**REPÚBLICA DE ANGOLA**

# POSITION OF THE REPUBLIC OF ANGOLA REGARDING ON A FUTURE UNITED NATIONS CONVENTION ON COUNTERING THE USE OF INFORMATION AND COMMUNICATION TECHNOLOGIES FOR CRIMINAL PURPOSES, PURSUANT TO RESOLUTIONS 74/247 AND 75/282 OF THE GENERAL ASSEMBLY OF NATIONS UNITED

With the emergence of new information and communication technologies, the first trends of misuse began to emerge and, consequently, legal issues associated with the use of information and communication technologies on a global scale.

The rapid evolution of these new technologies led to the existence of legislative gaps and the difficult definition of cybercrime on the one hand, and the initiatives to legislate on the matter, which should be coordinated and harmonized internationally, given its global dimension, became seen as an exclusive matter of domestic law, on the other hand.

The Republic of Angola, like most States in this global era, has faced an enormous challenge in combating the use of information and communication technologies for criminal purposes.

Modern societies are increasingly connected virtually through computer networks and information systems, so institutional relationships, the interaction between citizens and public and private institutions, as well as interpersonal relationships are increasingly carried out by electronic devices, using cyberspace, which leads to the natural migration of criminal practices to that sphere, either by committing traditional crimes in a digital environment, or by committing completely new crimes that are only possible through the use of information and communication technologies .

The crime situation in general, in itself already worrying, has experienced considerable growth with the practice of cybercrimes

in the last two years, due to the Covid-19 pandemic situation, which forced the country to declare a state of emergency and calamity, leading to home confinement and teleworking and, consequently, the massive use of information and communication technologies.

Although Angola has made some progress in terms of domestic legislation, with the inclusion of legal types of computer crimes in the New Angolan Penal Code in force, the challenges prevail, above all, because these are highly technological crimes, with a strong tendency towards organized crime and transnational, insofar as criminal acts are often carried out from other States or by groups located even in several continents, using information and communication technologies to identify their targets.

Collecting electronic evidence for the investigation and criminal prosecution of cybercrime agents brings with it several challenges. On the one hand, the lack of harmonization of both substantive and adjective laws of the States, to make possible the indispensable international cooperation in this matter, on the other hand, the need to provide law enforcement officers with technical knowledge so that they can successfully investigate and prosecute cybercrime agents.

Therefore, Angola is fully engaged in international efforts to create legal instruments aimed at combating this phenomenon that threatens social peace at an international level and applauds the present initiative to draft an International Convention on the Use of Information and Communication Technologies for Criminal Purposes, under the aegis of the United Nations.

## OBJECTIVES

- Encourage the adoption of policies and actions to increase the digital literacy of citizens in order to prevent them from becoming victims of cybercrime due to negligence or ignorance of the rules for using information and communication technologies safely.

- To be the most relevant international legal instrument in the global strategy to combat cybercrime;

- Be prepared in such a way as to keep up to date with the constant evolution of information and communication technologies.

- Provide rules for the harmonization of domestic legislation on cybercrime and electronic evidence;

- Safeguard the principles of equality and reciprocity between States with regard to the practice of collaboration in obtaining electronic evidence, recovery of assets, among others, respecting fundamental rights, freedoms and guarantees, as well as the protection of personal data.

- Focus on international cooperation, mutual legal assistance and capacity building of law enforcement officers as the most effective way to combat cybercrime and create swift and effective mechanisms for cooperation.

## SCOPE

• The Convention should define clear principles and rules on jurisdiction based on territory and jurisdiction, as the cybercrime phenomenon transcends current concepts of territory, space and jurisdiction;

• The Convention should contain a set of precise definitions of technical terms whose interpretation is ambiguous, using, whenever possible, technologically neutral language in the definitions;

• The Convention should identify and make effective the mechanisms and forms of cooperation between the authorities that investigate and prosecute cybercrime and the technological industry, the so-called technological giants, in a global perspective;

- The Convention should typify and criminalize the most serious conduct of cybercrime, especially when they affect critical infrastructure, classifying them as cyberterrorism or crimes against humanity and define priority and urgent rules of international cooperation for investigation and prosecute of its agents;

- The Convention should typify and criminalize cybercrime conducts involving cryptocurrencies and crypto-assets for the financing of terrorism and money laundering;

- The Convention should have as its focus and common understanding, the ability to offer specific tools for effective international cooperation, so that timely access to electronic evidence and other information that contributes to the investigation and suppression of cybercrimes, giving priority to the means cooperation expedients, safeguarding the principle of equity between States;

- The Convention should identify the means of obtaining electronic evidence for both the investigation and prosecution of cybercrime and other types of crime.

## STRUCTURE

With reference to the above considerations regarding the objectives and scope of the future Convention, the Republic of Angola agrees on the structure approved in the first negotiation session of the future United Nations Convention on Combating the Use of Information and Communication Technologies for Criminal Purposes, namely:

1. **Preamble;**
2. **General Provisions;**
3. **Criminalization;**
4. **Procedural Provisions and Law Enforcement;**
5. **International cooperation;**
6. **Technical assistance and including exchange of experience;**
7. **Preventive Measures;**
8. **Mechanisms of Implementation;**
9. **Final Provisions.**

Regarding the 2nd Negotiation Session of the Ad Hoc Committee, for which State contributions are requested regarding the Preamble, General Provisions, Criminalization and Procedural Provisions and Law Enforcement, the Republic of Angola proposes the following:

| Preamble |
| --- |
| The future Convention cannot ignore the existence of regional and international legal instruments that deal with similar and related matters, so it should, whenever possible, be in harmony with the following instruments: African Union Convention on Cybersecurity and Protection of Personal Data (**Malobo Convention**), Council of Europe Convention on Cybercrime (**Budapest Convention**), United Nations Convention against Transnational Organized Crime (**UNCTOC**) and United Nations Convention Against Corruption (**UNCAC**). |

| General Provisions | |
| --- | --- |
| **Definitions** | Cybercrime, electronic evidence, interception, computer system, computer data, metadata, traffic data, service providers, computer program, electronic communications network, critical infrastructure, topography, semiconductor product, cyberspace sovereignty. |
| For the elaboration of the concepts suggested here, it is possible to resort to the regional and international legal instruments mentioned above. | |

| Criminalization | |
| --- | --- |
| **Cyber-dependent crimes** (crimes against the confidentiality, integrity and availability of computer system and data) | Illegal access, illegal interception, damage to computer data, computer sabotage, computer falsity, illegal reproduction of a computer program. |

| | |
|---|---|
| **Cyber-instrumental crimes** (traditional crimes committed using information and communication technologies) | *Online* scams, phishing, *online* economic and financial crime, *online* identity theft, sexual abuse and exploitation of children *online*, Cyber-bullying, Cyber-stalking, revenge porn, cyberterrorism. |
| For the construction of the concepts of these legal types of crimes, it is possible to resort to the regional and international legal instruments mentioned above. | |

| **Procedural Provisions and Law Enforcement** | |
|---|---|
| **Means of Evidence** | Documentary evidence (electronic document, digital document), expert evidence (computer expertise). |
| **Means of Obtaining Evidence** | *Online* searches, expeditious preservation of data, expeditious disclosure of data, injunction to submit or grant access to data, search of computer data, seizure of computer data, seizure of electronic mail and recording of communications of a similar nature, interception of communication, actions hidden (*deepweb* and *darkweb*). |
| **Recovery of Assets and Loss of Assets in favor of the State** | Seizure and confiscation of traditional assets and crypto-assets. |
| The provisions of this chapter should apply to the investigation and criminal prosecution of agents of traditional crimes and not just to the investigation of cybercrimes. | |
| For the elaboration of the concepts related to this chapter, it is possible to resort to the regional and international legal instruments referred to above. | |