LEINOTECH
Legal Innovation Technology
Andisheh Varzaneh Fanavari Tanzimi

Andisheh Varzaneh Fanavari (Leinotech) Participation for the Fourth Session of the 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

11 January 11, 2023

Towards an integrated international cybercrime policy: from an issue-based strategy to a macro-view approach

From the beginning of the emergence and distribution of Information and communication technologies, they basically had a "tool" function; therefore, they were designed and built based on their scope of application and efficiency; a good illustration of them are accounting software and fixed communication software, each of which had wide applications in their own place, but there was still no opportunity for their full-fledged link and connection .

In this way, what has caused the emergence and development of new and innovative concepts such as e-banking, payment systems, financial technologies and now "Internet of Value", is the inevitable correlation of cyber worlds with the help of global convergent technologies, especially cloud computing, big data analysis, Internet of Things, distributed ledger technology, and artificial intelligence. Therefore, considering human "civilization-building" and "future-building" technologies that can define and determine our destiny in a completely different and distinct way from history, cannot be a way forward and will have adverse consequences.

Perhaps the "tool-oriented approach" to computer and telecommunication hardware and software still seemed justified until a decade ago. But since this time and with the expansion of social networks and various platforms that aggregate and at the same time analyze global digital services, we have faced the integration and even unity of many different applications and uses. Nowadays, few people are looking for an accounting software; instead, they try to use an accounting service or beyond that, use a corporate management, which are also online and based on all kinds of new convergent technologies.

In such a situation, what is the mission and responsibility of criminal justice systems, especially global coordinating systems such as the United Nations? Is it going to retrace the same path that was followed two decades ago in regional and international treaties to fight computer and telecommunication crimes, or is it going to build and provide its followers with a new path that is smoother, shorter and more reliable?

For an efficient and effective fight against cybercrimes, especially at the international level, relying on traditional issue-oriented and example-oriented solutions is no longer the answer, and policy makers and criminal policy researchers must upgrade their perspective to the macro and strategic level. In order to form an integrated and coordinated international system to fight against cybercrimes, instead of naming a few harmful actions or omissions that hurt

one or more cyber beneficiaries by targeting individual values, the fundamental values of the interactive arenas of global actors should be supported and protected by cybercrime.

In this way, the first step is to identify the interactive consensus areas of global cyber actors. As a general proposal, these areas can be divided into the following 8 sections: 1. Political-Administrative, 2. Security-Defense, 3. Economic-Commercial, 4. Industrial-Technological, 5. Cultural-Social, 6. Health and welfare, 7. education and research and 8. legal-judicial. Then, the fundamental values governing each of them, which are subject to the consensus of the global cyber community, should be listed. For example, in the economic-commercial sector, national criminal justice systems must support and protect values such as the right to own digital assets, healthy, transparent and competitive activity, the dignity of users and their personal data, as well as guaranteeing public income from digital markets. Now, the question regarding which behaviors or omissions in their national criminal law system should be taken into account in order to achieve such a goal, depends on different and distinct components and criteria that the international cybercrime policy document does not seem to be the right place to resolve. Incidentally, it can assign them to bilateral or multilateral treaties of similar and homogeneous countries. It is important that this international document requests and demands the adherence of countries to these values, that is, a full-fledged cyber-criminal protection.

Regarding the generalization and expansion of cyber-criminal justice to "legal entities" in order to complete and consolidate the criminal protection of cyber beneficiaries, the fact is that if such an emphasis was practical two decades ago, today it is not paid much attention by the beneficiaries of various cyber ecosystems and any activist who is able to gain the "trust" of others more than others, would receive the flood of capital and the material and spiritual benefits flows towards them. For example, is the creator of Bitcoin a natural person or a legal entity? Did the millions of users who trade this digital asset around the world think about this first and then buy and trade it, or do they rely on reliable and trustworthy cyber technological mechanisms?

The development of "Procedural" systems of cyber international criminal law also requires fundamental revisions in legal-governance insights and attitudes. In the "Criminal Jurisdictions" section, the feasibility of new cyber realms for national governance systems instead of relying and emphasizing traditional physical rules and mechanisms can be much more enlightening. As a general suggestion, the theory of "layered territories" can be used as the basis of national cyber-criminal jurisdiction; in the sense that unlike physical worlds where national sovereign territories only make sense next to each other, cyber territories can be placed on top of each other in accordance with the layers of infrastructure, platforms, services and content, and each of the countries that is responsible for the governance affairs of the layer in question has the relevant criminal jurisdiction. In addition, in such an assumption, the possibility of applying transnational cyber competences, i.e. citizenship, protection and global competencies, is provided in a more efficient and effective way.

Regarding the admissibility of digital data in the cyber-criminal justice system, many measures should be taken in the organizational, structural and mechanism sectors. From the training of manpower to the provision of network hardware and software equipment and facilities, as

well as the promotion of legal digital literacy of citizens and cyber activists, all are of fundamental importance in their place. The result of all this is the establishment of a "forensic computing organization" - like the forensic medicine organization that many countries have gained valuable experiences from. Not only can this organization provide judicial courts and law enforcement with valuable expert services in the analysis and evaluation of electronic evidence, but also it plays an effective role in the standardization and development of the "chain of protection" requirements for processors and owners of big data, especially in sensitive areas of various fields.