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

Building on the draft resolutions as established by the Preparatory Colloquium for Section IV held in Helsinki from 9 to 12 June 2013,

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 that accompany information society and cyberspace, and that therefore crimes in these areas affect important personal and collective interests;

Noting that states share sovereignty in cyberspace and have a common interest in its regulation and protection;

Recognizing that states have made considerable efforts to vest jurisdiction and determine the locus delicti of offences that may affect the integrity of ICT systems and cyberspace, as well as the related interests of persons and society;

Keeping in mind the particularities of cyberspace, such as the speed at which data flows, its volatility, and the fact that it can be accessed anywhere in the world;

Recognizing further the difficulties in localizing information and evidence in cyberspace;

Stressing the fundamental importance of the protection of human rights, in particular the principle of legality, the right to privacy and to data protection, the right to a fair trial, the principle of proportionality in the investigation and prosecution of offences, and in general the rules and principles regarding due process;


Building on the debates and resolutions of past International Congresses of Penal Law, especially the resolutions of Section II of the XV International Congress (1994) held in Rio de Janeiro, on computer crimes and other crimes against information technology, and the resolutions of Section III on Special Procedural measures and respect of Human rights and the resolutions of Section IV on universal jurisdiction of the XVIII International Congress (2009) held in Istanbul;

Defining for the purpose of this resolution that coercive measures means measures against the will of the subject or infringing upon their right to privacy;

Have adopted the following resolutions:

A. General Considerations

1. States should develop a coherent response to the challenge of cybercrime, in particular by keeping their legislation and practice under review in order to ensure that their criminal law, criminal procedure and mutual legal assistance regimes meet the needs of today’s interconnected globalised world, while respecting fundamental and human rights.

2. States should consider acceding to existing international instruments on cybercrime. States and the international community shall work to develop further international legal mechanisms, including compliance standards for multinational enterprises, in order to establish the rule of law in cyberspace and avoid potential conflicts between states on the enforcement of their legislation and policies in cyberspace.

B. Substantive Jurisdiction and Locus Delicti

3. While the principle of territoriality remains the primary principle of jurisdiction also in cyberspace, it produces adverse effects when applied to offences in cyberspace, in that it de facto allows states to localise offences on their territory almost on a universality basis and leaves individuals in doubt as to which states may claim jurisdiction. States should exercise restraint in exercising jurisdiction in situations in which the effect is not “pushed” by a perpetrator into the state, but “pulled” into it by an individual in that state.

4. In determining effects, states shall consider the existence of a particular nexus with the offence, such as the intent of the perpetrator as it may appear from the use of a given language, the provision of domestic payment facilities, a service offer in specific cities, etc.

5. When a state localizes the effects of an offence within its borders, the principle of legality requires that the perpetrator could have had a reasonable expectation that his or her conduct would cause effects in that country.

6. A state may exercise its jurisdiction over an individual on its territory who “pulls” content that is prohibited under its own legal system, even though it is legal under the local system of the producer.
7. States and the international community should consider establishing corporate compliance requirements and liability for criminal offences by legal entities with regard to cybercrime.

C. Investigations in Cyberspace

8. No state has exclusive sovereignty over the publicly accessible ICT networks.

9. Except in cases where coercive or undercover measures are applied, law enforcement agencies may access (and operate in) freely accessible ICT networks without permission from providers and/or states, and regardless of where the content looked at is stored.

10. In order to prevent cybercrime and make the investigation accountable, states and the international community should consider establishing upon service providers, software and application developers and other relevant private ICT stakeholders an obligation to enhance data protection, privacy friendly technology and setting.

11. States should consider establishing, under national law, an obligation upon service providers to cooperate, subject to authorisation by an independent judicial authority, with law enforcement agencies (e.g. by making data transfer in the cyberworld traceable, giving access to passwords, decrypting content or installing search devices for investigative purposes). This obligation is subject to the principle of proportionality and compliance with fundamental and international human rights.

12. States pursuing investigations must afford all persons involved the protection that would accrue to them in a similar domestic case, while also affording them the protection that accrues to them under the national legal system of the state where the investigative measures are taken or where the persons concerned are situated when the investigative measures are taken.

D. International Cooperation and Enforcement in Criminal Matters

13. States must make sure that, in granting mutual legal assistance with respect to cyber offences, they can take all investigative measures that could be lawfully taken in a similar domestic case.

14. States should in particular be able to provide fast assistance and to execute a provisional order to preserve or freeze information and evidence during a reasonable time and without unduly affecting the rights of parties.

15. States may not refuse mutual legal assistance based on a lack of dual criminality for cybercrime offences, the criminalisation whereof is required under an international legal obligation incumbent upon them.

16. A (provisional) decision by an independent judicial authority to close down a server or website or a request of a state to take down a botnet may be enforced directly if provided for by an international agreement or by the law of the state in which the service provider or the botnet command and control server is located. Wherever possible, preference should be given to make the website inaccessible on the territory of the requesting state only, thus avoiding unnecessary limitation of cyber freedom.

17. The later use of information gathered by intelligence services in criminal matters is only allowed where the information concerned could have been obtained through regular mechanisms for judicial or law enforcement cooperation in criminal matters.

E. Real Fundamental and Human Rights in a Virtual World

18. States shall respect internationally recognized fundamental and human rights standards applicable to them also in the context of the digital world.

19. If states act extraterritorially while investigating in cyberspace, they shall comply with the fundamental and human rights standards applicable to their jurisdiction (agent control standard), as well as those applicable to the state where the extraterritorial investigations are taking place and when the persons concerned are situated when the extraterritorial investigations are taking place.

20. States should record investigations in cyberspace with a view to ensuring state accountability in the event of violations of fundamental or human rights. They should also disclose such recordings to the defence with a view of ensuring a fair trial and seeking a remedy before supervisory mechanisms.

21. The responsibilities of a specific state for violations of fundamental or human rights should be decided after a finding of a violation and not as a condition for admissibility of a complaint with supervisory mechanisms.

F. Virtual Court Room

22. Communications may be digitally sent by the authorities directly to the suspects, accused, witnesses, victims and experts who are physically present in another state, subject to the acceptance of the latter of this method of communication. The communications must be accompanied by a translation into a language understood by the addressee and by a statement spelling out the rights and obligations of the addressee with regard to the communication received, in particular in so far as entitlement to assistance by a lawyer, a duty to appear, contempt of court and perjury are perceived.

23. The possibilities of making use of digital technology, such as videolinks, in international criminal justice should be expanded in order to lessen the need for coercive measures like extradition, as well as in order to avoid unnecessary temporary transfer of a detained person or the physical appearance of witnesses and experts before authorities abroad.
24. States should be encouraged to consider the possibility of and conditions for the presentation of evidence through digital technology during the trial stage, even where the accused is not physically present at the hearing.

25. The security, integrity and reliability of the digital communication in use by the authorities must be of the highest standard.

26. States must provide adequate facilities to enable direct client-lawyer digital communications, especially when the client is detained.

27. The confidentiality of digital communications used in international criminal justice must be sacrosanct.