LEINOTECH
Legal Innovation Technology
Andisheh Varzaneh Fanavari Tanzimi

Andisheh Varzaneh Fanavari (Leinotech) Statement on Criminalization for the Second Session 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

1 JUNE 2022

According to our proposed detailed Draft (including General Provisions, Provisions on Criminalization, Procedural Measures and Law Enforcement) that has been previously submitted on 8 April 2022, the principles on the chapter of criminalization are as follow:

1. Any international cyber criminalization and punishment must be in accordance with the principles of the consensus of modern criminal law, including the principle of legality of crimes and punishments and the principle of minimum criminalization.

2. On the one hand, cybercrime should not be so limited and narrow that it includes only a few cyber-dependent crimes; and on the other hand, it should not be considered so broadly that any traditional crime that is somehow committed by computer and communication systems could be included. Therefore, while balancing these two approaches, we should not ignore the behaviors that disrupt domestic, national, regional and international order and security, and behaviors that violate fundamental human rights and cultural, social, economic and even environmental values in criminalization.

3. In criminalization, in addition to paying attention to the main conduct that violates the aforementioned values, Parties should also pay attention to the criminalization of anterior and posterior conduct, which in any way facilitates the commission of the above conduct, like the lack of valid cyber identity.

4. Regarding the semantics of crime, the existence of violations should also be considered, which means reprehensible behaviors whose titles are defined by the "legislator" and whose instances are defined by the so-called "regulatory" authorities. This issue is of particular importance in cybercrime policy, and for various reasons, the prevention and response to cybercrime is left to the "regulatory" authorities. Therefore, it may be necessary to use terms to reflect the semantics of cybercrime, which also include violations (like “offence”). However, the inclusion of violations in the extent of the semantics of crime should not impede adhering to the principles enshrined in modern criminal law and lead to the unlimited expansion of the criminal scope.

5. On the other hand, in proportion to the establishment of conduct as crimes or offences, sanctions, both criminal and disciplinary, should be appropriate in terms of type and severity, appropriate to each of these two groups and in line with the initial objectives of prohibiting this conduct. Therefore, Parties should move away from mere reliance on traditional punishments (such as imprisonment) and enjoy new, cyberspace-compliant sanctions (such as deprivation of Internet services).

6. Qualities that can in any way increase the risks and harm of cybercrime, including the existence of terroristic purposes or organized form of crimes, should be considered as aggravating qualities.

7. In addition to criminalization and punishment, criminal, disciplinary and administrative liability should be provided in such a way that, besides the "liability of natural and juridical persons" and "liability arising from the act of things", it should include the liability for AI entities -robots, which may arise in the near future.

8. Due to the widespread harm and damage that cybercrime can cause, negligence in prescribing the civil liability of the above persons will, in practice, negate the objectives of the Convention. Therefore, regardless of criminal, disciplinary and administrative liability, the methods of compensation for material and moral damage resulting from cybercrimes and offences should also be specified.

9. Regarding the above-mentioned principles, it is worthwhile to take these following crimes and offences into consideration in the chapter of Criminalization:

   Article 4- Unauthorized access
   Article 5- Unauthorized interception
   Article 6- Data destruction and interference
   Article 7- Computer and communication systems destruction and interference
   Article 8- Impeding legal freedom of access to cyberspace
   Article 9- Digital forgery
   Article 10- Misuse of technological means
   Article 11- Training, facilitating and expediting the process of committing cybercrime
   Article 12- Unauthorized cyber border crossing
   Article 13- Cyber espionage
   Article 14- Incitement to commit subversive activities
   Article 15- Cyber theft
   Article 16- Crimes related to digital identities and personal data
   Article 17- Cyber fraud