Cybercrime and Fundamental Rights – Expert meeting

Bucharest, 15-16 November 2018

Summary outcome

I. Scope of the Handbook:

- The scope of the Handbook should include the relevant legislation of the EU, the relevant conventions of the Council of Europe and the relevant case law of the CJEU and ECtHR. If appropriate, references to national promising practices and to UN, OSCE and other multilateral sources may be included as well.
- Electronic evidence is of paramount relevance in the fight against cybercrime and it should feature in the Handbook, taking due consideration on-going legal developments at both, EU and CoE levels.
- The Handbook should not contain technical details of cybercrime investigative measures, which are not relevant for a fundamental rights approach and would restrict the public access to the document. However, the importance of a thorough understanding of fundamental rights principles when employing investigative techniques should be included in the Handbook.
- The Handbook should not cover cyber-security and cyber-defence. However, it should include guidance on fundamental rights standards applicable to the exchange of information between intelligence services and law enforcement, while countering terrorism and hybrid attacks.
- Finally, the rights of victims of cybercrime should be present horizontally in the different sections of the Handbook.

II. Target group of the Handbook:

- The Handbook should be a guiding tool on application of fundamental rights standards in cybercrime and electronic evidence matters for legal practitioners working in the field, such as judicial authorities, law enforcement authorities and lawyers as well as policy makers, legislators, civil society organisations, oversight bodies and media.

III. Main Features of the Handbook:

During the meeting, an initial brainstorming on fundamental rights challenges related to cybercrime and in particular, electronic evidence took place. As a result, participants agreed on the preliminary list of elements and suggestions that could be covered by the Handbook:

- **Key concepts and definitions**. including:
  - Computer systems vs. Information systems
  - Service providers
  - Type of data
  - Ownership of the data
  - Cyber-crime vs. Cyber-security vs. Cyber-warfare vs. Cyber-terrorism
  - Fundamental rights at stake
  - Privacy vs. Data Protection

    - Electronic evidence
    - Retention vs. preservation
    - Direct cooperation with providers vs. direct access
- **Applicable legal frameworks**, including CoE Conventions/ Guidance Notes/ Additional Protocols (e.g.: Budapest, Lanzarote, 108+, Istanbul, etc.) and EU Regulations/ Directives (e.g.: Directive on attacks to computer systems, e-Evidence, GDPR, e-Privacy, etc.).
- **Cybercrime threats to fundamental rights of the victim**
    - Positive obligations of the State to protect the rights of individuals.
    - Mapping fundamental rights threatened by cybercrime: human dignity, life, integrity of the person, prohibition of slavery and forced labour, privacy, data protection, freedom of expression, property, non-discrimination…etc.
    - Special focus on vulnerable groups: children, elderly, persons with disabilities, LGBTI and gender-oriented cybercrime (violence against women)
- **Substantive law: guidelines on criminalisation**
    - Under-criminalization vs. over-criminalization – general considerations
    - Criminalization of offences against confidentiality, integrity and availability of computer data and systems
    - Criminalization of content-related crimes
    - Sanctions and measures
- **Procedural powers and safeguards: guidelines on investigative measures**
    - Acquiring, preserving and presenting electronic evidence
    - Data protection principles in the context of the fight against cybercrime(e.g. GDPR/ WHOIS issue)
    - Loss of location and jurisdiction
    - Data retention
    - Cross-border access to data
    - Mediated access, direct access, direct cooperation and other forms of private-to-public collaboration
    - Encryption: Ownership of data and the right against self-incrimination
    - Legal hacking
    - National security and law enforcement, including cyber-investigations countering terrorism.
- **Oversight bodies and scrutiny controls**
- **Glossary of terms**

IV. Next steps

- The second expert meeting will be organised by the FRA in Vienna from 14 to 15 May 2019.