SECTION II – CRIMINAL LAW. SPECIAL PART

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

Noting that the global rapid growth of information and communications technology (ICT) networks in cyberspace leading to global connectivity is providing ample opportunities for various criminals in planning and perpetrating crime by taking advantage of online vulnerabilities and by threatening countries’ critical information and communications infrastructures,

Building on the draft resolutions as established by the Preparatory Colloquium for Section II held in Moscow, April 24th to 27th, 2013,

Realizing that the advent of the cyber world has created new legal interests that are at stake and deserve recognition and protection while, at the same time, existing legal interests face new challenges and new vulnerabilities, and new core cyber crimes arise,

Noting from the national reports convergence and harmonization on the one hand, but also some lack of implementation of the existing international legal standards on the other hand, resulting in a need for further work on converging and harmonizing the national legal frameworks, mindful of the subsidiary and ultima ratio role of criminal law (see recommendation #4, Section I),

Taking into account the strong importance and global impact of the cyber world on the daily life of people, on society as a whole, on international trade and commerce, on financial transactions, on political interactions and even on warfare, that give rise to new and challenging legal issues, including ones related to criminal justice,

Noting that in a globalized, interconnected and interdependent world, critical information and communications infrastructures play a vital role in governmental functions and services, national security, civil defense, public health and safety, and banking and financial services,

Aware that the promise of freer, more rapid, worldwide communications by electronic means also carries the risk for limitations on content and form and for widespread control and infringements on human rights and privacy,

Recognizing that at times society’s response to new challenges and threats posed by developments and change in technology, way of life and values leads to over-criminalization and the excessive use of criminal law protection,

Mindful of the importance to be vigilant and to protect and defend core legal values and principles, especially those related to human rights and the integrity, dignity, and value of human beings,

Taking into account the importance, usefulness, and critical role played by the social media in private and public life, maximum freedom of communication and expression should be ensured, balanced by the recognition and respect of mutual responsibilities,

Expressing its preoccupation that information and communications technology advances have created a serious need to develop and adopt a comprehensive legal policy for the cyber world in order to ensure its orderly and positive development, which should utilize technique-neutral legal norms to keep up with the pace of technical development,

Concerned by the potential over-reliance on repressive policies and criminal law protection instead of innovative approaches, and regulatory and administrative solutions, and public education, as well as technical, organizational and personal security measures,

Committed to contributing solutions to the problems and challenges presented by information and communications technology, especially new forms and types of crimes, while ensuring no-less online than offline protection of human rights, fundamental freedoms and legal interests,

Taking into account the important role that civil society, non-governmental organizations and business actors can play to address in a positive and constructive way new problems and new threats and their repercussions on the legal system,

Convincing of the importance of collaborating and cooperating with both the private and public sector, reminding them of their role and responsibilities in securing cyberspace and preventing cybercrimes for the overall benefit of society,

Stressing the need for a common understanding of cybercrime and cyber security and for collaborative efforts by the international legal community that may support and ensure a secure cyber world by shaping frameworks applicable across borders and inter-operable with international and national legal regimes and systems in place,

Noting with appreciation the work of international and regional organizations, and in particular the work of the Council of Europe in elaborating the Convention on Cybercrime (2001); the appropriate legal standards of the European Union; the contributions of the Organization of American States, the Arab League, the Economic Community of West African States, the Community of Independent States, the World Bank, the OECD, the United Nations and that of other organizations in initiating fruitful interaction between government and the private sector on security and anticrime measures in cyberspace,
Mindful of the main aim of the AIDP to uphold the rule of law and support the development of the law in addressing current trends and phenomena and in responding efficiently and positively to the constant need to raise the standards of protection of the individual and the community,

Underlining previous work by the AIDP in this crucial area, such as the conclusions of the Congress of the AIDP Young Penalists (Noto, June 2001, topic 3), the International Preparatory Colloquium on International Trafficking in Women and Children (Rio de Janeiro, April 2002) and the Round Table on international trafficking in women and children held on the occasion of the XVIIth AIDP Congress (Beijing, September 2004),

Have adopted the following resolutions:

1. In addressing the threat and reality of cybercrime and the necessity of cyber security, the legal and criminal justice system should balance individual, collective, private sector and public interests. Over reliance on criminal law protection should be avoided in favor of robust prevention, active defense, public education and awareness, and alternative sanctions.

2. Legal interests to be protected include the confidentiality, integrity and availability of data and ICT systems, authenticity of information, life and limb, integrity of children, privacy, protection from harm and loss of property (including virtual property), copyright and reputation, freedom of expression, and other fundamental human rights.

3. Consumer protection, informed consent, purpose limitation, right to erasure, correction and notification, shall be paramount values in guiding the formulation of laws and regulations on data collection, selling and buying on the Internet, financial transactions and investments, and marketing and promotional campaigns.

4. Commercial personal data processors, like Internet and telecommunications providers, social media platforms, and application developers, should be required to adopt privacy by design and by default policies, if necessary by compelling measures. The violation thereof should be redressed through non-criminal or criminal sanctions.

5. A concerted effort is essential to prevent and combat illegal access to ICT systems; the illegal interception of non-public transmissions of electronic data; data and system interference without right; the misuse of devices, software, passwords, and codes; computer-related forgery and fraud; and unauthorized access by government agencies. This includes a minimum standard of criminal law protection against intentional and harmful acts violating the confidentiality, integrity and accessibility of data and of ICT systems.

6. Appropriate legal measures should be adopted to provide aggravating circumstances or specific offenses with more-severe penalties for interfering with the functioning of critical information and communications infrastructures.

7. The production and the knowing distribution, dissemination, importing, exporting, offering, selling, purchasing, possessing, and accessing of child pornography and any complicity and participation in any of these acts shall be firmly and consistently prevented and criminalized with appropriate sanctions, especially when involving real children, unless for their own private use in case they have reached the age of sexual majority.

8. Identity theft, including through phishing, as a whole or in their components, should be criminalized, if not otherwise provided for by other criminal law provisions. If States choose to criminalize the mere possession of identity-related information or impersonating non-existing persons, it should be limited to acts committed with criminal intent to cause damage. Such provisions should neither restrict nor criminalize freedom of thought and expression, in particular, literary and artistic activities.

9. Given the growing concern about the frequency and seriousness of cyber stalking, cyber bullying, and cyber grooming, special attention shall be given to effectively respond to the problem, emphasizing positive approaches, prevention, public education and awareness, and alternative sanctions, rather than only applying criminal law protection.

10. The protection of intellectual property rights should focus on intentional violations with a significant commercial purpose or that produce serious damages.

11. Reckless or grossly negligent management of critical ICT infrastructure and of large amounts of sensitive data, such as credit card data, should be redressed through non-criminal or criminal sanctions. Likewise, failing to adopt reasonable security measures and/or to disclose required information about security breaches in a timely manner by ISPs may be grounds for civil or criminal action.