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 III held in Antalya from 24 to 27 September 2013,

Considering that the use of information and communications technologies (ICT)
- generates new social, cultural, economic and legal realities;
- poses new challenges for national and transnational criminal justice systems in the field of prevention, investigation and prosecution of crimes in general and cybercrime in particular;
- has the capacity to endanger in an unprecedented way human rights and freedoms, and particularly the right to privacy;

Recognising
- that the rapid development of ICTs has led to an extensive use by law enforcement authorities both in criminal proceedings, including the criminal investigation, and in the building of information positions for preventive purposes;

Taking into account that
- the AIDP Congresses of Penal Law have already addressed several aspects of these new challenges for criminal investigations resulting from the information society, especially:
  - the XVth International Congress of Penal Law (Rio de Janeiro, 1994) on “Reform Movements in Criminal Protection and the Protection of Human Rights”;
  - the XVIth International Congress of Penal Law (Budapest, 1999) on “The Criminal Justice System Facing Challenges of Organized Crime”; and
  - the XVIIIth International Congress of Penal Law (Istanbul 2009) on “Special Procedural Measures and Respect of Human Rights”;

Endeavoring
- to set out principles and rules of criminal procedure in line with the rule of law and human rights in the use of ICT in criminal proceedings and in the building of information positions for law enforcement purposes;
- to ensure that the use of ICT in criminal proceedings and in the building of information positions does not impair the right to privacy and data protection;
- to guarantee that the use of ICT does not violate defence rights and the fairness of criminal proceedings;
- to seek the efficient implementation of the new technologies in the fight against sophisticated serious crimes involving the use of information and communications technologies (ICT);

Have adopted the following resolutions:

A. The use of ICT and the protection of human rights

The use of ICT in criminal proceedings and in the building of information positions may represent a significant intrusion into fundamental rights. The following principles should be particularly respected:

1. Any restriction on the right to privacy shall be provided by law and be proportionate, legitimate and necessary in a democratic society.

2. The use of ICT in criminal proceedings and in the building of information positions should respect the right to data protection. The aims of criminal prevention and investigation should be proportionate to the encroachment on the fundamental right to data protection.

3. The purpose limitation principle should be respected in general, and, as a rule, when transferring electronic personal data to law enforcement authorities. The purpose limitation principle means that personal data can only be collected for an explicit, specified and legitimate purpose, and not further processed in a way incompatible with those purposes.

4. Derogation from the purpose limitation should only be permitted, according to the law, in exceptional cases, where the transfer of data to law enforcement authorities is necessary for the prevention, investigation, or prosecution of serious crimes and respects the proportionality principle.
5. The legal framework should ensure that adequate means and thresholds for the access and disclosure of stored data are established and that they are controlled by an independent authority. Any obligation of public and/or private companies to retain, preserve, and transfer computer data must respect the right to data protection.

6. The use of ICT in criminal proceedings shall not infringe fair trial rights, inter alia, the right to a public hearing, to cross-examination and confrontation, to access the file and to obtain the assistance of experts, specialized in the field of electronic evidence to ensure the equality of arms.

B. ICT intelligence and the building of information positions

7. The law shall regulate which measures can be used by law enforcement authorities for building information positions and determine the aim, scope and requirements of these measures, including the conditions for deletion of this data and/or destruction of the storage media.

8. Coercive measures should not be allowed to collect data for building information positions, unless there is court authorization. Court authorization should also be required for building information positions by means of non-open source data mining and/or data matching.

9. No surveillance powers used for building information positions should infringe the right to privacy or other fundamental rights.

10. Adequate technical means should be used to control the access to data for the purpose of building information positions. An independent authority should control the access to sensitive data.

11. The law should establish in which cases and under what conditions data collected for building information positions may be transferred to another authority.

C. ICT in the criminal investigation

12. ICT investigative measures, such as electronic surveillance, geo-location monitoring, real-time or stored data collection, covert on-line investigations, computer data seizures and searches, extended searches on connected networks, orders for providing or decoding computer data, access to and/or analysis of communication data stored on mobile devices, use of remote forensic tools and interception of any kind of communications carried out with the aim of a criminal investigation shall only be allowed in the cases specified by law when the desired information cannot be gathered through less-intrusive means. The law shall define the scope of the investigative powers, the maximum duration of any investigative act and requirements for the storage and/or deletion of the data obtained, and/or the destruction of the storage media. It should be ensured that the laws are adapted to the search and seizure of intangible data.

13. ICT investigative measures that seriously intrude on the right to privacy, such as those which access the content of communications, involve the real-time interception or collection of data, or the use of remote forensic tools, should, as a rule, only be granted under court authorization and only in cases where there is reasonable suspicion of the commission of serious crimes, and that the target is linked to the commission of such crimes.

14. Persons whose right to privacy has been affected by investigative measures involving ICT should be informed of the measures as soon as this disclosure does not jeopardize the purpose of the measure and/or the results of the criminal investigation. The law shall provide for effective judicial remedies to challenge the legality of the use of ICT investigative measures and protect their right to confidentiality.

15. Those carrying out ICT investigative measures that allow access to computer data and electronic communications must respect the right of confidentiality and professional privilege. The disclosure of data not related to the criminal proceedings should be prevented.

16. States have a positive obligation to ensure that law enforcement agents have the necessary technical means, capacities and expert training in the use of ICT to deal with sophisticated forms of cybercrime and electronic evidence in general. Best practice guidelines should be developed and applied in investigations involving the use of ICT.

17. The cooperation of private companies and ICT service providers with law enforcement authorities in the criminal investigation that may infringe fundamental rights shall be regulated by law. The scope, conditions and requirements for such cooperation must be set out in the law. Compliance with such legal obligations should not trigger any civil liability in relation to the company’s clients.

D. Evidence and ICT

18. Due to the volatile nature of electronic evidence the law should facilitate the expeditious preservation and storage of digital data. Forensic tools for preventing alterations of the stored data should be available and routinely employed.

19. If the reliability of ICT evidence is challenged, the “evidence continuity” or “chain-of-custody” must be established. The defense should be guaranteed access to digital data so as to be able to verify its authenticity, and to present it at trial in an effective and not unduly restricted manner.
20. Electronic evidence obtained directly or indirectly by means that constitute a violation of fundamental rights and freedoms that jeopardize equality of arms and the fairness of the proceedings shall be inadmissible.2

E. The use of ICT at trial

21. Courtrooms should be equipped for the use of ICT during criminal trial proceedings. Financial resources to achieve this goal should be provided.

22. Video-conferencing should be available to transmit the testimony of vulnerable or unavailable witnesses, warranting the identity of the witness and to allow their examination in those situations permitted by law.

23. The examination and cross-examination of child victims during the pre-trial stage should be video-recorded in case the child is unavailable to testify at trial for reasons relating to protection of the child's well-being.

24. The defendant, as a rule, should always be physically present during court proceedings. In the rare cases where presence through video-conferencing is allowed, it should be realized in a manner that adequately protects the privilege against self-incrimination, the right to counsel (including that of confidential communication with counsel) and the right to cross-examine witnesses.

---

2 For the admissibility of intelligence as evidence, see point 22 of the resolution adopted at the XVIIIth International Congress of Penal Law (Istanbul 2009) on "Special Procedural Measures and Respect of Human Rights."