SECTION I – CRIMINAL LAW. GENERAL PART

The participants in the XIXth International Congress of Penal Law, held in Rio de Janeiro from 31 August to 6 September 2014;

Considering that people's lives in the 21st century are heavily influenced and shaped by information and communication technology (ICT), as well as by the opportunities and risks offered by information society and cyberspace, and that therefore crimes in these areas affect important personal and collective interests;

Building on the draft resolutions prepared by the participants of the Preparatory Colloquium for Section I held in Verona on 28 – 30 November 2012;

Recognizing that states and international organisations have made considerable efforts to define and prosecute offenses that may affect the confidentiality, integrity and availability of ICT networks and cyberspace, as well as the interests of persons in these areas;

Keeping in mind that any overextension of criminal repression in these areas creates risks, especially for the freedom of expression and of receiving, collecting, processing and disseminating information;

Defining ICT networks as systems that make possible the acquisition, processing, storage and dissemination of audio, visual, textual, and numeric information through computer or telecommunication networks; and cyberspace as any space of communication conducted with the aid of such ICT networks;

Referring to valuable international instruments seeking to guide and coordinate efforts and to harmonize legislation, for example, the Budapest Convention on Cybercrime of 23 November 2001, the E-Commerce Directive 2000/31/CE, and the EU Directive 2013/40 of 12 August 2013, the Arab Convention on Combating Information Technology Offences of 2010, the Shanghai Cooperation Organization Agreement on Cooperation in the Field of International Information Security of 2010, and the draft African Union Convention on the Establishment of a Legal Framework Conducive to Cybersecurity in Africa of 2012;

Recalling the importance of protecting human rights, as well as of respecting basic principles of criminal legislation and adjudication, such as the principle of ultima ratio, the principle of legality, the harm principle limiting criminalization to conduct that is directly harmful or concretely dangerous to personal or collective interests, the principle of culpability, and the principle of proportionality;

Building on the debates and resolutions of past International Congresses of Penal Law, especially the resolutions of the XVth International Congress 1994 in Rio de Janeiro, Section II, on computer crimes and other crimes against information technology;

Have adopted the following resolutions:

A. General considerations for criminal legislation

1. ICT networks and cyberspace have created specific interests that need to be respected and protected, for example, privacy of individuals, confidentiality, integrity and availability of ICT networks, and integrity of personal identities in cyberspace. Perpetrators of some traditional crimes, for example, fraud, forgery and copyright violations, make use of ICT networks and cyberspace, thereby increasing the dangerousness of their conduct. Legislatures, courts and criminal justice systems need to accept the challenge of continuously adapting to this situation.

2. Because confidentiality, integrity and availability of ICT networks and of cyberspace are vital for individuals, as well as for the media, and harmful or dangerous conduct in these areas can affect important interests, states and international organisations should continue to devise effective policies with respect to protecting ICT networks and the interests affected. Such policies should respect human rights and be consistent with basic principles of criminal legislation, including the principle of proportionality. They should continually be kept up to date in order to prevent new forms of harmful or dangerous conduct. Empirical and technical research should be encouraged and funded in order to assist legislatures in these areas.

3. On the other hand, excessive regulation and overcriminalization of cyberspace should be avoided because it jeopardizes the very freedom of communication that is the hallmark of cyberspace. Legislatures should be aware that the regulation of conduct, the establishment of criminal laws and the imposition of disproportionately restrictive control measures in cyberspace may interfere with human rights, especially the freedom of expression and of receiving, processing and disseminating information.

4. Legislatures should not criminalize conduct that only violates religious or moral norms. Criminal policy should be consistent with the harm principle. Legislatures should therefore not criminalize conduct that does not harm or create a concrete danger to any interest of a person or a collective interest, including the confidentiality, integrity and availability of ICT networks.

B. Prevention of offenses and alternatives to criminal sanctioning

5. ICT network users and system providers should be encouraged to protect the safety of networks, including by self-regulation of providers. Neglect of safety measures should not lead to criminal liability on the part of users. Legislatures may, however, make punishable the violation of specific obligations to ensure the security of other persons' data.

6. If necessary for purposes of prevention, legislatures may, in accordance with the principle of proportionality, allow the storing of data that permits, under effective judicial control, the identification of users.

7. Because criminal prohibitions carry strong moral reprobation and can stigmatize offenders, states should carefully examine whether non-criminal measures can be equally effective in preventing attacks on ICT networks and abuses of cyberspace. Judicial orders and the award of damages to victims in accordance with civil law, as well as instruments of restorative justice, may be viable alternatives to criminal sanctioning. Administrative measures, for example, blocking access to illegal material or removing it from websites, may also have a sufficient preventive effect and make the use of criminal law unnecessary. However, administrative measures should not be disproportionate or turn into censorship practices applied by executive authorities.

C. Defining offenses

8. In accordance with the principle of legality, legislatures should define ICT offenses in functional terms as precisely as possible. When technology changes, the law may have to be adapted. The principle of legality also applies to the definition of duties and obligations of natural or legal persons to the extent that their violation can lead to criminal responsibility. Courts should not expand the wording of statutory criminal prohibitions beyond their plain meaning.

D. Extension of criminal laws

9. Incrimination of mere preparation for attacks on ICT networks and cyberspace, such as the production, distribution and possession of malware, are legitimate only to the extent that preparatory acts as such cause harm or create concrete danger to the protected interests of others or the confidentiality, integrity and availability of ICT networks. Where preparatory acts are made punishable, the penalty should be less than the penalty for the completed offense (see in this regard the resolutions of the XVIIIth International Congress of Penal Law in Istanbul 2009, Section I (A)).

10. Possession of software should not be criminalized only in order to facilitate proof of wrongdoing. Such criminalization should not unduly restrict the legitimate use of software.

11. The mere possession and viewing of data may be made punishable only where possession and viewing are intentional and cause direct or indirect harm or concrete danger to protected interests.

12.

a) Internet access providers should not be made criminally liable for failing to control contents that they process.

b) Criminal liability of host service providers should be limited to instances where

- they are specifically obliged by law to control certain contents before they are made available to users, it is reasonably feasible for them to do so, and they knowingly fail to fulfill this obligation

or

they have been alerted, in a reliable and specific manner, to the fact that they make illegal contents available, and knowingly fail to promptly take all reasonable measures to make such contents unavailable.

E. International harmonization of laws

13. Policies for the protection of ICT networks and cyberspace and the interests of users should be harmonized worldwide in order to avoid serious discrepancies between regulations of the same matter, to improve international cooperation, and to avoid conflicts of jurisdiction.