE

In light of the aforementioned considerations, Brazil deems that the Convention should have the following structure:

· Chapter I: Criminalization

· Chapter II: Criminal procedural law enabling timely investigation and prosecution

· Chapter III: International cooperation

- Section 1: Expedited preservation of electronic data

- Section 2: Mutual legal assistance

- Section 3: Spontaneous information

· Chapter IV: Cooperation Network

· Chapter V: Follow-up mechanism for monitoring and reviewing implementation