



27 Feb 2019

**Romanian Presidency of the Council of the European Union  
in cooperation with the Council of Europe**

**Conference on**

## **Criminal Justice in Cyberspace**

**25 – 27 February 2019**


### **Key messages**

More than 100 criminal justice experts from some 40 countries, including from public and private sectors as well as international organisations, participated in this Conference on Criminal Justice in Cyberspace.

The event was jointly organised by the Romanian Presidency of the Council of the European Union and the Council of Europe. It was opened by the Minister of Justice of Romania and the Deputy Secretary General of the Council of Europe. The Conference on 26 and 27 February was preceded by a special event on the 5<sup>th</sup> anniversary of the Cybercrime Programme Office of the Council of Europe (C-PROC) in Bucharest.


Key messages are:

- The question of electronic evidence touches upon core interest of governments, private sector entities and individuals. While solutions are necessary, reaching agreement on solutions that reconcile different interests is challenging.
- Criminal justice authorities need to have effective means to secure electronic evidence as cybercrime and technology evolve since otherwise trust in the rule of law may erode and powers may further shift away from criminal justice to national security institutions. Additional solutions are in the making and a very much needed.
- Overall, the type of threats of cybercrime that societies are faced with seem to be similar in all regions of the world. Many attacks come from outside or the evidence is abroad. It is clear that in order to understand and counter these threats it is necessary to look beyond individual countries and regions.
- Cybercrime is a transversal threat and thus interagency, public/private and international cooperation are essential. Cooperation at all levels needs to be backed up by capacity building programmes.
- Challenges for criminal justice in cyberspace include the need to make mutual legal assistance more efficient and to address the problem of evidence in the “cloud”, that is, in foreign, multiple or unknown locations, and the related issues of jurisdiction and loss of knowledge of location. At the same time, concepts of jurisdiction are evolving, and increasingly the location



of the person in possession or control of data is considered more relevant than the location of data.

- Private sector organisations from the USA receive large numbers of requests for data from law enforcement authorities around the world. While they are often able to respond to requests, the question of authentication and assessment of the lawfulness of a request is a challenge for providers. Single points of contact and a sufficient amount of detail in requests help address this challenge. Service providers remain concerned about being confronted with conflicting obligations resulting from different legal frameworks.
- Important steps have been taken in recent years by governments in different regions and European organisations to strengthen rules for the protection of personal data. The EU's General Data Protection Regulation and "Police" Directive 2016/680 are particularly influential. The Council of Europe's data protection Convention 108, modernised in 2018 ("Convention 108+"), serves many countries as a guideline and now has 54 Parties, including seven States from Africa and Latin America.
- Better understanding is needed on how to reconcile data protection and criminal justice requirements in practice, in particular in a cross-border context, and how data protection interests are weighed against important public interests such as crime prevention and public safety. It is recalled that governments have a positive obligation to protect the rights of individuals also against crime.
- Recent court decisions suggest that access to subscriber information is a lesser interference with the rights of individuals but that a case-by-case analysis taking into consideration the specific context may be required. This may also apply to the legal basis for the processing of data, where – depending on the situation – compliance with a legal obligation, vital interests, consent of the data subject, important public interests or legitimate interests of a data controller may be invoked.
- Solutions remain to be found regarding access to WHOIS data. Such data are not publicly available anymore as from May 2018, and criminal justice practitioners are now forced to abandon a considerable share of investigations.
- Capacity building on cybercrime and e-evidence – ranging from strengthening domestic legislation, training of judges, prosecutors and investigators, setting up of specialised institutions, and enabling cooperation at all levels – is a crucial part of the response and helps address urgent needs. The experience of the Cybercrime Programme Office of the Council of Europe in Bucharest over the past five years with more than 600 activities involving some 120 countries demonstrates that capacity building works and makes an impact.
- The joint projects of the European Union and the Council of Europe GLACY+, iPROCEEDS, CyberSouth and the forthcoming new project CyberEast underline the close cooperation between the European Union and the Council of Europe in support of capacity building in all regions of the world.
- The Budapest Convention remains the most relevant international agreement on cybercrime and electronic evidence and membership keeps increasing. Parties need to make maximum use of this treaty and to implement its provisions in domestic law, in particular procedural powers with conditions and safeguards. The Convention remains up to date through Guidance Notes and Protocols.

- 
- The negotiation of the 2<sup>nd</sup> Additional Protocol on enhanced international cooperation and access to evidence in the cloud will further equip current and future Parties to the Convention with the means to better uphold the rule of law in cyberspace.
  - Further consultations with private sector entities and data protection experts will be sought to finalise specific provisions in particular on direct cooperation with providers.
  - The EU e-evidence package consisting of a Regulation on a mandatory European Production and Preservation Order and a complementary Directive regarding legal representatives of service providers to be established within the EU, will provide an efficient system for EU Member States to access electronic evidence with safeguards.
  - These EU legislative proposals are complemented by technical measures such as a secure EU portal for e-evidence requests for which the concept is available and which authorities in EU Member States are now encouraged to test.
  - The development of solutions at the levels of the EU and the Council of Europe should remain mutually reinforcing, consistent and complementary. Considering that the additional Protocol needs to function for the currently 62 States that are Parties, flexibility is needed.
  - As technology and the threat landscape evolve, both the e-evidence proposals of the EU and the Protocol to the Budapest Convention need to be made future-proof.

Bucharest, 27 February 2019