Ad Hoc Committee to Elaborate a
Comprehensive International Convention
on Countering the Use of Information and
Communications Technologies for
Criminal Purposes
First session
New York, 28 February–11 March 2022

Brazil's statement on agenda item 6. Preliminary exchange of views on key elements of the convention.

Cybercrimes are the newest criminal phenomenon that is brought to the normative attention of the United Nations. More than twenty years ago, the universal criminal debate focused on transnational problems which were getting worse, but were old: corruption, organized crime, trafficking in people, drugs, firearms. At that time, entire chapters of international cooperation, if they had doctrines and practices of bilateral or regional cooperation, still were not crystallized multilaterally. Much time and energy had to be spent to achieve universal standards. Asset recovery is an example of such constructions of criminal conventions negotiated at the turn of the century.

All these transnational crimes, as well as almost all the conduct punished in penal codes, often have some cybernetic leg today. Among the cyber-dependent crimes themselves, legal interests protected and types of conduct disapproved also vary tremendously.

In this scenario, it seems clear that the only cementation between cybercrimes is their form – the cyber form –, that is, the operation of criminal offenses in the field of ICTs. It is in the cybernetic form that we believe, therefore, that this negotiating process should focus.

We do not ignore the generic pertinence, nor the legal relevance, nor the applicative ascendancy of several fundamental dimensions of international law raised here, such as sovereignty and human rights, which are not at all antithetical. They are the essential backdrop for all modern international legal cooperation, including against cybercrime. They are, however, equally fundamental for cooperation against all analogical crimes, which can only mean that, for the specific purposes of a criminal convention, there is nothing particular – or special – to negotiate about sovereignty and human rights in the fight against cybercrime. Sovereignty and human rights apply equally to cyber or analog crimes. The application of fundamental areas of international law is straightforward. It does not require any specific mediation arising from the cybernetic nature of the type of crime we pursue here.

We make this assessment pursuant to the specific instruments already in force and to the conclusions reached by the different specialized forums that have dedicated themselves to the matter, such as the group of specialists in Vienna. We should not allow this process to be contaminated by issues that are foreign to legal cooperation in criminal matters, issues whose language, doctrines and logic are sheltered by the First Committee and the OEWG, not in a forum dedicated to a strictly criminal mission.

Our human rights commitments are strong. Our proposal here is to deal with the important safeguards of human rights in the manner of private international law, with references to the fundamental principles of the requested State. There is nothing to innovate. We believe that it will also be worth including pertinent references to some human rights more directly linked to the cybernetic form, in order to facilitate the interpreters' access to the main concerns raised in the abstract by certain clauses. We anticipate, for example, due to the very nature of the cybernetic form, a reference to the human right to privacy. We do not, however, deem it necessary, nor convenient, to spend time and energy to re-discuss the content of this human right or any other human right, a matter that is alien to the purposes of this process and the vocation of this forum.

Under the broader concerns of sovereignty, we believe that the matter that warrants our main attention lies in the area of jurisdiction and the issue of possible exceptions to territoriality in matters of international distribution and coordination of jurisdiction against cybercrimes. Sovereign equality, territorial integrity and non-intervention are undisputed and immovable pillars of international law, but they do not seem to us to dialogue with particular relevance in the strictly criminal area.

In short, we must make use of the contents that the relevant fundamental areas of international law have acquired elsewhere, in the appropriate fields and forums, and use them here as presupposed references, without intending to revisit them as such. We see no substantive need, nor procedural adequacy in efforts to revisit here, in a convention negotiation on the criminal use of ICTs, what sovereignty and any human rights mean. It will suffice to recognize that they apply, as they stand today, to cooperation to prevent and repress cybercrime.

The core of this convention seems to us to be as simple in form as decisive in content: in an agreed mechanism of legal cooperation as expeditious as cybercrimes themselves (cyber-dependent and cyber-enabled), which procedural powers must Central Authorities and competent authorities have in common in order to be able to efficiently preserve the electronic data of interest to foreign counterparties so that it is duly accessible when the proper times of criminal proceedings manage to catch up with it and make use of it as evidence?

If we concentrate on this core question, we will not have to dedicate ourselves much to legal definitions or technical issues. In our view, our task here is, above all, how to adapt classic international legal cooperation to the specific challenges of the cyber form of criminality, be it cyber-dependent or cyber-enabled.