Andisheh Varzaneh Fanavari (Leinotech) Statement on Procedural Measures and Law Enforcement 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

8 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 procedural measures and law enforcement are as follow:

1. Due to executive mechanisms, this section includes a great many of keywords and terminologies, narrow definitions of which are necessary so as to reduce ambiguities and elucidate the terms as much as possible as well as providing the principle of legality of jurisdiction and criminal procedures. Hereafter the required terminologies will be addressed.

2. At the beginning of procedural measures, we deal with "jurisdiction", classified into the hierarchy of "legislative jurisdiction", "judicial jurisdiction", and "law enforcement jurisdiction". What these jurisdictions have in common is their meaningful connection with "national sovereignty". Hence, to tackle the jurisdiction-related section of the procedural measures and law enforcements, as stated in the general provisions of the Convention, it is firstly necessary to elaborate on cyber "territory" and "nationality".

3. With regard to "territorial jurisdiction" which is defined on the basis of "territory sovereignty", not only is it necessary to consider physical criteria such as the location of infrastructures, stations and communication and information technology systems, but also close attention should be paid to cyber criteria, such as defining Country Code Top-Level Domain (e.g., ir) as its national flag, as well as other technical criteria based on which we could adjust or at least make cyber territory closer to physical territories.

4. With regard to "personal jurisdiction", which is applied to "persons", besides "natural and legal persons", we should also define "AI entities", since they are very likely to be directly subject to judicial and law enforcement orders. Therefore, their nationality and adherence to their sovereign legislation must be clarified.

5. With regard to “protective jurisdiction” that applies to "critical assets of countries", it is necessary to agree on a specific list, such as data and operating systems supporting governmental and national technological infrastructures, the damage of which seriously undermines national order and security. This jurisdiction should be envisaged comprehensively and, especially, cover the political and economic sensitive points of the countries.

6. Regarding "universal jurisdiction", the emphasis should be on the "common cyber world heritage", which can be considered from different aspects; any threat that the international community considers to be a threat to this common heritage can be included in this list, such as cybercrime against children and other vulnerable people as well as cyber terrorism.

7. With regard to “domestic jurisdiction”, countries should undertake to revise and, if necessary, reproduce the relevant laws and regulations in such a way as not to prejudice the application of the provisions of the Convention. "Local" or "specialized" jurisdictions defined for the authorized courts, as well as law enforcement, must be able to comply with the authorization of the Convention and be able to uphold them without interruption.

8. Since the presumption of "conflict of jurisdiction", both "positive conflict" and "negative conflict" is quite probable, it is necessary to take the necessary measures to prevent the occurrence and, of course, to resolve it immediately and decisively. In any case, countries must commit that positive or negative conflict of jurisdiction should not be used as an excuse for non-cooperation or non-fulfillment of their procedural measures and law enforcements, and they must faithfully play their role as an independent and responsible member of the universal cyber community in combating cybercrimes until the objectives of the Convention are achieved.

9. Regarding the procedural and law enforcement provisions relating to "electronic evidence", the first undeniable principle is that the evidence is the same as "data" and "information". Therefore, in the first step, the main sources of data and information must be identified; resources that, by having access to them in due time, could fulfill the tasks set out in the Convention. It goes without saying that large cyber service providers, including providers of communication infrastructure and information technology services, especially platforms, messengers and financial and reg-tech services are recognized as the primary sources of electronic evidence. This

in itself proves that the "criminal management" of cyber data and information is a defining and undeniable common duty.

10. In directing the criminal management of electronic evidence, the role of service and government players should be specified separately. Since granting unauthorized powers to players such as cyber service providers can lead to loss of confidentiality and abuse of data transmitted and stored in cyberspace, their cooperation and role-playing should only be under the supervision and order of the judiciary, being done in accordance with the law.

11. The first topic of criminal management and management of cyber data and information is the definition and determination of conditions and requirements governing their "storage" and "retention". However, due to the diversity of data and information and their different levels of importance and sensitivity in the cybercrime system on the one hand and their associated costs on the other hand, it is necessary for all stakeholders to be identified and categorized in order to meet the requirements of criminal measures and arrangements, as well as bearing the lowest cost and damage for the beneficiaries. For instance, "traffic data" and "user/subscriber information" are amongst the key data to solve cybercrime cases and contain much less volume than "content". However, mere access to traffic data and user information is not necessarily the solution, and there must be a logical balance between the rules and requirements of the first and second groups of cyber information – the first one being “traffic data” and the second one being “content”. Nevertheless, the criminal justice authorities of countries, including courts and law enforcement, must be vigilant enough to meet their data and information needs in the shortest possible time so that limited resources can be dedicated and acted upon to optimally manage unlimited data and information.

12. One of the measures that can largely meet the considerations and expectations of the relevant authorities as well as stakeholders is to anticipate the status of "expedited preservation" of data and information. This special situation only burdens a certain group of data and information and, of course, does not impose unnecessary costs and effort on those in charge. In addition, this situation is temporary and must be assigned within the given period and can only be extended for one other period. The "expedited preservation" rule is particularly effective in preventing the partial or total destruction or vulnerability of content whose binding "storage" and "retention" interval is much shorter than "traffic data" and "user information".

13. The admissibility of electronic evidence in international cybercrime policy can achieve the set objectives only if the data and information in question have three characteristics: 1. integrity; 2. availability; and 3. confidentiality. Damage to any of these can shatter the foundations of this principle and consequently make cybercrime policy in vain and ineffective. Achieving such a goal requires having "integrated" and, ideally "unique" universal standards and criteria, in such a way as to provide the highest level of "credibility", "trust" and "confidence" in the judicial and law enforcement authorities for the proper administration of justice.

14. The development of integrated and unique global criteria and indicators for the admissibility of electronic evidence requires the knowledge of the "processing chain" of data and information; meaning that from the time data and information production to the time they are irreversibly destroyed, this process must be based on unified global standards and indicators, and if any of the links in this vital chain of electronic evidence is ignored, the criminal policy system can cause serious troubles for international criminal policy system.

15. In parallel with the "processing chain" of data and information, the "chain of custody" of electronic evidence must be designed and defined. Obviously, the beginning of this chain goes back to before "storage", "retention" and "expedited preservation" of data and information, and it ends with the "retrieval" and "presentation" of electronic evidence to the judicial and law enforcement authorities. Hence, countries have a duty to carefully identify the starting points of this chain and to establish their connecting links.

16. With regard to the provisions of "search" and "seizure", it is necessary to consider the two categories of "data and information" and "systems, devices and tools of computer, communication, digital and electronic", both "independently" and "comprehensively". Sometimes, the search and seizure of data and information is independent of the systems, and sometimes it involves each other, and the terms and conditions of each must be anticipated and assigned separately.

17. In the implementation of "search and seizure" of data and systems, compliance with the three principles of "necessity", "accuracy" and "appropriateness" is mandatory. As far as possible, we should be confined to the necessities and avoid access to indefinite and unknown sources. In addition, there must be a reasonable appropriateness between the seriousness of crime or charges and the type and amount of data and systems subject to search and seizure. Therefore, the use of

accurate search software (both hard and soft) to evaluate the first data available in the target systems is of particular importance and reduces undue harm to stakeholders. The "seizure" of the system or data should only be implemented where there is no other way to protect the evidence.

18. Real-time collection (interception) of electronic communication content requires compliance with special regulations and should be limited to specific circumstances and crimes. This means it should be prescribed only where it is not possible to prove the accusation by other means or if the crime in question is so serious that it is necessary to identify and arrest the perpetrators as soon as possible.

19. Providing and ensuring the validity and reliability of electronic evidence resulting from the search and seizure of data and systems and real-time collection of content-related crime require comprehensive and accurate "documentation" of the "processing chain" and "chain of custody" of electronic data and evidence by authorized governmental and service players. It must be noted that in enforcing the rules and requirements of "documentation", the so-called "controller" and "processor" players have the same level of responsibility and even beyond the "law enforcers", and any negligence or fault must be guaranteed with decisive and deterrent responses.

20. In defining and implementing the procedural measures of the cybercrime Convention, it is essential to strike a reasonable balance between "sovereignty considerations" and "public interests" on the one hand, and "fundamental human rights" on the other. Rights such as "ownership" and "dignity" must be carefully defined and their various aspects in conflict with the rules and regulations of the Convention must be weighed and evaluated. For example, when organizing data and information sources, the necessary distinction must be made between the "owner" and the "subject" of the data and information. Even if communication and IT service providers "own" data and information, they will certainly not be their "subject" and the necessary legal and regulatory mechanism for obtaining "explicit prior consent" from the subjects (i.e. users/subscribers) should be provided for the application of the relevant executive rules and requirements. Also, regarding the protection of "privacy" and "personal information", it is necessary to explain the relationship between this “sphere” and the information with "public sphere and information" so that law enforcement on the one hand in the strict rules of access to data and personal information in privacy do not be trapped; and, on the other hand, holders of the right to privacy and personal information be assured of the proper protection of their legitimate rights and freedoms.

21. In addition to prescribing the enforcement of civil, disciplinary, and criminal sanctions for breach of the above-mentioned electronic evidence standards, another mechanism that can somehow guarantee "fundamental human rights" in the procedural measures and law enforcement of the Convention is that the "right to object" should be considered for beneficiaries in any of the above measures, from storage and retention to search and seizure of data, information and systems.

22. "Achilles heel" for procedural measures and law enforcement of the International Convention against cybercrime is that the structures, the organizations, the mechanisms and the systems, either physical or electronic, which are responsible for the Convention in accordance with domestic laws and regulations, are mainly “worn out”. Countries must commit themselves to making the necessary efforts to "modernize" their fleets and "empower" their manpower within the stipulated timeframe, and to define and implement legal and regulatory requirements based on national "government/e-government" strategies to operate in a safe and secure environment of electronic communications and exchanges, in the shortest time and at the highest level of domestic interaction. In this case, it is hoped that the rules governing transnational cooperation can be properly implemented and it is expected that to achieve this objective, the countries with technology do the necessary cooperation to improve the quality and quantity level of the countries that use technology.

23. Regarding the above-mentioned principles, it is worthwhile to take these following main subjects into consideration in the chapter of Procedural Measures and Law Enforcement:

Article 35- Scope of procedural provisions
Article 36- Jurisdiction
Article 37- Rules governing electronic evidence
Article 38- Collecting, storing and maintaining traffic data and logs
Article 39- Interception of the content being transmitted by non-public communication
Article 40- Expedited preservation and maintenance of data
Article 41- Presenting and making available the data
Article 42- Search of data, cloud computing and computer and communication systems
Article 43- Seizure of data, cloud computing and computer and communication systems
Article 44- The right to object