Cybercrime and Fundamental Rights – 2nd Expert meeting

Summary outcome

14-15 May 2019
EU Agency for Fundamental Rights (FRA), Vienna.

This document summarises discussions at the expert meeting that took place in Vienna on 14-15 May 2019. This consultation follows an initial exchange held in Bucharest on 15-16 November 2018 (see summary). Both meetings were organised in the context of the joint project by the EU Agency for Fundamental Rights and the Council of Europe to prepare a Handbook relating to cybercrime and fundamental rights.

Aim and scope of the Handbook

- Following a request from the European Parliament, the future Handbook should serve to build capacity and raise awareness on practical issues relating to cybercrime and fundamental rights.
- The Handbook will present European law (EU and Council of Europe) and existing international standards on human rights (incl. from the UN and Organisation for Security and Cooperation in Europe (OSCE)) relevant to cybercrime. Handbooks are not standard-setting documents, but present relevant existing standards and practices in a neutral (non-opinionated) form. Where legislation or case law do not provide clear legal standards, the Handbook will highlight the fundamental rights at stake, but it will not provide policy guidelines.
- Following the flexible approach of the Budapest Convention on cybercrime, the Handbook will present the extent to which computer and information systems are both the object and a tool of crime, with a fundamental rights focus. The Handbook will cover the perspective of both victims and suspects. Similarly to the Budapest Convention, the Handbook will include reference to the procedural powers to investigate cybercrime and the relevant legal frameworks on electronic evidence.
- Cybersecurity and cyber defence, while beyond the scope of the Handbook, will be mentioned to highlight common challenges within the area of criminal justice.

Target group

- The primary target group is legal practitioners, including criminal justice authorities, criminal lawyers and victim support services.
- The Handbook should be an accessible tool for a non-specialised audience. However, this publication should also include references and a bibliography allowing access to more specialised guidance for interested readers.

Structure

- An **introductory chapter** should present the phenomenon of cybercrime, the complexity of reaching common definitions, and delineate the differences between cybercrime, cybersecurity and cyber defence. Recognising that there is not a universally acknowledged definition of cybercrime, the Handbook will not aim to provide one; it will instead refer to accepted/existing standards where criminal conduct in the area of cybercrime are defined, such as the Budapest Convention. This chapter will

present the methodology for the application of general fundamental rights principles that come into play when dealing with such conduct (i.e. legality, legitimacy, necessity and proportionality). It will also include case law and case studies relating to the practical application of fundamental rights principles in the area of cybercrime.

- The Handbook will include a chapter **describing the threats cybercrime poses to fundamental rights**. Rather than a catalogue or mapping exercise, a reference to common challenges and day-to-day situations could be more useful for practitioners. This description should be as technologically neutral as possible to avoid the risk of becoming rapidly outdated, and present the main features of cybercrime, including: its borderless nature and the jurisdictional challenges this poses, speed of commission and related investigative challenges, the high volume of data involved and potential challenges to the fundamental rights of victims.
- The Handbook will include a focus on **victims' rights**, in particular those in vulnerable situations. Given that children are large consumers of the online world, they are particularly susceptible to cybercrime. This section should highlight specific aspects of victimisation of children in the online context and its impact on victims' access to justice.
- Along with the description of threats to fundamental rights, the Handbook will include European standards on the **criminalisation** of cybercrime. The Handbook will present, using examples from national law, the risks to fundamental rights associated with over-criminalisation (e.g. the consequences for freedom of expression of over-reaching legislation criminalising content-related cybercrime) and under-criminalisation (e.g. the consequences of applying off-line criminal definitions to similar conduct in the on-line context, with a different impact on fundamental rights). This analysis of substantive criminal law will include challenges relating to the proportionality of criminal offences and penalties, especially in the context of juvenile delinquency and the criminalisation of preparatory acts of cybercrime.
- **Procedural powers and safeguards** should be presented along with the key milestones of criminal investigations, such as:
    - **Detecting and reporting crime**, including cooperation with cybersecurity actors and the responsibilities of the private sector.
    - **Investigative measures**: the structure could follow Section 2 of the Budapest Convention, reflecting the different degrees of intrusiveness of the measures and the corresponding safeguards. These include judicial oversight and scrutiny by other institutions, such as data protection authorities and ombudspersons. This section will cover current challenges, for example data retention and encryption, potentially using case studies. The Handbook should be forward-looking on challenges that will emerge with the internet of things or the use of new investigative techniques (i.e. those based on Artificial Intelligence and Open Source Intelligence).
    - **Notification** of the measures to the suspect, effective **remedies** and the principle of equality of arms in a **fair trial**.
    - **Deterrence and disruption**: including the fundamental rights challenges associated with taking down illegal content or cleaning/deleting malware from infected information systems.

  International cooperation between criminal justice authorities and issues related to jurisdictional challenges, including dual criminality and *ne bis in idem* issues. A relevant topic under this section would be cross-border access to electronic evidence. A separate chapter of the Handbook will be dedicated to this topic

PARTICIPANTS

Experts invitees

Name	Organisation and position
Philipp AMANN	Europol, EC3, Head of strategy
Jan ELLERMANN (joining via VC)	Europol, Senior Specialist in the Data Protection Function
Judith HERRNFELD	Public Prosecutor, Austria
Kamola IBRAGIMOVA	UNODC, Officer, Counter-Cybercrime education
Demosthenes IKONOMOU	ENISA, HoU Operational Security
Robert LAID	Eurojust, prosecutor, Operations department
Karl LINDERBORG	European Commission, DG HOME -D4-, Policy officer
Denise MAZZOLANI	OSCE, Deputy Head of Strategic Police Matters Unit and Adviser on Cybercrime
Michael PALMER (joining via VC)	European Commission, DG JUST –B2-, Policy officer
Silvia POPA	Public Prosecutor, Romania
Geoffrey SHANNON	Special Rapporteur on child protection, Ireland
Xavier TRACOL (joining via VC)	Eurojust, DPO, senior legal officer
Lodewijk VAN ZWIETEN (joining via VC)	Public Prosecutor, The Netherlands

FRA Staff

Name	Unit
Albin DEARING	Research and Data Unit
Jana GAJDOSOVA	Research and Data Unit
Joanna GOODEY	Research and Data Unit
Antonio GUTIERREZ	Research and Data Unit, SNE
Alexandros KARGOPOULOS	Research and Data Unit, SNE
Michal NESPOR	Research and Data Unit
Elise LASSUS	Research and Data Unit
Mario OETHEIMER	Research and Data Unit
Lilla OZORAKOVA	Research and Data Unit, Trainee
Eliska PIRKOVA	Research and Data Unit, Trainee
Martha STICKINGS	Institutional cooperation and networks Unit

CoE Staff

Name	Position
Matteo LUCCHETTI	Programme Manager, Cybercrime Programme Office (C-PROC) Bucharest