JUST-2021-JACC

Action grants to support transnational projects
to enhance the rights of persons suspected
or accused of crime and the rights of victims of crime

JUSTICE PROGRAMME

GA No. 101056685

Improving the application of the presumption of iNNOCENce when applying elecTronic evidence

INNOCENT

WP 3: Advancing capacities of professionals on e-evidence

D3.1 Guidelines and Capacity Building modules for INNOCENT capacity-building activities

WP3 leader: Human Rights House Zagreb

Funded by the European Union

This deliverable was funded by the European Union under Grant Agreement 101056685. The content of this report, including views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union. Neither the European Union nor the European Commission can be held responsible for them.

Acronym	**INNOCENT**
Title	Improving the application of the presumption of iNNOCENce when applying elecTronic evidence
Coordinator	Law and Internet Foundation
GA No.	101056685
Programme	Justice Programme (JUST)
Topic	JUST-2021-JACC
Start	16 May 2022
Duration	24 months
Consortium	Law and Internet Foundation (LIF), Bulgaria Adam Mickiewicz University Poznań (AMU), Poland Human Rights House Zagreb (HRHZ), Croatia Bratislava Policy Institute (BPI), Slovakia CEELI Institute (CEELI), Czechia Science and Research Centre of Koper (ZRS), Slovenia

Dissemination level		
PU	Public	X
SEN	Sensitive, limited under the conditions of the Grant Agreement	
EU - R	RESTREINT-UE/EU-RESTRICTED under Decision 2015/444.	
EU - C	CONFIDENTIEL-UE/EU-CONFIDENTIAL under Decision 2015/444	
EU - S	SECRET-UE/EU-SECRET under Decision 2015/444	
Document version control:		
	Author(s)	**Date**
Version 1	Drafted by: Klara Horvat, Martina Refi Homolak, **HRZR**	22.12.2022
Version 1	Reviewed by: George Dimitrov, **LIF**	22.12.2022
Version 2	Drafted by: Martina Refi Homolak, **HRZR**	24.02.2023
Version 2	Reviewed by: Snezhana Krumova, **LIF**	27.02.2023
Version 3	Drafted by: Martina Refi Homolak, **HRZR**	16.03.2023
Version 3	Reviewed by: Snezhana Krumova, Denitsa Kozhuharova, **LIF**	18.03.2023
Version 3	Reviewed by: Erazem Bohinc, **ZRS**	03.04.2023
Version 4	Drafted by: Martina Refi Homolak, **HRZR**	03.05.2023
Version 4	Reviewed by: Denitsa Kozhuharova, **LIF**	04.05.2023
Version 5	Drafted by: **HRZR**	11.05.2023
Version 5	Reviewed by: George Dimitrov, **LIF**	16.05.2023
Version 5	Reviewed by: all partners	01.06.2023

Version 5	Final review: George Dimitrov, **LIF**	02.06.2023

Table of contents

Executive Summary

The present report provides information to the INNOCENT project partners in terms of how to organise the national capacity building events, as well as what the content of those events should be. It starts off providing the idea behind the capacity building events, as well as their planned scope. It sets out specific goals and learning objectives, namely, to enhance the capacity of key professionals to:

- properly approach and assess e-evidence;
- better understand procedural rights of persons suspected or accused of crime, in particular on the right to be presumed innocent until proven guilty in context of applying electronic evidence;
- detect issues relating to electronic evidence such as the various types that they may encounter, how it is recovered and handled during investigations and produced for criminal trials;
- basis for challenging the admissibility of e-evidence in court;
- improve knowledge and awareness of interinstitutional and international cooperation in the context of e-evidence.

The guidelines outline who are the target participants, namely judges, prosecutors and defence attorneys, as well as the profile of the speakers and trainers. They further shed light into the appropriate teaching methods proposing useful approaches. The guidelines note additionally in terms how to overcome possible challenges and what is the ideal timeframe for the carryout of the capacity building events. They provide INNOCENT partners with hints how to select the location, as well as useful tools for the events' evaluation.

The guidelines come with practical information organised in the form as appendices. Appendix 1-4 provide support from logistical perspective, while Appendix 5 contains information directed towards speakers and trainers in terms of what topic to address during the national capacity building events, how to present to the participants and what are the main takeaways, along with recommendations for further reading.

Abbreviations

Abbreviations	Descriptions
BG	Bulgaria
CZ	Czechia
EAW	European Arrest Warrant
EIO	European Investigation Order
EU	European Union
HR	Croatia
LEA	Law Enforcement Agency
PIN	Personal identification Number
PL	Poland
PSAC	Person Suspected or Accused of Crimes
SI	Slovenia
SK	Slovakia
WP	Work Package

General reasoning

The training aims to improve the practical implementation of the presumption of innocence in the context of e-evidence and enhance the capacity of relevant stakeholder groups to address the more effective use of e-evidence. In order to achieve this, national capacity-building activities will be conducted in a coherent manner in all partner countries (BG, HR, SK, CZ, SI, PL) where they will be implemented.

The current capacity-building guidelines provide a structural basis for drafting specific capacity-building modules that are aimed at developing and improving the skills and knowledge of relevant professionals for better understanding the specific challenges related to the use of e-evidence in each country. The guidelines also lay out logistics and organizational aspects to be considered by each partner when planning and carrying out the respective capacity-building activities. These materials and suggestions contained in the guidelines, such as learning methods, pre- and post-evaluation questionnaires, and exercises, will need to be adapted to country-specific circumstances and target group needs.

The guidelines are based on D2.1 INNOCENT Report and D2.2 INNOCENT Case Law Analysis, which are deliverables of Work Package 2 (WP2) "Comparative Analysis of Data." The guidelines provide a framework for building the capacity of professionals to handle e-evidence and contribute to fully respecting the presumption of innocence in the context of e-evidence. By ensuring that the capacity-building activities are conducted in a coherent and structured manner, the guidelines can help to achieve a more effective use of e-evidence and improve the implementation of the presumption of innocence.

Scope and aim of the guidelines

The project, started in May 2022, focuses on procedural rights of persons suspected or accused of crime, in particular on the right to be presumed innocent until proven guilty, and how it should be understood in context of applying electronic evidence. INNOCENT targets exclusively Central and Eastern Europe in order to map the similarities, best and worst practices in the region with regards to the practical application of the presumption of innocence. It further aims to enhance the cooperation between these neighbouring jurisdictions in regard to the juncture between the presumption of innocence and electronic evidence.

Work package 3's objective is advancing capacities of professionals on e-evidence. It aims to enhance the capacity of the target groups in the partner countries in regard to the presumption of innocence in the context of e-evidence and to elaborate a toolkit for handling and admissibility of e-evidence.

Under WP3, task T3.1 consists of creating guidelines for the capacity building activities.

These guidelines are created in order for the national capacity building activities to be conducted in a coherent manner and to provide general guidance when creating modules that will:

- develop and improve skills and knowledge of relevant professionals about procedural rights of persons suspected or accused of crime, in particular on the right to be presumed innocent until proven guilty in the context of applying electronic evidence;
- increase understanding of specific challenges related to use of e- evidence and provide practical guidance for handling and admitting e-evidence through use of "knowledge alliance"-approach, focusing on participants and trainers producing effective outputs together.

The following task T3.2 includes elaboration of modules for capacity building activities. The Modules consist of two types – theoretical and practical, which means that in each partner country 2 capacity building events will be held, each of which 2 days long. As an alternative capacity building events in partner countries can be organised as 1 day event, but instead of holding two events the respective partner will have to plan three or four ones. The decision should be based on stakeholders' needs and availability as well as the national context and its particularities. The first day will be focused on theory, and the second day – on practical activities. Another possibility is to have a mixture of both theoretical and practical on each day. In case of one day events, modules can be combined for e.g. theoretical sessions in the morning, practical sessions in the afternoon. Each event will welcome at least 20 target groups' representatives.

Specific goals

Trainings for professionals will focus on:

- strengthening the capacity of professionals to handle e-evidence through providing them with knowledge of issues such as the various types of e-evidence that they may encounter, how it is recovered and handled during investigations and used in criminal trials;
- increasing capacities of target groups to make clear assessment of circumstances when e-evidence should be admitted without hindering the presumption of innocence;
- discussing the admissibility of electronic evidence in judicial proceedings;
- contributing to fully respecting the presumption of innocence in the context of use of e-evidence;
- addressing the challenges of retrieving e-evidence from other jurisdictions (including the cross-border cooperation tools and methods);
- explaining the principles of best practice relating to the seizure and handling of electronic evidence.
- Develop skills in setting specific goals for e-evidence handling during investigations and criminal trial;

- Identify and prioritize key pieces of e-evidence to build a strong case;
- Improve the ability to communicate the relevance and reliability of e-evidence to judges and juries while respecting the rights of the accused.

Learning objectives

The in-depth analysis of electronic evidence and presumption of innocence leads to a conclusion that the topic is still under-explored and needs attention from both academics, policy makers and practitioners.[1] First of all, it occurred that the lack of specialised training of judges, prosecutors, LEAs is a main threat to protection of fundamental rights of suspects and accused, particularly when it comes to applying the presumption of innocence. This gap needs to be covered by workshops and relevant training sessions for the representatives of these professions.

What is more, judges face difficulties when handling e-evidence in court. It has been examined that in the past, judges seemed to be untruthful considering using electronic evidence and give a judgment basing on its content. What is particularly important is to arm judges and prosecutors in the knowledge about the digital forensic court experts and how to cooperate with them, particularly: what kind of expert can be used in the specific case, and which questioned should be posed to acquire desirable knowledge.

What seems to be equally important is to arm judges and defence lawyers with the knowledge how electronic evidence can be verified and challenged or questioned during judicial stage of the proceedings. Assumption of the „infallibility" of the electronic evidence violates the presumption of innocence, as their content is considered as certainty. It should be well-known information what kind of non-content data must be checked to make sure about the genesis of e-evidence.

Therefore, learning objectives aim to enhance the capacity of key professionals to:

- properly approach and assess e-evidence;
- better understand procedural rights of persons suspected or accused of crime, in particular on the right to be presumed innocent until proven guilty in context of applying electronic evidence;
- detect issues relating to electronic evidence such as the various types that they may encounter, how it is recovered and handled during investigations and produced for criminal trials;
- basis for challenging the admissibility of e-evidence in court;
- improve knowledge and awareness of interinstitutional and international cooperation in the context of e-evidence'

In the short term, the main expected result of the project will be the increased capacity of the target groups - prosecutors, judges, and defence lawyers, to understand and evaluate e-evidence considering the relevant aspects of the presumption of innocence. This will reduce the risk of fair trial breach. Another effect stemming out of INNOCENT

[1] D 2.1. INNOCENT Report

implementation in the short term is the enhanced cooperation and exchange of information between the relevant stakeholders in Central and Eastern Europe region In relation to handling and admissibility of e-evidence, the gaps that will be addressed will be the general disregard of the presumption of innocence, misinterpretation, and lack of understanding of e-evidence, and lack of questioning e-evidence in front of / by the court.

In the medium term, the enhanced knowledge and capabilities of the target groups will result into strengthened cooperation forged during the planned events and supported by the contents of the INNOCENT Report, Case Law Analysis and Toolkit.

In the long term the elaborated policy guidelines and recommendations will result in an increased awareness of the relevant policy makers and potentially trigger a policy change on the practical implementation of the presumption of innocence in relation to e-evidence. The main impact of the project would be the advanced capacities of the target groups which are now identified as lacking with regards to the understanding and interpretation of e-evidence implications on the presumption of innocence. Another cornerstone impact of the project is its consistent effort to nurture not only mutual learning but also fruitful cross-border multi-stakeholder cooperation by providing for online and offline opportunities such as workshops, capacity building events, webinars, and international conference. In general, the implementation of the INNOCENT project will lead to an improved knowledge on the legislation and administrative practices related to the presumption of innocence of suspects and accused in criminal proceedings as well as to the harmonisation of the administrative practices in 8 EU countries.

Participants

Relevant stakeholder groups include: state attorneys, prosecution office, judges, investigative judges, lawyers, legal aid practitioners

Prospective participants can be recruited for the training through the respective national Judicial Academy and bar associations, representatives of the academia or by publishing open calls on different media outlets, sending e-mails to relevant mailing lists, publication on websites and social media platforms and by involving other stakeholders that may be acquainted with the topic and actively working on it.

In order to ensure a high level of participants' involvement, it is recommended to include as much practical modules content as possible and/or use the World café discussion approach.

In order to ensure for both participants and trainers to produce effective outputs together, organisers should consider the maximum number of participants to take into account.

In cases where the number of participants cannot be kept within the determined range, each event with 20 target group representatives, it is advisable to have more trainings in different cities, e.g. 4 cities in order to reach the targeted number.

In order to assess the participants level of expertise on the subject, a pre-evaluation questionnaire will be handed out at the beginning of the training.

In case participants cannot attend training in-person due to COVID-19 related prevention measures, trainers are encouraged to use online interactive tools that make it possible to break into small groups for certain activities, share ideas, brainstorm etc.

In case target groups (relevant stakeholders) are unable/ unwilling to participate in the envisaged project activities, all partners should have extensive partner networks through which they can reach the target groups. Enough time is envisioned to invite and select participants. Participants will be introduced to the INNOCENT concept, outputs and long-term impact in order to ensure attendance and proper engagement. An appropriate budget has been distributed to provide for services' delivery/supply, and catering costs of events' participants.

Speakers / Trainers

Trainers should be professionals with different expertise, knowledge and backgrounds including academics, legal practitioners working as state prosecutors, judges and lawyers, who are experienced in the area of e-evidence. In addition, inviting expert witnesses as speakers might be considered as well.

An interdisciplinary approach should be applied when possible as it offers different perspectives on the subject and is critical to the study of complex themes. Along with legal experts of different backgrounds, the considered disciplines include sociologists, political scientists, IT experts and legal scholars.

The above professionals do not need to have specific training skills. It should be up to the trainer / facilitator to ensure that their contents are delivered in the most conducive learning environment for the trainees.

Having more than one trainer brings numerous advantages including better management of the group, feedback from breakout sessions, responding to trainees' needs while training is in progress etc., but it has to be assessed in line with the project budget.

When working with a professionally homogenous group of participants, it helps to have a co-trainer who shares the professional background of the trainees or, at least, as a speaker on one of the modules.

It helps to open a training session with the introductions of all participants. Based on the specific circumstances, the trainer will decide the most appropriate way of doing it. It can be formal or informal and creative; it can be an ice breaking exercise that allows participants to take turns to introduce themselves. It can also be formal and straightforward, sharing with the entire group, one or two personal information the trainer deems fit. It is not necessarily a moment of direct interaction and/or discussions between participants.

Information on the Innocent project should be provided. Results of main activities and research findings could be shared with participants.

Methods and approach

Capacity building activities will be organised as 2 events, each of which 2 days long. Each event should welcome 20 target groups' representatives. Ideally, they will be organised in two different cities in each partner country. The first day should focused on theory, and the second day – on practical activities. As an alternative capacity building events in partner countries can be organised as 1 day event, but instead of holding two events the respective partner will have to plan four ones. The decision should be based on stakeholders' needs and availability as well as the national context and its particularities.

Some of the advised methods of approach are:

- theoretical overview by key professionals
- applicable legal framework
- case studies
- real life examples
- discussion with academic professionals
- icebreaker activities
- experience exchange
- practical exercises
- demos
- PPTs (lecturing aspect)
- peer learning

Possible challenges and mitigation measures

Risk number	Description	Proposed mitigation measures
1.	Target groups (relevant stakeholders) are unable/ unwilling to participate in the envisaged project activities (low)	All partners have extensive partner networks through which they can reach the target groups. Enough time is envisioned to invite and select participants. Participants will be introduced to the INNOCENT concept, outputs and long-term impact in order to ensure attendance and proper engagement. Appropriate budget has been distributed to provide for services' delivery/supply.

2.	Unavailability of participants to attend due to their tight schedules and numerous commitments (low)	An advanced planning and send out 'save the date' as soon as possible might be deployed as mitigation measures. Another measure can be to limit the national events to one day event instead of two days event to make it more accessible in terms of workload and time needed.
3.	COVID-19 unforeseen negative impacts (medium)	Regular communication and early planning of events is envisaged to follow the best approach depending on the current situation.

Timeline of activities

Capacity building activities should be held in participating countries during M12-M16, namely, between May and September 2023. Taking into the account the judicial vacation during summer and potential unavailability of target groups, it is suggested that the events take place in June at the latest or in September.

Sample timeline:

- ✓ April- select a city, fix a date, send invitations and confirm speakers, start engaging relevant stakeholders, send out save the date
- ✓ May- draft agenda, book venue, invite external speakers, arrange catering
- ✓ June-1st week-event in the first city of choice
- ✓ June-2nd week-event in the second city of choice

Strategic planning

For example, the opportunity to hold the national events in cooperation with local courts and/or prosecution services or the respective Judicial Academy.

March:

Review and finalize the capacity-building plan for the participating countries
Identify the cities and venues for the events and secure the necessary permits and approvals
Initiate discussions with local courts, prosecution services, and Judicial Academy for potential collaboration and partnership
Develop a comprehensive timeline for the activities

April:

Send official invitations to the target groups and confirm participation

Engage relevant stakeholders and partners for the events
Confirm the availability and participation of external speakers and resource persons
Prepare and distribute save-the-date notices and promotional materials

May:

Develop the detailed agenda and program for the events, including the topics, sessions, and speakers
Finalize the selection of the catering, transportation, and accommodation providers
Set up the registration and feedback mechanisms for the participants
Review and finalize the logistical and operational plan for the events

June:

Hold the first week event in the first city of choice, with close coordination and support from the local partners
Conduct the second week event in the second city of choice, with the same level of preparation and execution
Facilitate the capacity-building sessions and ensure the effective delivery of the knowledge and skills to the target groups
Monitor and evaluate the outcomes and impacts of the events, including the level of participation, satisfaction, and learning

July-August:

Analyze the feedback and lessons learned from the events and prepare the necessary reports and assessments
Share the results and recommendations with the relevant stakeholders and partners
Develop a follow-up plan for sustaining and scaling up the capacity-building activities

September:

Closeout the capacity-building program and document the achievements and challenges
Review and reflect on the overall process and outcomes of the program
Prepare for future capacity-building initiatives and collaborations with the partners and stakeholders.

Selection of cities where activities are carried-out

Capacity building activities ideally should be carried out in two different cities in each partner country. The method of selection of the cities depends on national specific context. They can be selected based on identified needs, available statistics, or the number of interested parties in order to reach the target number of participants.

Evaluation

In order to assess participants' familiarity and experience with e-evidence and respect of presumption of innocence in this context, a pre-training questionnaire is developed. Moreover, it will allow us to manage participants' needs and expectations in an effective manner.

It is recommended to adapt it to the specific situation of target groups and national contexts. Additionally, some optional questions are included in the questionnaire, and it is up to the trainers to decide whether or not to incorporate them into the intended version depending on the type of training, target group etc.

A sample of pre-training questionnaire can be found in Appendix 2:

In order to assess the immediate impact of the training, a post-training questionnaire has been developed. The feedback can be done both in paper or online via Microsoft Forms application depending on the needs of the activity. It is recommended that users adapt it to the specific situation of their target groups and national context. Additionally, some optional questions are included in the questionnaire and it is up to the trainers to decide whether or not to incorporate them into the version they intend to use, depending on the type of training, target group etc.

A sample post-training questionnaire can be found in Appendix 3.

Alongside specially designed feedback forms detailed below, the INNOCENT team will also kindly ask the participants to complete the target EU survey as per the requirement of DG Justice and Consumers of the European Commission. Considering that INNOCENT is funded by the Justice Programme, the following link will be distributed to the participants: https://ec.europa.eu/eusurvey/runner/Justice_2021-2027#page0.

Appendix 1 Agenda Sample

Day 1

Pre Evaluation Questionnaire- to be handed out before training starts

09:30 - 10:00	Registration
10:00 - 10:30	Introductory words, Introducing INNOCENT project (aims/goals)
10:30 - 11:15	Module of choice and discussion
11:15 - 11:45	Coffee break
11:45 - 12:30	Module of choice and discussion
12:30 - 13:30	Moot court case
13:30 - 14:30	Lunch break
14:30 - 15:15	Module of choice and discussion
15:15 - 15:30	Coffee break
15:30 - 16:30	Moot Court case
16:30 – 17:00	Closing remarks, Post Evaluation

Day 2

09:30 - 10:00	Registration
10:00 - 10:45	Module of choice and discussion
10:45 - 11:00	Coffee break
11:00 - 12:00	Moot Court case
12:00 - 13:00	Lunch break
13:00 - 14:00	Panel discussion
14:15 - 14:30	Coffee break
14:30 - 15:30	World café or Moot Court case
15:30 - 16:00	Closing remarks, Post-training Evaluation

Appendix 2 Pre-training questionnaire

Title of the training:

_____

Location and date:

_____

Instructions: Please tick the box that reflects your opinion in relation to the statements below or write your answer into the text box.

What describes best your gender identification?

- Female
- Male
- Transgender
- Intersexual
- _____

Profession/role:

_____

Have you already participated in training/education/workshops on the topic of the presumption of innocence in the context of e-evidence?

- Yes
- No

1. How familiar are you with e-evidence?

- not at all
- somewhat familiar
- very familiar

2. How familiar are you with presumption of innocence in the context of e-evidence?

- not at all
- somewhat familiar
- very familiar

3. To what extent do you encounter e-evidence in your work?

- never
- rarely
- sometimes
- often
- everyday

In case you have encountered e-evidence in your work, please describe what are the challenges/problems faced in relation to its handling and implementation.

How would you rate your knowledge on the topic of the training?

- very weak
- weak
- good
- very good
- excellent

Appendix 3 Event-planning checklist

The event planning checklist:

- ✓ select a city
- ✓ fix a date
- ✓ start engaging relevant stakeholders
- ✓ send out save the date
- ✓ draft agenda
- ✓ book venue
- ✓ invite external speakers
- ✓ arrange catering
- ✓ print materials
- ✓ establish registration form
- ✓ draft list of participants
- ✓ prepare project feedback form and EC feedback form
- ✓ consent forms for photos and others
- ✓ draft certificates for participation
- ✓ follow up with attendees (send out materials, thanks for attending)
- ✓ draft news for the carried-out event and share it

Appendix 4 Feedback form

INNOCENT CAPACITY-BUILDING ACTIVITIES

Instructions: Please check the box that reflects your opinion in relation to the statements below or write your answer into the text box.

CONTENT

1. The content of the training was of interest to me.

- ☐ Yes, completely
- ☐ To a great extent
- ☐ To some extent
- ☐ Partly
- ☐ No

2. During the training I learned new and interesting information.

- ☐ Yes, completely
- ☐ To a great extent
- ☐ To some extent
- ☐ Partly
- ☐ No

3. To me, the content of the training was relevant to my professional context.

- ☐ Yes, completely
- ☐ To a great extent
- ☐ To some extent
- ☐ Partly
- ☐ No

4. Which of the sessions will be most useful for you? Why?

5. Which was the most interesting topic for you?

FACILITATION

6. The event facilitated the exchange of practices and communication with other participants.
- □ Yes, completely
- □ To a great extent
- □ To some extent
- □ Partly
- □ No

7. The trainers/facilitators presented the topics in an interesting and engaging manner.
- □ Yes, completely
- □ To a great extent
- □ To some extent
- □ Partly
- □ No

8. The trainers/facilitators managed to create a pleasant atmosphere.
- □ Yes, completely
- □ To a great extent
- □ To some extent
- □ Partly
- □ No

9. The trainers/facilitators were competent and well prepared.
- □ Yes, completely
- □ To a great extent
- □ To some extent
- □ Partly
- □ No

10. The trainers/facilitators provided all participants with the opportunity to ask questions and share opinions.
- □ Yes, completely
- □ To a great extent
- □ To some extent

- ☐ Partly
- ☐ No

11. The event included a variety of methods to facilitate the learning of the content.
- ☐ Yes, completely
- ☐ To a great extent
- ☐ To some extent
- ☐ Partly
- ☐ No

LOGISTICS AND LEARNING MATERIALS

12. The duration of the different sessions of the event was well balanced.
- ☐ Yes, completely
- ☐ To a great extent
- ☐ To some extent
- ☐ Partly
- ☐ No

13. The training environment (room, technical aspects, logistics, coffee breaks, etc.) contributed to creating a pleasant work atmosphere.
- ☐ Yes, completely
- ☐ To a great extent
- ☐ To some extent
- ☐ Partly
- ☐ No

14. The learning materials provided are well structured and can be used even after the training.
- ☐ Yes, completely
- ☐ To a great extent
- ☐ To some extent
- ☐ Partly
- ☐ No

OUTCOMES

15. My understanding of using e-evidence increased.
- ☐ Yes, completely
- ☐ To a great extent
- ☐ To some extent
- ☐ Partly
- ☐ No

Can you please explain in what way? (optional)

16. I will embed the learned during my daily work.

- □ Yes, completely
- □ To a great extent
- □ To some extent
- □ Partly
- □ No

18. What did you like the most about the training?

19. Which parts of the training could be improved?

20. Additional comments and recommendations

Appendix 5 Capacity Building Modules

The length and the topics covered should be adapted to the national context and needs of the target group. The selection of modules and particular topics that are going to be covered during each national capacity building event should be aligned with level of knowledge and competence of the participants as well as the speakers who are going to join and their background.

The modules will be divided into theoretical and practical ones.

The contents of the training modules for professionals are focused on topics relevant for handling and admissibility of e-evidence as well as on how the presumption of innocence should be protected in this context.

All trainings should be held in person when possible. Alternatively, taking into account country specific situations regarding COVID-19 pandemic and other circumstances, 3 different online options for organising the training are suggested:

1. Hybrid model – participants are present partly online, partly at the venue (e.g. 10 of them at the venue, 15 online) and trainers are present at the venue.

2. Model 2 – all participants are present online, and trainers are present at the venue.

3. Model 3 - online model, where all the participants and trainers are present online.

Training module contents for professionals

The modules are based on D2.1. INNOCENT Report and D2.2 INNOCENT case law analysis as deliverables of Work Package 2 (WP2) "Comparative Analysis of Data". In addition, a co-creation workshop was held in Poznan with relevant stakeholders. They have provided insights from their practice and what they really need when it comes to interpreting and using e-evidence in the context of the presumption of innocence. They could be divided into theoretical and practical modules or could be a combination of both as presented below.

The content of modules aims to answer the needs that have been indicated in project conclusions of the "European Informatics Data Exchange Framework for Courts and Evidence" project[2] :

1) as proof of the extent to which electronic evidence is less willingly accepted at court, it was observed that in many cases judges are mistrustful and ask for more guarantees than with other kinds of evidence,

[2] MAP OF OBSTACLES AND FACILITATING FACTORS BEFORE VALIDATION, European Informatics Data Exchange Framework for Courts and Evidence project, 2015, available at:http://s.evidenceproject.eu/p/e/v/evidence-ga-608185-d7-2-420.pdf

2) one of the reasons why judges and prosecutors often reject electronic evidence in trials is that they do not understand the nature and characteristics of this kind of evidence very well,

3) many working in the legal profession (judges, lawyers, etc.) have not received adequate training in the management of electronic evidence (for example, prosecutors were found to lack computer skills),

4) there is a widespread shortage of courses that offer structured, continuous and certified training in the field of electronic evidence management,

5) the shortage or lack of specialised judicial services is a serious impediment to the speed and effectiveness of electronic evidence collection and management.

What seems to be equally important is to arm judges and defence lawyers with the knowledge how electronic evidence can be verified and challenged or questioned during judicial stage of the proceedings. Assumption of the „infallibility" of the electronic evidence violates the presumption of innocence, as their content is considered as certainty. It should be well-known information what kind of non-content data must be checked to make sure about the genesis of e-evidence.

Introduction to the INNOCENT project and e-evidence topic

This introductory module is foreseen as an introduction to the INNOCENT project objectives as well as the project topic, aiming at providing the context of the importance and use of electronic evidence, regulative framework and potential issues and challenges concerning the growing number of criminal cases that require exchange of data and handling e-evidence across borders.

The introduction should give the brief overview of the training which will cover topics of handling of electronic evidence during its entire lifecycle (the acquisition and collection, decryption, analysis, preservation, admissibility, use and exchange of electronic evidence).

Module 1: E-Evidence Collection - Balancing Fairness and Digital Forensics

Overview

Dear trainers,

Electronic evidence (e-evidence) has become an increasingly important aspect of criminal investigations and prosecutions in the European Union (EU). This is due to the widespread use of digital devices and the internet in modern society. E-evidence can provide valuable information in criminal investigations, but it also poses significant

challenges to the criminal justice system, particularly in terms of balancing the need for effective investigation and prosecution with the rights of the accused, including the presumption of innocence.

In this training module, we will explore the legal framework governing the collection of e-evidence in the EU, with a focus on the balance between fairness and digital forensics. We will examine the role of authorities involved in collecting e-evidence, the methods used to ensure authenticity and integrity of the data, the imbalance of power between the defence and criminal justice authorities, the chain of custody, and admissibility tests that apply to e-evidence.

Legal Framework Governing E-evidence Collection:

The legal framework governing e-evidence collection in the EU is complex and involves a range of legal instruments, including the EU Charter of Fundamental Rights, the European Convention on Human Rights, the EU Data Protection Regulation, and various national laws. The EU Charter of Fundamental Rights provides that everyone has the right to a fair trial, which includes the right to be presumed innocent until proven guilty. The European Convention on Human Rights further protects this right and requires that any interference with this right is necessary and proportionate.

The EU Data Protection Regulation sets out the rules for the processing of personal data by both public and private bodies. It aims to protect the fundamental rights and freedoms of individuals, including the right to privacy. The regulation imposes obligations on data controllers, such as criminal justice authorities, to ensure that the processing of personal data is lawful, fair, and transparent.

The national laws of each EU member state also play a crucial role in governing e-evidence collection. These laws can vary significantly between member states, and it is essential to understand the specific laws that apply in each case.The introduction should give an overview of the term and types of e-evidence, including an overview of the types of e-evidence most commonly requested by the authorities, which e.g. include connection logs, names, registration IP addresses, telephone numbers, billing and payment data, device location and e-mail address.

Authorities Involved in E-evidence Collection:

The collection of e-evidence involves various authorities, including law enforcement agencies, prosecutors, judges, and forensic experts. The model of authorities involved in e-evidence collection can impact the presumption of innocence and the fairness of the criminal justice system.

Judicial oversight is crucial in ensuring that the collection of e-evidence is necessary, proportionate, and respectful of the rights of the accused. However, the level of

oversight required can depend on the type of data being collected and the level of intrusiveness involved.

For example, subscriber data, such as the name, address, and phone number of the user, may require less oversight than content data, such as emails or text messages. Similarly, the level of oversight required may depend on whether the data is being collected directly from the suspect or from a third party, such as a service provider.

Methods for Ensuring Authenticity and Integrity of E-evidence:

The authenticity and integrity of e-evidence are essential for ensuring that it is admissible in court and reliable for the purposes of the criminal investigation. Criminal justice authorities must use appropriate methods to ensure that e-evidence is authentic and has not been tampered with.

One method for ensuring authenticity and integrity is the use of digital signatures or hashes. These are cryptographic methods that can be used to verify that the data has not been altered since it was collected. Another method is the use of forensic tools, such as write-blockers, which prevent the alteration of data during the collection process.

- The Imbalance of Powers between Defence and Criminal Justice Authorities:

  There is often an imbalance of powers between the defence and criminal justice authorities with regard to the collection of e-evidence. Criminal justice authorities have extensive powers to collect and analyze e-evidence, while the defence may have limited access to the same evidence.

  To address this imbalance, it is essential to ensure that the defence has adequate resources and expertise to review and challenge the e-evidence presented by the prosecution. This can include the provision of legal aid, the appointment of expert witnesses, and the provision of training and education for defence lawyers on e-evidence collection and analysis.

- The Chain of Custody:

  The chain of custody is crucial in ensuring that the handling of e-evidence respects the presumption of innocence. The chain of custody refers to the process of documenting the movement of evidence from the time it is collected until it is presented in court. This process ensures that the evidence is not tampered with or contaminated during the investigation.

  Criminal justice authorities must document every step in the chain of custody, including who collected the evidence, when it was collected, where it was stored,

and who had access to it. They must also ensure that the evidence is stored securely and that only authorized personnel have access to it.

- Verification of the Lawfulness, Authenticity, and Accuracy of E-evidence:

  Before e-evidence can be admitted in court, it must be verified for its lawfulness, authenticity, and accuracy. This verification process involves a range of methods, including the use of digital signatures or hashes, forensic tools, and expert analysis.

  The authenticity and accuracy of e-evidence can be challenged by the defence, and it is essential to ensure that the defence has access to the same resources and expertise as the prosecution to challenge the evidence.

- Admissibility Tests for E-evidence:

  Admissibility tests for e-evidence are similar to those for traditional evidence, but there are some differences due to the unique nature of e-evidence. The primary admissibility test for e-evidence is relevance. E-evidence must be relevant to the case and must have a probative value, which means that it must have the potential to prove or disprove a fact in the case.

  Other admissibility tests for e-evidence include the reliability test, which ensures that the evidence is reliable and trustworthy, and the authenticity test, which ensures that the evidence is what it purports to be. The hearsay rule also applies to e-evidence, which means that e-evidence that is not based on personal knowledge or observation may be excluded.

Module I Checklist

- The collection of e-evidence is a complex process that involves various authorities and legal frameworks. Balancing the need for effective investigation and prosecution with the rights of the accused, including the presumption of innocence, is crucial to ensuring a fair and just criminal justice system.
- Judicial oversight, methods for ensuring authenticity and integrity, the imbalance of powers between defence and criminal justice authorities, the chain of custody, and admissibility tests for e-evidence are all critical aspects of e-evidence collection.
- Training and education for criminal justice authorities and defence lawyers are essential to ensure that all parties understand the legal framework and procedures for e-evidence collection. By ensuring that e-evidence is collected lawfully, ethically, and with the proper safeguards in place, we can achieve a fair and just criminal justice system that respects the rights of all parties involved.

Questions for further consideration in the discussion:

- According to what rules e-evidence is collected?

- How does the model of authorities involved in collecting e-evidence impact on the presumption of innocence? Is judicial (or other independent) oversight always needed or does it depend on the type of data which may be of different use in the proceedings and level of intrusiveness (for example subscriber vs content data)?
- What methods should be used by authorities to ensure authenticity and integrity of the data?
- Is there an imbalance in powers between the defence and criminal justice authorities with regard to collecting e-evidence? If so, how to enhance the position of the defence?
- How does the chain of custody ensure that handling of e-evidence respects the presumption of innocence?
- What are the methods of verification of the lawfulness, authenticity and accuracy of the collected data?
- What admissibility tests should apply to e-evidence? Is this approach different from 'regular' evidence?

Further readings:

- Sonmez, Y. U., & Varol, A. (2017). Review of evidence collection and protection phases in digital forensics process. *International Journal of Information Security Science*, *6*(4), 39-45.
- Turnbull, B., & Slay, J. (2007, January). Wireless forensic analysis tools for use in the electronic evidence collection process. In *2007 40th Annual Hawaii International Conference on System Sciences (HICSS'07)* (pp. 267a-267a). IEEE.
- Dykstra, J., & Riehl, D. (2012). Forensic collection of electronic evidence from infrastructure-as-a-service cloud computing. *Rich. JL & Tech.*, *19*, 1.
- Wang, B., & Liu, Y. (2019). Collection and judgment of electronic data evidence in criminal cases: From the perspective of investigation and evidence collection by public security organs. *Journal of Forensic Science and Medicine*, *5*(4), 187-194.
- Newman, R. C. (2007). *Computer forensics: evidence collection and management*. CRC Press.
- Kenneally, E. E., & Brown, C. L. (2005). Risk sensitive digital evidence collection. *Digital Investigation*, *2*(2), 101-119.

Module 2: Expert Witnesses in E-Evidence - Assessing and Handling Digital Data for Legal Proceedings

Overview:

The module activities consider following distinctions of electronic evidence:

- data stored and data gathered real-time,
- content and non-content data[3].

[3] Study on the retention of electronic communications non-content data for law enforcement, 2020, Final report, https://www.statewatch.org/media/1453/eu-com-study-data-retention-10- 20.pdf

It is assumed that different rules, requirements, and practices apply for evidence considering what type of electronic evidence it is. In the realm of E-Evidence and EU Law, a crucial assumption is that the treatment of evidence varies depending on the specific type of electronic evidence under consideration. This assumption acknowledges that disparate rules, requirements, and practices come into play when dealing with diverse categories of electronic evidence.

The recognition of this assumption highlights the multifaceted nature of electronic evidence within the legal framework. Given the diverse forms that electronic evidence can assume, such as emails, text messages, social media posts, digital documents, or computer-generated records, it is reasonable to expect that different rules and practices will govern their admissibility, authenticity, and the manner in which they are collected, preserved, and presented in legal proceedings.

By acknowledging the distinct rules, requirements, and practices that apply to different types of electronic evidence, EU Law strives to ensure that the complex intricacies of digital information are appropriately considered within the legal system. This acknowledgement reflects a deep understanding of the unique challenges posed by electronic evidence and underscores the need for tailored approaches to its treatment based on its specific characteristics and the legal context in which it is presented.

This module is focused on technical issues concerning electronic evidence - how they should be acquired, preserved, collected, decoded, analysed stored, presented, what are the methods of interference (e.g. deleting files, recovering them, content modification) and how their authenticity can be verified.

The next field that is further explored is the way that electronic evidence are preserved and stored, in the context of presumption of innocence rule. What can be seen as particularly important is to set a rule package on that to: avoid files modification after possessing e-evidence and interference of the third parties, enable PSACs (Persons Suspected or Accused of Crimes) and defence lawyers to check the authenticity of the electronic evidence, the chain of custody and eventually, to challenge evidence in the court.

There are more and more technological challenges such as the retention of dynamic IP addresses, 5G and Internet of Things.[4] Within the realm of E-Evidence and EU Law, technological challenges continue to arise as technology advances. One of the latest challenges concerns the retention of dynamic IP addresses, the advent of 5G, and the Internet of Things (IoT). Dynamic IP addresses are IP addresses that change frequently and are often used by internet service providers (ISPs) to conserve IP address space. Retaining dynamic IP addresses presents a challenge for law enforcement agencies as they try to identify the user responsible for a particular action on the internet. For example, in a criminal investigation, law enforcement may need to identify the individual who sent a threatening email or engaged

[4] Ibid.

in online harassment. However, with dynamic IP addresses, the user's identity may change each time they log on to the internet, making it difficult to trace their activities.

The emergence of 5G technology and the IoT presents additional challenges for E-Evidence and EU Law. 5G technology promises faster speeds, more bandwidth, and lower latency, which could make it more challenging to monitor and intercept communications. With the IoT, an increasing number of everyday devices are connected to the internet, such as smart homes, cars, and wearable devices. These devices can generate vast amounts of data that may be relevant in legal proceedings, but accessing and analyzing this data can be complex and time-consuming.

Overall, the evolving technological landscape presents ongoing challenges for E-Evidence and EU Law. The retention of dynamic IP addresses, the rise of 5G technology, and the growth of the IoT are just a few examples of the challenges that legal practitioners and law enforcement agencies must grapple with to effectively use electronic evidence in legal proceedings.

The following practical examples demonstrate how the retention of dynamic IP addresses, the impact of 5G technology, and the proliferation of IoT devices present real-world challenges in E-Evidence and EU Law:

1. Cybercrime Investigation: In a cybercrime investigation, law enforcement authorities may need to trace the source of a cyber attack, such as a distributed denial-of-service (DDoS) attack, where multiple devices flood a target server with traffic to overwhelm it. With the increasing use of botnets, which are networks of infected computers controlled by a single attacker, dynamic IP addresses are often used to obfuscate the origin of the attack. Law enforcement agencies face the challenge of identifying the actual perpetrator behind the attack when the IP address changes frequently. They may need to collaborate with ISPs, utilize advanced network monitoring techniques, and employ forensic analysis to piece together the evidence and track down the responsible party.

2. Data Collection in IoT-enabled Devices: With the proliferation of IoT-enabled devices, such as smart home appliances or wearable devices, these devices generate significant amounts of data that may be relevant to legal proceedings. For instance, in a personal injury case, data from a smartwatch could provide insights into an individual's physical activities leading up to an accident. However, accessing and analyzing this data presents challenges due to the diverse nature of IoT devices, their proprietary software, and varying data formats. Moreover, privacy concerns and data protection regulations must be carefully navigated to ensure compliance while obtaining and processing such data as evidence.

Addressing the challenges from these examples requires the development of effective legal frameworks, a collaboration between law enforcement agencies and technology providers,

and the deployment of advanced investigative techniques to ensure that electronic evidence can be appropriately collected, preserved, and utilized in legal proceedings.

The overall module objective is to provide an in-depth understanding of the role of expert witnesses, specifically forensic examiners, in the assessment and handling of electronic evidence (e-evidence) within the context of criminal proceedings, while addressing the challenges and implications of emerging technologies.

This advanced training module aims to educate participants on the complex role of expert witnesses in assessing and managing e-evidence in criminal proceedings. The module assumes participants have extensive prior knowledge and experience in the field. By the end of the module, participants should be able to:

- Differentiate between various types of e-evidence and the specific rules, requirements, and practices that apply to each.
- Understand the technical issues surrounding e-evidence, including acquisition, preservation, collection, decoding, analysis, storage, presentation, interference methods, and authenticity verification.
- Recognize the importance of preserving and storing e-evidence in the context of the presumption of innocence and the role of expert witnesses in this process.
- Address the challenges posed by emerging technologies such as dynamic IP addresses, 5G, and the Internet of Things.

Module 2 Outline:

Types of Electronic Evidence: Distinctions and Implications

a. Data stored vs. data gathered in real-time:
    - Data stored: Refers to electronic information that is stored or recorded in a fixed medium, such as hard drives, databases, or cloud storage. It encompasses electronic data that has been previously created, transmitted, or received and is retrievable for analysis and use as evidence in legal proceedings.
    - Data gathered in real-time: Refers to electronic information that is collected or intercepted contemporaneously as it is being transmitted or generated, without being stored or recorded in a fixed medium. It includes real-time monitoring or capturing of electronic communications or activities, such as live interception of emails, instant messages, or digital transactions.
b. Content and non-content data:
    - Content data: Refers to the substantive information contained within electronic communications or documents. It encompasses the actual text, images, audio, video, or other tangible information transmitted, stored, or presented. Examples include the body of an email, the text of a chat conversation, or the contents of a digital file.

- Non-content data: Refers to the metadata or contextual information associated with electronic communications or activities, which provides details about the communication or transaction but does not encompass the substantive content. It includes information such as sender and recipient addresses, date and time of transmission, IP addresses, call logs, or website visitation records.

c. The role of expert witnesses in differentiating e-evidence types:
   - Expert witness: Refers to a qualified professional who possesses specialized knowledge, skills, and experience in a specific field relevant to electronic evidence. In the context of e-evidence, an expert witness is someone who assists the court, legal practitioners, and other parties in understanding, interpreting, and analyzing complex electronic evidence.
   - Differentiating e-evidence types: Refers to the expertise of expert witnesses in distinguishing and explaining the various categories and characteristics of electronic evidence. They possess the knowledge and technical proficiency to differentiate data stored from data gathered in real-time, identify content and non-content data, and provide clarity on the implications and legal treatment of each type of electronic evidence in legal proceedings. Expert witnesses play a vital role in providing unbiased opinions, conducting forensic examinations, presenting technical analysis, and assisting in the admissibility and evaluation of e-evidence.

Technical Issues in E-Evidence Assessment and Management

a. Acquisition, preservation, and collection of e-evidence
   - Acquisition: Refers to the process of obtaining electronic evidence from its source or relevant storage medium. It involves legally and technically sound methods for capturing or copying electronic data, ensuring its integrity and admissibility in legal proceedings.
   - Preservation: Involves the actions taken to maintain the integrity and original state of electronic evidence once it has been acquired. It includes steps to prevent alteration, deletion, or unauthorized access to the evidence during storage or handling.
   - Collection: Refers to the systematic gathering of electronic evidence, including the identification, location, and retrieval of relevant data sources. It involves employing appropriate tools and techniques to secure and extract electronic evidence in a forensically sound manner.

b. Decoding and analysis of e-evidence
   - Decoding: Refers to the process of converting encoded or encrypted electronic evidence into a readable format. It involves the application of specialized tools, algorithms, or decryption methods to reveal the content or meaning of encrypted or encoded data.

- Analysis: Involves the examination and interpretation of electronic evidence to extract relevant information, identify patterns, establish connections, and draw conclusions. It may include techniques such as data filtering, keyword searching, metadata analysis, or forensic analysis to uncover hidden or deleted data.

c. Storage and presentation of e-evidence
   - Storage: Refers to the secure and reliable storage of electronic evidence, ensuring its integrity, accessibility, and preservation for future use in legal proceedings. It involves employing appropriate storage media, encryption, access controls, and backup strategies to safeguard the evidence from loss, alteration, or unauthorized access.
   - Presentation: Involves the effective and organized display of electronic evidence in a legal setting, such as a courtroom. It includes presenting the evidence in a clear, understandable format that supports the arguments or positions of the parties involved. This may involve the use of visual aids, summaries, timelines, or expert testimony to assist in the comprehension and evaluation of the evidence.

d. Interference methods: deleting files, recovering data, and content modification
   - Interference methods: Refers to actions taken by individuals to manipulate or alter electronic evidence with the intention of concealing or distorting information. Common interference methods include deleting files or data, attempting to recover deleted or hidden data, or modifying the content or metadata of electronic evidence.
   - Data recovery: Involves the process of retrieving deleted, damaged, or hidden data from electronic storage devices. It may utilize specialized software, forensic techniques, or hardware-based methods to extract and reconstruct data that has been deliberately or accidentally removed from a storage medium.
   - Content modification: Refers to the intentional alteration or modification of the content or metadata of electronic evidence. This can involve changing the actual text, images, or other information contained within the evidence, as well as manipulating the associated metadata, timestamps, or file attributes.
   - Authenticity verification: Authenticity verification in the context of e-evidence involves establishing the origin, integrity, and unchanged nature of electronic evidence. It includes methods and techniques to ensure that the evidence has not been tampered with, altered, or falsified, and that it can be attributed to the purported source or creator with a high level of confidence. Authentication may involve digital signatures, hash values, chain of custody documentation, or expert testimony to support the veracity of electronic evidence.

Expert Witnesses and the Presumption of Innocence

a. The significance of expert witnesses in preserving and storing e-evidence
   - Expert witnesses: Refers to qualified professionals with specialized knowledge and expertise in preserving and storing electronic evidence. They play a crucial role in

advising and assisting legal practitioners in ensuring the integrity, authenticity, and admissibility of e-evidence. Expert witnesses possess the technical proficiency to employ appropriate methodologies, tools, and protocols for acquiring, preserving, and securely storing electronic evidence throughout the legal process.

b. Rule packages: preventing file modification, interference, and ensuring chain of custody

- Rule packages: Refers to a set of predefined rules, protocols, and procedures designed to prevent file modification, interference, and ensure the proper chain of custody of electronic evidence. These packages outline best practices and standards for securing and handling e-evidence to maintain its integrity and reliability. They may include encryption measures, access controls, backup procedures, documentation requirements, and audit trails to safeguard against unauthorized modifications or tampering and to establish a clear record of custody.

c. Enabling defence lawyers to verify e-evidence authenticity

- Authenticity verification: Refers to the process of establishing the genuineness and integrity of e-evidence. It is essential for defence lawyers to verify the authenticity of electronic evidence presented by the prosecution. This may involve scrutinizing the chain of custody, examining the metadata, checking digital signatures, or consulting with expert witnesses to ensure that the evidence has not been tampered with, fabricated, or manipulated. Verification of authenticity allows defence lawyers to effectively challenge the credibility and reliability of e-evidence during legal proceedings.
- Challenging e-evidence in court: Refers to the process of questioning or contesting the validity, reliability, or admissibility of electronic evidence presented in court. Defence lawyers have the right to challenge the e-evidence provided by the prosecution through cross-examination, presenting contradictory evidence, or raising objections based on legal grounds. Challenges may focus on issues such as chain of custody, authenticity, relevance, accuracy, or the qualifications of expert witnesses. By challenging e-evidence, defence lawyers seek to cast doubt on its probative value or to exclude it from consideration by the court.

Emerging Technological Challenges

a. Retention of dynamic IP addresses

- Dynamic IP addresses: Refers to temporary, dynamically assigned Internet Protocol (IP) addresses that are assigned to devices by an Internet Service Provider (ISP) when they connect to a network. These IP addresses are subject to change each time the device connects to the network or after a certain period of time. Retention of dynamic IP addresses involves the process of capturing and storing the association between a specific IP address and the device or user that was assigned that IP address at a given time. This is important in investigations and legal proceedings to

establish the connection between an IP address and a specific user or device at a particular point in time.

b. Implications of 5G technology

- 5G technology: Refers to the fifth generation of mobile network technology that offers significantly faster data speeds, lower latency, and increased network capacity compared to previous generations. The implications of 5G technology in the context of e-evidence involve the unique challenges and opportunities it presents. These include the ability to transmit and process larger volumes of data in real-time, the increased complexity of network infrastructure, the potential for more diverse and interconnected devices, and the impact on the collection, preservation, and analysis of e-evidence. Understanding the implications of 5G technology is crucial for legal practitioners to effectively navigate the changing landscape of electronic evidence in the 5G era.

c. The Internet of Things (IoT) and its impact on e-evidence

- Internet of Things (IoT): Refers to the network of interconnected physical devices, vehicles, appliances, and other objects that are embedded with sensors, software, and network connectivity to exchange data and enable remote monitoring and control. The IoT has a significant impact on e-evidence as it expands the potential sources of electronic evidence beyond traditional computers and mobile devices. The IoT generates vast amounts of data from various interconnected devices, such as smart home devices, wearables, or connected cars. This poses challenges in terms of the acquisition, preservation, analysis, and authentication of IoT-generated e-evidence, as well as considerations regarding privacy, security, and reliability.
- The role of expert witnesses in addressing these challenges: Refers to individuals with specialized knowledge, expertise, and experience in specific areas relevant to emerging technological challenges in e-evidence. In addressing challenges related to the retention of dynamic IP addresses, implications of 5G technology, and the impact of IoT on e-evidence, expert witnesses play a crucial role. They provide technical insights, analysis, and expert opinions to legal practitioners and the court. Expert witnesses help interpret and explain the complexities of these emerging technological challenges, assist in acquiring and authenticating relevant e-evidence, propose methodologies and tools for addressing these challenges, and offer guidance on the admissibility, reliability, and probative value of e-evidence in legal proceedings. Their expertise is essential in navigating the intersection of technology and the law, ensuring a fair and informed evaluation of emerging technological challenges in the context of e-evidence.

<u>Moot Court Case:</u>

The case before the Polish court[5] is about the charge of aiding in murder by providing telecommunication data of the victim's location. The accused, Marek, used his access to work and provided the information to his friend, who committed the murder. The prosecution claims that Marek is guilty of aiding and abetting in the murder of the victim by providing the data to his friend. On the other hand, Marek's defense counsel argues that he had no intention to aid in the murder and that he only provided the data as a part of his job responsibilities. During the investigation, most of the evidence was found on the defendant's computer. A forensic computer examination was appointed to examine the evidence. However, the forensic examiner did not follow the most recent research developments and current practice for dealing with electronic files. Consequently, the respective forensic examiner's work is now the subject of a legal dispute between the defendant and the court.

Questions for the Parties:

Prosecution:

- Can you provide evidence to support your claim that the accused had an intention to aid in the murder of the victim?
- Can you explain the significance of the telecommunication data provided by the accused in the commission of the murder?
- Do you believe that the accused should be held responsible for the actions of the person who committed the murder, given that he only provided data?

Defence:

- Can you explain the nature of the defendant's job and his access to telecommunication data?
- Can you provide evidence to support your claim that the defendant had no intention to aid in the murder of the victim?
- What steps, if any, did the defendant take to prevent the person who received the data from using it to commit murder?

What is Expected from the Judge:

As a judge, you are expected to impartially evaluate the evidence presented in court and to make a fair and just decision based on the facts of the case. You should also consider the legal arguments presented by both parties and apply the relevant laws to the case. Additionally, you should address the legal dispute regarding the forensic examiner's work and its impact on the evidence presented in the case.

Module 2 Checklist:

[5] Polish Supreme Court, Judgment of 20 June 2013, Case No. III KK 12/13, LEX No. 1341691.

Types of Electronic Evidence

- Data stored
- Data gathered in real-time
- Content data
- Non-content data

Technical Issues in E-Evidence Assessment and Management

- Acquisition of e-evidence
- Preservation of e-evidence
- Collection of e-evidence
- Decoding of e-evidence
- Analysis of e-evidence
- Storage of e-evidence
- Presentation of e-evidence
- Interference methods
- Authenticity verification

Expert Witnesses and the Presumption of Innocence

- Preserve and store e-evidence
- Implement rule packages
- Prevent file modification
- Prevent third-party interference
- Ensure chain of custody
- Enable PSACs and defence lawyers to verify authenticity
- Assist in challenging e-evidence in court

Emerging Technological Challenges

- Address dynamic IP address retention
- Consider implications of 5G technology
- Understand the impact of the Internet of Things (IoT)
- Adapt to new challenges in e-evidence assessment and management

Further Readings

- Morgan, L. (2006). Authenticating Documents and Printouts of E-evidence. *Fam. Advoc.*, *29*, 43.
- Aitken, C., Roberts, P., & Jackson, G. (2010). *Fundamentals of probability and statistical evidence in criminal proceedings: guidance for judges, lawyers, forensic scientists and expert witnesses*.
- Sugisaka, K. L., & Herr, D. F. (2008). Admissibility of E-Evidence in Minnesota: New Problems or Evidence as Usual. *Wm. Mitchell L. Rev.*, *35*, 1453.

- Theophilopoulos, C. (2015). The admissibility of data, data messages, and electronic documents at trial. *Journal of South African Law/Tydskrif vir die Suid-Afrikaanse Reg*, *2015*(3), 461-481.
- Raj, K. (2020). E-Evidence: Moving Parallel with Today's World. *Issue 4 Int'l JL Mgmt. & Human.*, *3*, 709.
- Jerman Blažič, B., & Klobučar, T. (2019). Advancement in cybercrime investigation–the new European legal instruments for collecting cross-border e-evidence. In *Information Technology and Systems: Proceedings of ICITS 2019* (pp. 858-867). Springer International Publishing.

Module 3: Judicial evaluation and assessment of authenticity and integrity of e-evidence

Overview

As digital technologies continue to advance, electronic evidence (e-evidence) has become an increasingly important part of criminal investigations and court proceedings. However, ensuring the authenticity and integrity of e-evidence poses a significant challenge, as it can be easily manipulated and falsified. Therefore, it is essential for judges and legal practitioners to have a thorough understanding of the methods and techniques used to evaluate and assess the authenticity and integrity of e-evidence.

This training module aims to equip the trainers and provide a comprehensive overview of the issues surrounding the judicial evaluation and assessment of the authenticity and integrity of e-evidence. It will explore the various methods and techniques used to ensure that e-evidence is reliable, trustworthy, and admissible in court.

Part 1: Rules Governing the Collection of E-Evidence

The collection of e-evidence is subject to specific rules and regulations that vary depending on the country and the type of data being collected. Generally, the collection of e-evidence is subject to the same rules as traditional evidence, including the principle of legality, proportionality, and respect for fundamental rights.

However, there are some unique challenges associated with the collection of e-evidence, such as the ease with which it can be altered or falsified. Therefore, it is essential for legal practitioners to have a thorough understanding of the methods and techniques used to ensure the authenticity and integrity of e-evidence.

Part 2: Methods for Ensuring Authenticity and Integrity of E-Evidence

There are several methods and techniques used to ensure the authenticity and integrity of e-evidence, including:

- Digital Signatures

Digital signatures are electronic signatures that are attached to a document to ensure its authenticity and integrity. Digital signatures use a mathematical algorithm to create a unique code that is attached to the document. The code can be verified to ensure that the document has not been altered since it was signed.

- Hash Values

Hash values are unique codes generated by a mathematical algorithm that is applied to a document. The hash value is a unique identifier for the document, and any changes to the document will result in a different hash value. Hash values are used to ensure the integrity of e-evidence, as they can be used to verify that the document has not been altered since it was created.

- Time-Stamping

Time-stamping is a method used to verify the time and date of the creation, modification, or transmission of a document. Time-stamping is essential for e-evidence, as it can be used to establish the timeline of events and to verify that the document has not been altered since it was created.

- Chain of Custody

The chain of custody is the documented history of the movement of e-evidence from the time it is collected to the time it is presented in court. The chain of custody is essential for ensuring the authenticity and integrity of e-evidence, as it establishes the continuity of the evidence and the integrity of the evidence.

Part 3: Admissibility of E-Evidence

The admissibility of e-evidence is subject to the same rules as traditional evidence, including the principle of legality, proportionality, and respect for fundamental rights. However, there are some unique challenges associated with the admissibility of e-evidence, such as the ease with which it can be altered or falsified.

Therefore, legal practitioners must be aware of the different admissibility tests that apply to e-evidence. Admissibility tests for e-evidence include the following:

- Authentication

Authentication is the process of verifying that the e-evidence is what it purports to be. Authentication is essential for ensuring the admissibility of e-evidence, as it establishes the identity of the author and the integrity of the document.

- Hearsay

Hearsay is an out of-court statement that is offered as evidence to prove the truth of the matter asserted. Hearsay is generally not admissible in court, but there are exceptions for certain types of hearsay, such as business records and public records.

- Best Evidence Rule

The best evidence rule requires that the original document be presented in court, rather than a copy or a secondary source. This rule is designed to ensure that the evidence presented is the best possible evidence available.

- Chain of Custody

As mentioned in Part 2, the chain of custody is essential for ensuring the admissibility of e-evidence. The chain of custody establishes the continuity of the evidence and the integrity of the evidence, making it essential for the admissibility of e-evidence.

Part 4: Role of the Judiciary in Assessing Authenticity and Integrity of E-Evidence

The role of the judiciary in assessing the authenticity and integrity of e-evidence is essential for ensuring that justice is served. The judiciary has a duty to ensure that e-evidence is reliable, trustworthy, and admissible in court. Therefore, judges must have a thorough understanding of the methods and techniques used to evaluate and assess the authenticity and integrity of e-evidence.

Judges must also be able to assess the credibility and reliability of expert witnesses who testify about e-evidence. Expert witnesses are often called upon to perform forensic examination and to explain complex concepts related to e-evidence. Therefore, judges must be able to evaluate the credibility and reliability of expert witnesses to ensure that the evidence presented is reliable and trustworthy.

Part 5: Main takes

The judicial evaluation and assessment of authenticity and integrity of e-evidence is essential for ensuring that justice is served. Legal practitioners and judges must be aware of the various methods and techniques used to ensure the authenticity and integrity of e-evidence, as well as the different admissibility tests that apply to e-evidence.

Furthermore, judges must be able to assess the credibility and reliability of expert witnesses who testify about e-evidence. The role of the judiciary in assessing the authenticity and integrity of e-evidence is essential for ensuring that justice is served, and legal practitioners and judges must continue to develop their understanding of this area to ensure that e-evidence is used effectively and fairly in court proceedings.

Moot court case

Matjaž, a Slovenian[6] national born in 1982 and residing in Koper, has filed a complaint regarding the lack of a court order to access his mobile phone data. This evidence was allegedly used to convict him of aggravated murder in September 2009. Matjaž appeals the judgment on the grounds that the police had illegally accessed his mobile phone data and that of the victim without obtaining a court order to examine the devices.

Questions for the Parties:

Counsel for the Applicant, what specific evidence do you have to show that the police illegally accessed your client's mobile phone data?

Counsel for the Applicant, can you provide any evidence that the evidence obtained from your client's mobile phone was inadmissible and should not have been used in the criminal proceedings against him?

Counsel for the Respondent, what justification does the police have for accessing the mobile phone data without obtaining a court order?

Counsel for the Respondent, can you provide any evidence that the evidence obtained from the victim's mobile phone was obtained legally and should be admissible in court?

Counsel for the Applicant, can you provide any evidence that the evidence obtained from the victim's mobile phone was obtained illegally and should not have been used in the criminal proceedings against your client?

Role of the Judge:

The role of the judge in this moot court case is to listen to the arguments made by both parties and to make a ruling on whether the evidence obtained from the mobile phone data of both the applicant and the victim was obtained legally or illegally. The judge must determine whether the evidence obtained should be admissible in court and whether it violates the rights of the applicant under Article 6 § 1 of the European Convention on Human Rights (right to a fair trial). The judge must also ensure that both parties have a fair and equal opportunity to present their arguments and evidence.

Module 3 - Checklist

Part 1: Introduction

- Explain the importance of authenticity and integrity of e-evidence
- Highlight the challenges associated with e-evidence

Part 2: Authenticity and Integrity of E-Evidence

[6] *Svetina v. Slovenia*, ECtHR, Application No. 38059/13, Judgment of 22 May 2018.

Explain the concepts of authenticity and integrity of e-evidence
Discuss the importance of chain of custody
Discuss the methods used to ensure the authenticity and integrity of e-evidence, such as hashing and digital signatures

Part 3: Admissibility of E-Evidence

Explain the different admissibility tests that apply to e-evidence.
Discuss the best evidence rule
Highlight the importance of the chain of custody for the admissibility of e-evidence

Part 4: Role of the Judiciary in Assessing Authenticity and Integrity of E-Evidence

Discuss the role of the judiciary in assessing authenticity and integrity of e-evidence
Explain the importance of judges having a thorough understanding of the methods and techniques used to evaluate and assess the authenticity and integrity of e-evidence
Discuss the importance of judges being able to assess the credibility and reliability of expert witnesses who testify about e-evidence
Highlight the importance of judicial evaluation and assessment of authenticity and integrity of e-evidence
Emphasize the need for legal practitioners and judges to develop their understanding of this area to ensure that e-evidence is used effectively and fairly in court proceedings

Further Readings:

- Vazquez Maymir, S. (2020). Anchoring the need to revise cross-border access to e-evidence. *Internet Policy Review*, *9*(3), 1-24.
- Kubi, A. K., Saleem, S., & Popov, O. (2011, October). Evaluation of some tools for extracting e-evidence from mobile devices. In *2011 5th International Conference on Application of Information and Communication Technologies (AICT)* (pp. 1-6). IEEE.
- Naichenko, A. (2021). E-evidence and e-court in the Context of the Covid-19 Pandemic: A Study from Ukraine. *Access to Just. E. Eur.*, 163.
- Hariharan, K., Rajkumar, K., Manikandan, R., Kumar, A., & Gupta, D. (2021). Deep learning for optimization of e-evidence. *Cyber Crime and Forensic Computing: Modern Principles, Practices, and Algorithms*, *11*, 111.
- Custers, B., & Stevens, L. (2021). The use of data as evidence in Dutch criminal courts. *European Journal of Crime, Criminal Law and Criminal Justice*, *29*(1), 25-46.
- Mifsud Bonnici, J. P., Tudorica, M., & Cannataci, J. A. (2018). *The European legal framework on electronic evidence: complex and in need of reform* (pp. 189-234). Springer International Publishing.

Module 4: Protection of the presumption of innocence and other rights and guarantees

Overview:

Defendants do not have any obligation to share data with LEAs, including computer, email passwords, PINs. However, the findings in suggested literature show that such situations occur (See further reading below).. The LEAs try to encourage them by promise or threat. They can suggest that that kind of cooperation can result in shorter proceedings or milder treatment.

Early access to a defence lawyer is a key safeguard of a defendant's rights, including to be given adequate information about the right to remain silent and not to self-incriminate. Video documenting police interrogations can be a key to the protection of a defendant's right to remain silent if a defence lawyer is not present - in order to avoid any violations of the informing obligation about the right to remain silent.

What areas seem to be the main threat are the issues with reverse burden of proof, low quality data processing, reliance on untested digital expert evidence (opinion), and lack of criminal procedure guarantees in data retention, crime prevention and suspicion-based procedures.[7] The first area is the issue of reverse burden of proof, which means that the defendant is required to prove their innocence rather than the prosecution proving their guilt. This can lead to unfairness and violates the principle of innocent until proven guilty. The second area of concern is low-quality data processing. The use of electronic evidence requires specific technical knowledge, and if not handled correctly, it can lead to inaccurate or unreliable evidence being presented in court. The third area of concern is the reliance on untested digital expert evidence, which refers to the opinions of digital forensic experts that have not been sufficiently tested or validated. This can lead to the presentation of misleading or inaccurate evidence in court. The final area of concern is the lack of criminal procedure guarantees in data retention, crime prevention, and suspicion-based procedures. This can lead to abuse of power by law enforcement agencies and undermines the right to a fair trial. These areas of concern highlight the importance of ensuring that electronic evidence is collected, processed, and presented in a fair and transparent manner, with sufficient safeguards in place to protect the rights of the accused. This underscores the importance of having trained and qualified digital forensic experts who follow established protocols and procedures to ensure the reliability and admissibility of electronic evidence in legal proceedings.

Under the rule of presumption of innocence there could be found several issues: the use of compulsion, the right to remain silent, the right not to incriminate oneself,

[7] Ibid.

reversal of the burden of proof and all of them should be examined in the context of the kind of actions that violate these rights and standards and which ones do not.

Possibilities to examine/question e-evidence by defence which ensure/enhance the presumption of innocence.

When it comes to the effective remedy issues, the question must be posed: what are the consequences of breaching the right to presumption of innocence? Nevertheless, it has to be assumed that the rules and procedure will not always be respected, and the rights will be violated. It has to be considered what consequences it should presuppose.

Access to effective remedies in case of fundamental rights violation can be problematic as there are no guarantees for PSACs of the judicial control on the process of acquiring e-evidence.[8] The main concerns are caused by the lack of a duty to inform the subjects potentially affected by the proposed measure about taken actions. That seems to be contrary to existing EU privacy and data protection regulations, the principle of equality of arms and the adversarial principle in criminal proceedings.

This advanced-level training module provides an in-depth analysis of the challenges and potential threats to the presumption of innocence and other defendants' rights in the context of electronic evidence (e-evidence) within the European Union. Participants with extensive prior knowledge in this field will develop a comprehensive understanding of the key legal principles, procedural safeguards, and the role of expert witnesses in the evaluation of e-evidence.

Upon completing this training module, participants will have gained a nuanced understanding of the complexities surrounding the protection of the presumption of innocence and other defendants' rights in the context of e-evidence within the European Union. They will be equipped to analyse and address potential threats and challenges to defendants' rights, promote procedural fairness, and uphold the fundamental principles of the criminal justice system.

Module Outline:

The Presumption of Innocence and Defendants' Rights in the Digital Context

a. Theoretical foundations and underlying principles
b. The right to remain silent and not to self-incriminate
c. Reverse burden of proof
d. Challenges in data retention, crime prevention, and suspicion-based procedures

[8] S. Carrera, M. Stefan, *Access to Electronic Data for Criminal Investigations Purposes in the EU*, CEPS Papers in Liberty and Security in Europe 2020, https://www.ceps.eu/wpcontent/uploads/2020/02/LSE20120-01_JUD-IT_Electronic-Data-for-Criminal-InvestigationsPurposes.pdf

The Role of Law Enforcement Authorities (LEAs) and Compulsion in E-Evidence Collection

a. Ethical boundaries and legal constraints
b. The impact of promises or threats on defendants' rights
c. Strategies to ensure voluntary cooperation without violating defendants' rights

Safeguarding Defendants' Rights Through Early Access to Defence Lawyers

a. The importance of adequate information on the right to remain silent and not to self-incriminate
b. Video documentation of police interrogations as a protective measure
c. Balancing efficiency and fairness in investigative procedures

The Reliability and Admissibility of E- Evidence

a. Assessing the quality of data processing in criminal proceedings
b. Evaluating untested digital expert opinions
c. The role of expert witnesses in e-evidence assessment

Empowering the Defence in Examining and Questioning E-Evidence

a. Strategies to ensure and enhance the presumption of innocence
b. Identifying potential violations of defendants' rights and procedural standards
c. Effective remedies for breaches of the presumption of innocence

Access to Effective Remedies in Case of Fundamental Rights Violations

a. Challenges in judicial control over e-evidence acquisition
b. The duty to inform subjects potentially affected by proposed measures
c. Balancing EU privacy and data protection regulations with the principle of equality of arms and the adversarial principle in criminal proceedings

Moot Court Case

The case before the Croatian court[9] involves five offences - two criminal offences of sexual abuse of a child under the age of fifteen, the criminal offence of enticing children to meet sexual needs, the criminal offence of introducing children to pornography, and the criminal offence of exploiting children for pornography. The defendant, Ivan, claims that the charges against him are excessive, and the judgments are based on unlawful evidence, which violated his right to a fair trial. He argues that evidence from social media was collected without a proper search warrant.

[9] Supreme Court of Croatia, Judgment of 25 March 2021, Case No. III Kr 120/2020-3.

During the investigation, the defendant's home and other premises were searched in the presence of two adult citizens as witnesses. A laptop, tablet, several mobile phones, a USB stick, and two CDs were taken. Additionally, based on the order of the investigative judge, a further search was carried out on the defendant's cell phones and the Facebook profile of another person.

Questions for the Parties:

Prosecution:

- Can you explain the nature of the five offences with which the defendant is charged?
- Can you provide evidence to support your claim that the defendant committed these offences?
- What is your response to the defendant's claim that the evidence was collected without a proper search warrant?

Defence:

- Can you explain the circumstances surrounding the search of the defendant's home and premises?
- Can you provide evidence to support your claim that the evidence was collected unlawfully?
- What is your response to the prosecution's claims that the defendant committed the five offences?

What is Expected from the Judge:

As a judge, you are expected to impartially evaluate the evidence presented in court and make a fair and just decision based on the facts of the case. You should consider the legal arguments presented by both parties and apply the relevant laws to the case. Additionally, you should address the defendant's claim that the evidence was collected without a proper search warrant and whether this violates his right to a fair trial. Finally, you should evaluate whether the evidence presented supports the charges against the defendant and whether he is guilty of the offences with which he is charged.

Module 4 Checklist:

Understand and apply the principles of the presumption of innocence and defendants' rights in the digital context.

Evaluate the role of Law Enforcement Authorities (LEAs) in e-evidence collection and ensure ethical boundaries and legal constraints are respected.

Prioritize early access to defence lawyers for defendants, guaranteeing their rights to remain silent and not to self-incriminate.

Verify the reliability and admissibility of digital expert evidence, including the quality of data processing and evaluation of untested digital expert opinions.

Promote the involvement of expert witnesses in assessing e-evidence to ensure its authenticity, accuracy, and relevance.

Empower the defence in examining and questioning e-evidence, reinforcing the presumption of innocence and addressing potential violations of defendants' rights and procedural standards.

Provide access to effective remedies for defendants in case of fundamental rights violations, such as breaches of the presumption of innocence.

Ensure transparency and compliance with the duty to inform subjects potentially affected by proposed measures, in line with EU privacy and data protection regulations.

Balance the principle of equality of arms and the adversarial principle in criminal proceedings while respecting the privacy and data protection rights of all parties involved.

Continuously update knowledge on the evolving legal landscape and technological advancements in the context of e-evidence, to ensure effective protection of defendants' rights in the digital era.

Further readings

- Stoykova, R. (2021). Digital evidence: Unaddressed threats to fairness and the presumption of innocence. *Computer Law & Security Review*, *42*, 105575.
- Sachoulidou, A. (2023). Going beyond the "common suspects": to be presumed innocent in the era of algorithms, big data and artificial intelligence. *Artificial Intelligence and Law*, 1-54.
- Sachoulidou, A. (2022). OK Google: is (s) he guilty?. *Journal of Contemporary European Studies*, *30*(2), 284-296.
- Chavleski, A., & Galev, G. (2019). GATHERING E-EVIDENCE IN CROSS-BORDER CASES: RECENT DEVELOPMENTS IN EU LAW. *KNOWLEDGE-International Journal*, *32*(1), 155-162.
- Stoykova, R. (2021). The Presumption of Innocence as a Source for Universal Rules on Digital Evidence—The guiding principle for digital forensics in producing digital evidence for criminal investigations. *Computer Law Review International*, *22*(3), 74-82.

- Smuha, N. A. (2018). Towards the EU harmonization of access to cross-border e-evidence: Challenges for fundamental rights & consistency. *European Criminal Law Review*, *8*(1), 83-115.

Module 5: European Production and Preservation Orders-balancing between efficiency and guarantees

Module Overview

The European Union has developed several tools to facilitate cross-border criminal investigations and the cooperation between Member States in the field of criminal justice. This training module will focus on three of these tools: the European Production and Preservation Orders, the European Investigation Order, and the European Arrest Warrant.

The aim of this module is to provide an in-depth analysis of the legal framework, procedures, and issues related to these three instruments, with a particular emphasis on the balance between efficiency and guarantees in criminal investigations.

The European Production and Preservation Orders

- Legal framework and Procedure

Presently, authorities in Member States face challenges in obtaining electronic evidence, relying on lengthy judicial cooperation procedures. This process carries the inherent risk of data being moved or deleted, or resorting to voluntary cooperation with service providers that lacks reliability, transparency, accountability, and legal certainty. The new e-Evidence Regulation which should be adopted in 2023, aim to address these issues by providing national authorities with a reliable channel to obtain e-evidence while incorporating robust safeguards to protect the rights of individuals involved. In order to ensure a reliable, transparent, and expeditious exchange of e-evidence while upholding a high level of protection, the e-Evidence Regulation would offer a solution that acknowledges the volatile nature of electronic evidence and its international dimension. By adapting cooperation mechanisms to the digital era, this Regulation is planned to equip the judiciary and law enforcement with the necessary tools to effectively combat modern forms of criminality and address the way criminals communicate today. The introduction of a European Production Order would enable a judicial authority in one Member State to directly request electronic evidence from a service provider in another Member State through a decentralized IT system. The service provider would be obligated to respond within ten days, or within eight hours in cases of emergency. Additionally, a European Preservation Order would prevent the deletion of data by compelling a service provider in one Member State to preserve specific data for future retrieval. It is planned that both type of orders can only be issued within the framework of criminal proceedings to facilitate the location of individuals evading justice.

Furthermore, the new rules encompass robust safeguards and remedies to ensure the protection of fundamental rights and personal information. They include additional requirements for obtaining sensitive data and stipulate that when seeking traffic and content data from a service provider in a different jurisdiction, Member States would need to notify the national authority where the service provider is located. The notified authority would have the right to refuse the order on various grounds, such as the protection of fundamental rights or immunities and privileges.

The new legislation would also bring increased legal certainty for businesses and service providers. Currently, law enforcement authorities often rely on voluntary cooperation from service providers to disclose evidence, resulting in uncertainty and significant procedural differences among companies. The Regulation would establish a clear legal framework that outlines the rights and obligations of service providers, imposing sanctions of up to 2% of total worldwide turnover for non-compliance with European Preservation and Production Orders.

- Issues

The e-Evidence Regulation raises several issues related to the balance between efficiency and guarantees in criminal investigations. One of the main concerns is the potential for abuse of the e-Evidence system by law enforcement authorities, particularly in light of the broad scope of electronic evidence covered by the Regulation. There is also a risk that the e-Evidence system may be used to circumvent national laws on data protection and privacy.

To address these concerns, the EPPO Regulation includes a number of safeguards, such as the requirement for prior judicial authorization and the possibility of challenging the order before a judicial authority. However, the effectiveness of these safeguards will depend on the implementation and enforcement by national authorities.

The European Investigation Order

- Legal framework and Procedure

The European Investigation Order (EIO) Directive (Directive 2014/41/EU) was adopted on 3 April 2014 and entered into force on 22 May 2014. The purpose of the EIO Directive is to simplify and accelerate cross-border access to evidence in criminal proceedings, while ensuring a high level of protection of fundamental rights. Under the EIO Directive, a judicial authority in one Member State can request evidence directly from a competent authority in another Member State, without the need for a mutual legal assistance request. The EIO Directive applies to all types of evidence, including witness statements, physical evidence, and documents. The EIO Directive sets out detailed procedures for the issuing, executing, and challenging of EIOs. The requesting authority must provide detailed information about the requested evidence and the suspected criminal offence, and the executing authority must ensure that the EIO is compatible with the

fundamental rights of the affected persons, including the right to respect for private and family life, the right to the protection of personal data, and the right to a fair trial.

The EIO Directive also establishes a fast-track procedure for urgent cases, which allows the requesting and executing authorities to communicate directly and swiftly without the need for intermediaries.

- Issues

The EIO Directive also raises several issues related to the balance between efficiency and guarantees in criminal investigations. One of the main concerns is the potential for unequal access to justice, as some Member States may have less developed legal systems or less respect for fundamental rights than others. There is also a risk that the EIO system may be used to circumvent national laws on data protection and privacy.

To address these concerns, the EIO Directive includes a number of safeguards, such as the requirement for prior judicial authorization and the possibility of challenging the order before a judicial authority. However, the effectiveness of these safeguards will depend on the implementation and enforcement by national authorities.

The European Arrest Warrant

- Legal framework and Procedures

The European Arrest Warrant (EAW) Framework Decision (Council Framework Decision 2002/584/JHA) was adopted on 13 June 2002 and has been in force since 1 January 2004. The purpose of the EAW Framework Decision is to simplify and accelerate the extradition of persons who have been accused or convicted of a criminal offence in one Member State and are located in another Member State, while ensuring a high level of protection of fundamental rights.

Under the EAW Framework Decision, a judicial authority in one Member State can issue an arrest warrant for a person located in another Member State, without the need for a formal extradition procedure. The EAW Framework Decision applies to all types of criminal offences, except for certain political offences. The EAW Framework Decision sets out detailed procedures for the issuing, executing, and challenging of EAWs. The issuing authority must provide detailed information about the person sought and the criminal offence, and the executing authority must ensure that the EAW is compatible with the fundamental rights of the affected person, including the right to a fair trial and the prohibition of inhuman or degrading treatment.

The EAW Framework Decision also establishes a fast-track procedure for urgent cases, which allows the issuing and executing authorities to communicate directly and swiftly without the need for intermediaries.

- Issues

The EAW Framework Decision raises several issues related to the balance between efficiency and guarantees in criminal investigations. One of the main concerns is the potential for the extradition of persons who may face human rights violations or unfair trials in the requesting Member State. There is also a risk that the EAW system may be used for minor offences or for political purposes.

To address these concerns, the EAW Framework Decision includes a number of safeguards, such as the requirement for prior judicial authorization and the possibility of challenging the EAW before a judicial authority. However, the effectiveness of these safeguards will depend on the implementation and enforcement by national authorities.

Module outline

The European Union has developed several tools to facilitate cross-border criminal investigations and the cooperation between Member States in the field of criminal justice. The European Production and Preservation Orders, the European Investigation Order, and the European Arrest Warrant are important instruments that contribute to the efficiency and effectiveness of criminal investigations, while ensuring a high level of protection of fundamental rights.

However, these instruments also raise several issues related to the balance between efficiency and guarantees in criminal investigations, including the potential for abuse by law enforcement authorities and the risk of unequal access to justice. To address these concerns, the legal framework of these instruments includes several safeguards, such as the requirement for prior judicial authorization and the possibility of challenging the orders or warrants before a judicial authority. It is important that these safeguards are implemented and enforced effectively by national authorities to ensure that the balance between efficiency and guarantees is maintained.

Moot court case

The case[10] concerns the lawfulness of four European Investigation Orders (EIOs) issued by the Bulgarian public prosecutor's office to collect traffic and location data associated with telecommunications in Belgium, Germany, Austria, and Sweden. The data was gathered in the course of a criminal investigation against Hristo on the suspicion of illegally financing terrorist activities and participating in a criminal organization seeking to finance those activities. The question before the court is whether the EIOs were lawfully issued and whether the evidence obtained from them can be used in the criminal proceedings against Hristo.

[10] The case of *Spetsializirana prokuratura*, CJEU, Judgement of 16 December 2021, Case C-724/19.

Questions for the Parties:

Counsel for the Applicant, can you provide any evidence that the EIOs were not lawfully issued and that the evidence obtained from them should be inadmissible in the criminal proceedings against your client?

Counsel for the Respondent, can you provide any evidence that the EIOs were lawfully issued and that the evidence obtained from them should be admissible in the criminal proceedings against the applicant?

Counsel for the Applicant, can you provide any evidence that the competent authority to issue an EIO should be a judge, rather than a public prosecutor, under the principle of equivalence?

Counsel for the Respondent, can you provide any evidence that the national law transposing Directive 2014/41, which designates the public prosecutor as the competent authority to issue an EIO, is consistent with the principle of equivalence?

Counsel for the Applicant, can you provide any evidence that the recognition decision taken by the competent authority of the executing state may not validly replace the decision that should have been taken by the judge of the issuing state in order to safeguard the principles of legality and inviolability of private life?

Counsel for the Respondent, can you provide any evidence that the recognition decision taken by the competent authority of the executing state is compatible with Article 6 and Article 9(1) and (3) of Directive 2014/41?

Role of the Judge:

The role of the judge in this moot court case is to determine whether the EIOs issued by the Bulgarian public prosecutor's office to collect traffic and location data associated with telecommunications in Belgium, Germany, Austria, and Sweden were lawfully issued and whether the evidence obtained from them is admissible in the criminal proceedings against Hristo. The judge must also consider whether the national law designating the public prosecutor as the competent authority to issue an EIO is consistent with the principle of equivalence and whether the recognition decision taken by the competent authority of the executing state is compatible with Article 6 and Article 9(1) and (3) of Directive 2014/41. The judge must ensure that both parties have a fair and equal opportunity to present their arguments and evidence.

Module Checklist

I. European Production and Preservation Orders

A. Legal Framework and Procedure

EPPO Regulation would simplify and accelerate cross-border access to electronic evidence in criminal proceedings, while ensuring a high level of protection of fundamental rights

A judicial authority in one Member State would be able to issue a production or preservation order for electronic evidence located in another Member State without the need for a mutual legal assistance request

B. Procedures

e-Evidence Regulation would set out detailed procedures for issuing, executing, and challenging production and preservation orders

Requesting authority would need provide detailed information about requested evidence and suspected criminal offense

Executing authority would need to ensure order is compatible with fundamental rights of affected persons

C. Issues

Potential for abuse of the e-Evidence system by law enforcement authorities

Risk that the e-Evidence system may be used to circumvent national laws on data protection and privacy

e-Evidence Regulation includes safeguards such as the requirement for prior judicial authorization and the possibility of challenging the order before a judicial authority

II. European Investigation Order

A. Legal Framework and Procedure

The EIO Directive was adopted on 3 April 2014 and entered into force on 22 May 2014

EIO Directive simplifies and accelerates cross-border access to evidence in criminal proceedings, while ensuring a high level of protection of fundamental rights

A judicial authority in one Member State can request evidence directly from a competent authority in another Member State without the need for a mutual legal assistance request

B. Procedures

EIO Directive sets out detailed procedures for issuing, executing, and challenging EIOs

Requesting authority must provide detailed information about the requested evidence and the suspected criminal offense

Executing authority must ensure the EIO is compatible with fundamental rights of the affected persons

C. Issues

Potential for unequal access to justice as some Member States may have less developed legal systems or less respect for fundamental rights than others

Risk that the EIO system may be used to circumvent national laws on data protection and privacy

EIO Directive includes safeguards such as the requirement for prior judicial authorization and the possibility of challenging the order before a judicial authority

III. European Arrest Warrant

A. Legal Framework and Procedures

The EAW Framework Decision was adopted on 13 June 2002 and has been in force since 1 January 2004

EAW Framework Decision simplifies and accelerates the extradition of persons who have been accused or convicted of a criminal offense in one Member State and are located in another Member State, while ensuring a high level of protection of fundamental rights

A judicial authority in one Member State can issue an arrest warrant for a person located in another Member State without the need for a formal extradition procedure

B. Procedures

EAW Framework Decision sets out detailed procedures for issuing, executing, and challenging EAWs

Issuing authority must provide detailed information about the person sought and the criminal offense

Executing authority must ensure the EAW is compatible with fundamental rights of the affected person

C. Issues

Risk of violating fundamental rights of the person being extradited

Some Member States may not have adequate safeguards for fundamental rights

EAW Framework Decision includes safeguards such as the requirement for detailed information and compatibility with fundamental rights.

Further Readings:

- Buono, L. (2019, March). The genesis of the European Union's new proposed legal instrument (s) on e-evidence: Towards the EU Production and Preservation Orders. In *Era Forum* (Vol. 19, No. 3, pp. 307-312). Berlin/Heidelberg: Springer Berlin Heidelberg.
- Mitsilegas, V. (2018). The privatisation of mutual trust in Europe's area of criminal justice: The case of e-evidence. *Maastricht Journal of European and Comparative Law*, *25*(3), 263-265.
- Verbruggen, F. (2021). What to expect from the proposed European Production and Preservation Orders?. In *Procedural Rights in the Context of Evidence-Gathering, Date: 2021/04/15-2021/04/16, Location: Online*.
- Chankova, D., & Voynova, R. (2018). Towards new European regulation for handling electronic evidence. *US-China L. Rev.*, *15*, 121.
- Vermeulen, G. (2019). European e-evidence developments. In *Seminar 'Applying the European Investigation Order'*.
- Tinoco Pastrana, Á. (2020). The proposal on electronic evidence in the European Union. *eucrim, 1, 46-50.*

Practical Modules:

Module 6: Questions for the discussion concerning the toolkit for handling and admissibility of electronic evidence

1. Are you aware of any already existing document, which addresses the area of handling and admissibility of electronic evidence?

2. Do you think that such a document (i.e. a Toolkit) could be useful for prosecutors, defence lawyers and judges in their work?

3. Should the Toolkit include the information on its preparation and determine its purpose, objectives and structure?

4. Should the Toolkit include a general overview of the international and European legal framework and relevant case law of the European courts (CJEU, ECtHR) concerning electronic evidence and the presumption of innocence?

5. Should the Toolkit include an overview of the proposed EU legislation relating to the cross-border gathering of electronic evidence (i.e. European production order and European preservation order)?

6. Do you think that the Toolkit should also provide users with (at least indicative) information on the legal framework, case law and examples of good practice in relation to electronic evidence in EU Member States?

7. Should the Toolkit also provide users with information on the following issues:

    - The role of individual criminal justice actors in the so-called chain of custody and their tasks in order to ensure that handling of electronic evidence respects the presumption of innocence;

    - Methods that should be used by the criminal justice actors to ensure the authenticity and integrity of the data;

    - Judicial (or other independent) oversight over gathering different types of the electronic data (i.e. subscriber, traffic and content data) when these data are to be preserved and produced by the service providers on the request of the law enforcement agencies (LEA);

    - The relevant legal provisions determining a duty of the provider and the LEA to inform the person concerned that his or her electronic evidence has been collected?

    - The imbalance in powers between the LEA and prosecution and defence with regard to collecting electronic evidence (i.e. the possibility to enhance the position of the defence lawyers so that they can effectively check the authenticity of the electronic evidence, monitor the chain of custody and challenge the evidence in the court)?

    - Expert witnesses involvement in cases relating to electronic evidence (incl. expert opinions' impact on the proceedings, translating the technical aspects of the issue into a legal environment, ensuring the same access to expert knowledge to both the prosecutors and defence lawyers, etc.);

- The influence of the use of e-evidence in criminal proceedings on the burden of proof, right to remain silent, privilege against self-incrimination and other rights and guarantees;

- Actions of criminal justice agents – during both pre-trial proceedings and judicial proceedings – that violate the above rights and actions that do not violate the rights;

- Effective remedies for the violation of presumption of innocence when using electronic evidence.

- Can you suggest additional issues & questions that you think the Toolkit should also address and provide additional guidance for users?

8. Would it have been more appropriate to limit the Toolkit (to make it as practical as possible and not too extensive) exclusively to guidelines & recommendations and brief information for users on the handling of electronic evidence during its entire "lifecycle" (i.e. during the acquisition and collection, decryption, analysis, preservation, admissibility, use and exchange of electronic evidence)?

9. Should the Toolkit also provide judges, prosecutors and lawyers with more detailed information on the methods and approaches concerning the police work when seizing and investigating electronic devices and electronic data carriers?

10. Can you present an example (a hypothetical situation or circumstance) from your work in which you could use such Toolkit?