LEINOTECH
Legal Innovation Technology

Andisheh Varzaneh Fanavari Tanzimi

Andisheh Varzaneh Fanavari Tanzimi (Leinotech) Contribution for the Fifth Intersessional consultation of Ad Hoc Committee to Elaborate a Comprehensive International Convention on Countering the Use of Information and Communications Technologies for Criminal Purposes

Islamic Republic of IRAN - Private Sector

20-21 June 2023

General Provisions

As regard to second question of General Provisions, for obtaining the best result of the implementation of the new convention, we are suggesting to use the term "use of information and communications technologies for criminal purposes" and the term "computer and communication systems". Using these terms will help us to have a proportionate scope that won`t be dysfunctional through decades.

On question 3 and 4, we are suggesting to member states to follow the same approach as the previous universally agreed conventions, like UNTAC and UNCAC, mentioning the respect to fundamental rights and compatibility with the Charter of the United Nations in the preamble section.

Criminalization

On the Criminalization, regarding question 6, we are of the opinion to include traditional crimes facilitated or committed by means of ICT devices in a limited scope so as to avoid a very large list of crimes that is hardly possible to be agreed on.

As regard to question 8, in general, we propose to member states so as to recognize not only the criminal, disciplinary or administrative liability for natural and legal persons, but also the liability arising from the act of the object and the liability for AI entities -robots- that may have a large presence in the near future.

On Questions 9, we believe that criminalization provisions should be on the basis of Criminal Justice Principles and the referral to fundamental rights and compliance with the Charter of the United Nation in the Preamble section governs the entire convention.

As regard to question 10, we are of the opinion that at these circumstances, member states may consider that the crime is aggravated:

A. being organized, whether at the domestic or international level;
B. the affiliation of the data or system to governments or national and transnational institutions providing public services;

C. the actual use of crime target data and systems in vital and critical national and transnational infrastructure and services;
D. committing a crime as a profession or a habit, whether with the intent of earning money or not;
E. the extent of the effects of the crime, whether the greatness of its expansion is domestic or international and in cyberspace or real space;
F. the high number of victims, whether they are citizens of one or more countries;
G. the abuse of the victims' weakness or vulnerability due to having a special social, mental, psychological, physical or sexual status in a way that has facilitated the commission of the crime or resulted in the severity of its effects;
H. the anonymity of the perpetrator in cyberspace during the commission of the crime, in such a way that it is not possible for the victim to identify him/her.

We are of the opinion that the most effective way to implement the Procedural Measures, Law Enforcement and International Cooperation is to give Interpol a central role so as all parties and even stakeholders, specially service providers, could have neutral and appropriate ground for cooperation to combat cybercrimes, noting that Interpol has qualified human resources and technical equipment, and more important, acting neutrally.

Preventive Measures

On the Preventive Measures, we believe that member states should have great attention to production and distribution of awareness-raising and general training content for common and current cyber threats (digital literacy promotion); (the main cause of vulnerability of users in this environment is due to their lack of awareness or fallacious awareness of the above threats).

Providers of intermediary services, such as platforms, which provide the infrastructure and applications, have Due Diligence obligations to combat cybercrimes and shall participate in the following:

- Authenticating real cyber actors and updating their identity information;
- Authenticating the legal competence of cyber actors, especially for sensitive processes and transactions, such as big data processing and electronic financial transactions;
- Requiring cyber actors, especially businesses and services active on the platform, to have a specialized and dedicated cybercrime prevention policy, code of conduct and ethical charter(s);
- Producing and distributing appropriate warning/precautionary content to prevent delinquency or victimhood of platform operators, especially as cybercrime threats become imminent;

- Continuous monitoring of criminal and incident-prone zones, as well as identification of suspicious criminal procedures and processes on the platform, especially serious crimes, in accordance with the infrastructure and specialized and dedicated functions of the platform;
- Providing technical and technological tools for the prevention of crimes that can be committed on the platform for the actors or guiding the actors on how to provide these tools safely and cost-effectively;
- Providing the technical and legal possibility of temporarily restricting or depriving actors of the access to the platform to prevent delinquency or victimhood, in particular by setting up and managing a dedicated system for immediately responding to cyber threats; and
- Making the platform's lines of communication accessible and interactive with operators and those responsible for cybercrime prevention, both for themselves and the platform's actors.

Cyber businesses that offer a variety of digital or physical goods and services to customers or consumers in cyberspace or through this space shall participate in the following:

- Refusing to provide goods and services to customers or consumers without identity or with a false identity;
- Operating only on platforms or in authorized computing spaces;
- Refraining from cooperating with unauthorized businesses in any way;
- Refraining from supplying goods or services that are typically and generally used to commit crimes or, in a regulated manner, make them available only to qualified persons;
- If the safe and secure utilization of goods or services requires the use of technology or the implementation of a special preventive process, cyber businesses provide the necessary information or training to their customers and consumers; and
- Refraining from disclosing their data and information, especially related to their customers or consumers or partners, to unauthorized persons.