Novel Strategies to Fight Child Sexual Exploitation and Human Trafficking Crimes and Protect their Victims

H2020 – 101021801

www.heroes-fct.eu

D3.3 HEROES Data Protection Legal Framework V1

Authors: Sara Domingo Andrés (TRI)

Deliverable nature	Report [R]
Dissemination level	Public [PU]
Version	1.0
Date	30 November 2022

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 101021801

Document Information

Project Acronym	HEROES
Project Title	Novel Strategies to Fight Child Sexual Exploitation and Human Trafficking Crimes and Protect their Victims – HEROES
Grant Agreement No.	101021801
Project URL	www.heroes-fct.eu
EU Project Officer	Markus Walter

Deliverable	**Number**	3.3	**Title**	HEROES Data Protection Legal Framework V1	
Work Package	**Number**	WP3	**Title**	Privacy, ethical data management and social impact assessment	
Date of Delivery	**Contractual**		M12	**Actual**	M12
Status	1.0			Final	
Nature	R		**Dissemination level**		PU

Responsible partner	**Name**	Trilateral Research Ltd.	**E-mail**	Sara.domingo.andres@trilateralresearch.com
	Partner	TRI	**Phone**	+353 (0)51 833 958
Contributing partners	ESMIR, HELLENIC POLICE, SPL, GDCOC			
Reviewers	Juan Carlos Ortiz-Pradillo (UCM)			
Security Approval	Pablo Fernández López (ESMIR)			

Abstract (for dissemination)

Nowadays, a large percentage of crime investigations involve electronic evidence. Even when investigating domestic cases, LEAs often face a cross-border element when obtaining electronic evidence, simply because a foreign service provider might have been used, and the information is stored electronically in another Member State or a third country. In 2018, the Commission proposed the so-called e-evidence package –a Regulation and a Directive. This deliverable assesses the current and proposed mechanisms for the obtention of cross-border evidence by LEAs along with an analysis of the data protection acquis in the EU.

Keywords	e-evidence, data protection, LEAs, survey

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No. 101021801. The opinions expressed and arguments employed herein do not necessarily reflect the official views of the funding body.

Version History

Version	Date	Change Editor	Changes
0.1	25/11/2022	Sara Domingo Andrés (TRI)	First draft
0.2	28/11/2022	Juan Carlos Ortiz-Pradillo (UCM)	Internal review
1.0	30/11/2022	Sara Domingo Andrés (TRI)	Final version

Table of Contents

List of Tables

Executive summary

This deliverable 3.3 corresponds to task 3.3 as per the description in the HEROES Grant Agreement (GA). Nowadays, a large percentage of crime investigations involve electronic evidence. Even when investigating domestic cases, LEAs increasingly need to gather information hold in another jurisdiction, sometimes, simply because a foreign service provider might have been used, and the information is stored electronically in another Member State or a third country. In 2018, the Commission proposed the so-called e-evidence package –a Regulation and a Directive. This deliverable assesses the current and proposed mechanisms for the obtention of cross-border evidence by LEAs along with an analysis of the data protection acquis in the EU. In addition, 4 European LEAs have been interviewed to understand their current difficulties faced in this process.

The first section of this deliverable includes and introduction to the content and a definition of electronic evidence. Section 2 analyses the current legal framework around electronic evidence, i.e letters rogatory, diplomatic channels, the European Investigation Orders and the Convention on mutual assistance, along with the proposed regulation and directive for electronic evidence. In addition, the constraints of the proposed legislation with the existing data protection legal framework are analysed through the opinions issued by the European Data Protection Board (EDPB) and the European Data Protection Supervisor (EDPS).

Section 3 provides a summary of the questions answered by the LEAs. The aim of the interviews undertaken with the LEAs was to understand the difficulties they face when obtaining electronic evidence from a provider based in another Member State or a third country. This way, we have carried out an analysis of how the proposed legal framework would help to overcome these difficulties or on the contrary hinder the LEAs' position.

A second iteration of this deliverable (D3.6) will follow in month 24 of the project, assessing the current development in the negotiations of a cooperation agreement between the European Union and the US in the provision and request of electronic evidence, and will also include updates on the proposed e-Privacy Regulation.

Abbreviations

AB	Advisory Board
CA	Consortium Agreement
CSA/CSE	Child Sexual Abuse and Exploitation
EDPB	European Data Protection Board
EDPS	European Data Protection Supervisor
EIO(s)	European Investigation Order(s)
E-evidence	Electronic Evidence
EU	European Union
EUROJUST	European Agency for Criminal Justice Cooperation
GA	HEROES Grant Agreement, number 101021801
GDPR	General Data Protection Regulation 2016/679
LEA(s)	Law Enforcement Authority(ies)
LED	Law Enforcement Directive 2016/680
LoR(s)	Letter(s) of Request or Rogatory Letter(s)
EUDPR	Regulation 2018/1725
EUROPOL	EU Agency for Law Enforcement Cooperation
THB	Trafficking in Human Beings

1. Introduction

Electronic evidence, or **'e-evidence'**, refers to **digital data** that is used to investigate and prosecute criminal offences. It may include, amongst others, e-mails, text messages, photographs and videos, traffic information, location data, information on user accounts etc. In the digital age, a great deal of our activities in our daily lives, leave a digital trace. In addition, criminals are making use of new sophisticated technological means to perpetrate crimes. Nowadays, 85% of criminal investigations involve digital data[1].

Getting access to e-evidence in an efficient and timely manner has proven to be challenging for Law Enforcement Authorities (LEAs) since often it is saved, stored or guarded, in another jurisdiction within or without the European Union (EU) boundaries. It is stated that in almost two thirds (65%) of the investigations where e-evidence is relevant, there is a request to service providers across borders[2]. In addition, online service providers may be based outside the EU and the data stored on servers which might be located in several countries.

The cross-border factor makes it much more difficult for judicial authorities and LEAs to gather e-evidence within criminal investigations and prosecutions. Some crimes cannot be effectively investigated and prosecuted in the EU because of challenges in cross-border access to electronic evidence[3]. Enhancing the procedures to facilitate cross-border access to e-evidence will significantly contribute to the fight against offline and online crime, including organised crime, trafficking in human being (THB) and child sexual abuse and exploitation (CSA/CSE). To this end, the former Europol's Executive Director Ms Catherine de Bolle expressed: '*Effective policing in the digital age largely relies on harnessing the potential of online processes, alongside the ability to handle electronic evidence securely and verifiably.*[4]

[1] European Commission, press release April 2018, FAQs: New rules to obtain electronic evidence: https://ec.europa.eu/commission/presscorner/detail/en/MEMO_18_3345

[2] European Commission, Impact Assessment Accompanying the document "Proposal for a Regulation of the European Parliament and of the Council on European Production and Preservation Orders for electronic evidence in criminal matters and Proposal for a Directive of the EP and the Council laying down harmonised rules on the appointment of legal representatives for the purpose of gathering evidence in criminal proceedings: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=SWD%3A2018%3A118%3AFIN

[3] European Commission, Impact Assessment accompanying the e-evidence package, 2018: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=SWD%3A2018%3A118%3AFIN

[4] Eurojust, November 2021 "Cross-border access to electronic evidence: update and impact of the pandemic on data requests": https://www.eurojust.europa.eu/news/cross-border-access-electronic-evidence-update-and-impact-pandemic-data-requests

2. Cross-border evidence legal framework analysis

When gathering cross-border information during criminal investigations, a wide variety of laws apply, namely, EU law, rules at Member State level governing criminal investigations, international conventions and bilateral agreements. US law also plays an important role, as major service providers holding relevant evidence operate under US jurisdiction., This section will provide a general overview and analysis of the current legal framework in cross-border evidence requests and the proposed legislation at EU level. Since e-evidence is also personal data, we will explore the current data protection acquis and analyse the opinions of the EDPS and EDPB on the proposed package.

2.1.Convention on Mutual Assistance in Criminal Matters

Article 82 of the Treaty of the Functioning of the EU lays down the basis for **judicial cooperation in criminal matters** amongst Member States **based on the principle of mutual recognition of judgments and judicial decisions**.

The legal instruments establishing a framework for mutual assistance in criminal matters amongst Member States include, without limitation:

- Convention on Mutual Assistance in Criminal Matters[5] (the Convention),
- Council Act May 2000, establishing the Convention on Mutual Assistance in Criminal Matters[6],
- Protocol established by the Council in accordance with Article 34 of the Treaty on European Union to the Convention on Mutual Assistance in Criminal Matters between the Member States of the European Union[7].

The Convention aims to encourage and facilitate mutual assistance between judicial, police and custom authorities on criminal matters. It allows for a Member State to request assistance to another Member State. The requests must be made in writing and carried out directly by the national judicial authorities. It is established that the requested country shall abide by the formalities and deadlines specified by the requesting country as much as possible. It is also provided for a judicial authority to make direct contact with a police or customs authority from another country, however, the requested country may refuse to comply with it or to be applied only under specific circumstances[8].

[5] Convention established by the Council in accordance with Article 34 of the Treaty on European Union, on Mutual Assistance in Criminal Matters between the Member States of the European Union - Council Declaration on Article 10(9) - Declaration by the United Kingdom on Article 20: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A42000A0712%2801%29

[6] Council Act of 29 May 2000 establishing in accordance with Article 34 of the Treaty on European Union the Convention on Mutual Assistance in Criminal Matters between the Member States of the European Union: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32000F0712%2802%29

[7] Protocol established by the Council in accordance with Article 34 of the Treaty on European Union to the Convention on Mutual Assistance in Criminal Matters between the Member States of the European Union[7] https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A42001A1121%2801%29

[8] Eur- lex, Mutual Assistance in criminal matters between EU Member States: https://eur-lex.europa.eu/EN/legal-content/summary/mutual-assistance-in-criminal-matters-between-eu-countries.html

2.2.Directive 2014/41 regarding the European investigation order in criminal matters

Directive 2014/41 was due to transposed by Member States in May 2017 whereby**,** on the basis of the mutual recognition principle and in accordance with the provisions contained in the Directive, a Member State can issue (the '**issuing State'**) a European Investigation Order (EIO). An EIO is a judicial decision issued or validated by a judicial authority from the issuing State to obtain evidence or have one or several investigative measures carried out in another Member State, (the '**executing State'**) including to obtain evidence already in possession of the competent authorities of the executing State. An EIO might also be requested by a suspected or accused person or by a lawyer on his/her behalf in accordance with national criminal procedures.

The EIO shall be requested to the executing State by a judicial authority in the issuing State. Article 2.1.C defines an issuing authority as a judge, court or public prosecutor. Other authorities with investigative capacities like LEAs can also request an EIO but it shall be validated in ultimate instance by a judge, court or public prosecutor in the issuing State. If the EIO has not been issued or validated by a judicial authority the executing State and authority shall return the EIO to the issuing State.

On the other hand, the EIO will be received by the authority within the executing State having competence to recognise the EIO and in accordance with the national law on criminal procedure where it can be required to have a court authorisation. Therefore, the executing authority means an authority having competence to recognise an EIO and ensure its execution in accordance with this Directive and the procedures applicable in a similar domestic case. Such procedures may require a court authorisation in the executing State where provided by its national law.[9]

The EIO can instruct the executing State to perform covert investigation and intercepting telecommunications, to implement measures to preserve evidence, to perform checks on bank accounts of suspects, to temporary transfer persons in custody, etc. In addition, an EIO may request that one or more of the authorities of the issuing State to assist the authorities in the executing State. However, the authorities of the issuing State shall be bound by the executing State law and shall not have any law enforcement powers.

The executing authority shall comply with the formalities, procedures and deadlines described in the EIO provided that such procedures and formalities are not contrary to the fundamental principles of law of the executing State. However, the executing authority may invoke one of the grounds of non-recognition, non-execution or postponement provided in the Directive.

Grounds for refusal of an EIO:

The executing State can refuse to execute the EIO based on one or more of the listed grounds for non-recognition or non-execution contained in Article 11, where:

a) there is an immunity or a privilege under the law of the executing State which makes it impossible to execute the EIO or there are rules on determination and limitation of criminal liability relating to

[9] Directive 2014/41, Article 2 (d): https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32014L0041

freedom of the press and freedom of expression in other media, which make it impossible to execute the EIO;

b) in a specific case the execution of the EIO would harm essential national security interests, jeopardise the source of the information or involve the use of classified information relating to specific intelligence activities;

c) the investigative measure would not be authorised under the law of the executing State in a similar domestic case;

d) the execution of the EIO would be contrary to the principle of *ne bis in idem*;

e) the EIO relates to a criminal offence which is alleged to have been committed outside the territory of the issuing State and wholly or partially on the territory of the executing State, and the conduct in connection with which the EIO is issued is not an offence in the executing State;

f) there are substantial grounds to believe that the execution of the investigative measure indicated in the EIO would be incompatible with the executing State's obligations in accordance with Article 6 TEU and the Charter;

g) the conduct for which the EIO has been issued does not constitute an offence under the law of the executing State, unless it concerns an offence listed within the categories of offences set out in Annex D of the Directive (which provides a long list including acts of terrorism, trafficking in human beings, etc.), as indicated by the issuing authority in the EIO, if it is punishable in the issuing State by a custodial sentence or a detention order for a maximum period of at least three years; or the use of the investigative measure indicated in the EIO is restricted under the law of the executing State to a list or category of offences or to offences punishable by a certain threshold, which does not include the offence covered by the EIO.

Timelines for recognition and execution of an EIO:

Article 12 of the Directive sets out the timelines for recognition and execution. It is established than an EIO and the measures requested therein shall be treated with the same celerity and priority as a similar domestic case by the executing authority and State. The executing authority shall take a decision on the recognition or execution of the EIOI as soon as possible and no later than 30 days for the receipt of the EIO, unless the executing authority invoke one of the provided grounds for postponement. Once the EIO has been recognised the executing authority shall carry out the investigative measure within 90 days following the decision. All the costs of acting on the EIO shall be borne by the executing State.

When it has been indicated in an EIO that due to the seriousness of the offence or other urgent circumstances a shorter deadline than those provided above is necessary, the executing authority shall take as full account as possible of this requirement.

Denmark and Ireland:

Directive 2014/41applies to all EU countries except Ireland and Denmark which opted out but are still bound by the mutual assistance principle. In the report of Eurojust, it is reflected that the fact that Ireland and Denmark are not part of the EIO Directive "*does not necessarily mean that such requests are inevitably lengthy and cumbersome. For instance, in one case in which a Member State requested assistance from Ireland, all requested measures were executed in less than 3 days*".[10]

Eurojust:

The European Agency for Criminal Justice Cooperation (Eurojust). Amongst its function, Eurojust supports and advises national authorities on the issuing, recognition and execution of EIOs from the drafting phase to its final execution.

The Eurojust published a report in 2020 around the implementation in practice of the EIO Directive by Member States. One of the issues identified is that authorities sometimes struggle to understand the boundaries between law enforcement cooperation (police authorities) and judicial cooperation (amongst judicial authorities).

"In some cases, authorities questioned why documents that had already been provided on a police-to-police basis had to be provided again under an EIO. There was a lack of understanding of whether a request could be executed on a police- to-police basis or an EIO [which is issued or validated by a judicial authority] *was required. Eurojust provided guidance on when an EIO could or should be used".*

The report expresses that cross-border requests have been a point of discussion amongst Member States, some of them considering it a matter of police cooperation and some others considering it judicial cooperation. When a police order has been validated by a judicial authority (as the EIO requires) it adds an extra layer of protection of fundamental rights, including the right to a due process, the right to a fair trial, the rights of privacy and data protection and the right of defence. However, national criminal procedural laws differ from one Member State to another and where a police order might suffice for a specific investigative measure in the issuing State a judicial authorisation might be needed in the executing State, and this creates confusion in practice amongst the authorities. The report points out that in several cases, executing authorities have refused to execute on EIO on this basis, including covert investigations.[11]

The report in its final conclusions also emphasises that that due to the significant differences between the Member States distribution of judicial authorities, the authorities of the issuing State often requested support for Eurojust to assist them in identifying the relevant competent authority(ies) to send the EIOs.[12]

[10] Report on Eurojust's casework in the field of the European Investigation Order, November 2020, Page 21: https://www.eurojust.europa.eu/sites/default/files/assets/2020_11_eio_casework_report_corr.pdf
[11] Ibid page 15
[12] Ibid page 56

2.3. Letters Rogatory

Also known as letters of request, is a request from a court in one country to the court of another country outside of its jurisdiction, commonly requesting cooperation to gather evidence, serving of a summons, subpoena or other legal notice or the execution of a judgement.

Letters rogatory are used regardless of the existence of a multi or bilateral agreement or treaties in force with the executing country. Often, letters rogatory used in countries with no treaty or agreement in place are submitted through diplomatic channels, whereas if there is a treaty in force, they are usually submitted directly to the judicial authorities in the issuing country.

2.4. The e-evidence package

On April 2018 and following the publication of an impact assessment report[13], the EC published a legislative proposal package around e-evidence. This package consists of a proposal for a:

- Directive laying down harmonised rules on the appointment of legal representatives for the purposes of gathering evidence in criminal proceedings ("**Proposed Directive**")[14]; and
- Regulation on European Production and Preservation Orders for electronic evidence in criminal matters ("**Proposed Regulation**").[15]

The overarching objective of the proposed e-evidence package is to speed up the process of securing and obtaining e-evidence across borders. In many cases the time is of essence in the investigation and prosecution of criminal offences, and even if the cases do not have an international component, often LEAs need to gather e-evidence simply because the suspect, victim or convicted person used a (digital) service provided by an entity situated in another Member State and valuable information is stored electronically by such service provider.

After 4 years of debate and negotiations and following the sixth political trilogue on 14 June 2022, legislators have confirmed their willingness to move forward and finalise the legislative processe to enact both legal instruments. However, there has not been significant progress yet.

[13] 17 April, 2028, Impact Assessment Accompanying the document Proposal for a Regulation of the European Parliament and of the Council on European Production and Preservation Orders for electronic evidence in criminal matters and Proposal for a Directive of the European Parliament and of the Council laying down harmonised rules on the appointment of legal representatives for the purpose of gathering evidence in criminal proceedings: https://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1524129550845&uri=SWD:2018:118:FIN

[14] Directive of the European Parliament and of the Council laying down harmonised rules on the appointment of legal representatives for the purpose of gathering evidence in criminal proceedings: https://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1524129181403&uri=COM:2018:226:FIN

[15] Regulation of the European Parliament and of the Council on European Production and Preservation Orders for electronic evidence in criminal matters: https://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1524129181403&uri=COM:2018:225:FIN

2.4.1. The Proposed Directive: appointment of legal representatives

The Proposed Directive lays down rules on certain service providers (as defined below) for the receipt of, compliance with and enforcement of decisions and orders issued by competent authorities of the Member States for the purposes of gathering evidence in criminal proceedings.

Necessity of the Proposed Directive:

Online service providers can be (1) headquartered in a Member State offering services only in the territory of that Member State; (2) headquartered in a Member State offering services in several Member States; (3) headquartered outside the EU offering services in one or several Member States, with or without one or various establishments within the EU.

In all three scenarios described, the service providers offering services within the EU are bound by EU law and each and every national law of the Member State(s) where the services are provided. In the era of the Internet where there is no requirement for service providers to have a physical presence where their services are rendered, national authorities have taken different steps and approaches to ensure that national law is complied with by service providers. One of these obligations to comply revolves around national authorities requiring access to e-evidence in the context of criminal proceedings which often are time sensitive. National strategies vary widely, for instance, Germany has recently passed the "Network Enforcement Act"[16] whereby providers rendering their services in Germany are obliged to designate a person residing in Germany who is authorised to receive law enforcement requests on behalf of the company. The law sets out the possibility to impose sanctions in case of failure to designate a person or failure to comply with the requests.

The impact assessment which accompanied the Proposed Directive and Regulation, stated that 55% of total investigations include a request to cross-border access to e-evidence and that the number of requests had increased by 70% in the 4 preceding years. It is estimated that a total of 75%[17] of the requests to access e-evidence across borders are negatively affected due to the lack of timely access, denied access or other causes that affect the cooperation.

Material scope:

Article 2.2 of the text defines the service providers which would fall under the scope of the Proposed Directive as any natural or legal person that provides one or more of the following categories of services:

- Electronic communication services;

[16] Explanatory Memorandum: Context of the Proposal, Directive of the European Parliament and of the Council laying down harmonised rules on the appointment of legal representatives for the purpose of gathering evidence in Criminal Proceedings, 2018: https://eur-lex.europa.eu/legal-content/EN/TXT/?LinkSource=PassleApp&uri=CELEX:52018PC0226

[17] 17 April, 2028, Table 4, Impact Assessment Accompanying the document Proposal for a Regulation of the European Parliament and of the Council on European Production and Preservation Orders for electronic evidence in criminal matters and Proposal for a Directive of the European Parliament and of the Council laying down harmonised rules on the appointment of legal representatives for the purpose of gathering evidence in criminal proceedings: https://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1524129550845&uri=SWD:2018:118:FIN

- Information society services, including social networks, online marketplaces and hosting service providers; and
- Internet domain name and IP numbering services such as IP address providers, domain name registries, domain name registrants and related privacy proxy services.

The Proposed Directive shall apply to the service providers offering services in the EU and it shall not apply where those services providers are established in the territory of a single Member State and offer services exclusively on the territory of that Member State[18].

Obligation to appoint a legal representative:

According to Article 3 of the Proposed Directive:

- Member States shall ensure that service providers established in the territory of that Member State and offering services in the EU, designate at least one legal representative[19] for the receipt of, compliance with and enforcement of decisions for the purpose of gathering evidence in criminal proceedings. The legal representative shall reside or be established in one of the Member States where the service provider is established or offers its services.
- When the service provider is not established in the EU, Member States shall ensure that such service provider offering services on their territory, designates at least one legal representative in the EU for the receipt, compliance with an enforcement for the purposes of gathering evidence. Again here, the legal representative shall reside or be established in one of the Member States where it renders the services.
- Service providers shall be free to designate additional legal representatives.
- Member States shall ensure that the decision and orders for the purpose of evidence gathering are addressed to the legal representative designated by the service provider.
- Member States shall ensure that the legal representative(s) residing or established in their territory cooperates with the competent authorities which issue access requests and shall ensure that the designated representative(s) can be held liable for non-compliance, without prejudice to the liability and legal actions that can be initiated against the service provider.

In addition, Member States shall designate a central authority to ensure the application of the provisions of the Directive. The Commission will make public a list of central authorities to facilitate the coordination and foster mutual assistance.[20]

[18] Article1.4 of the Proposed Directive
[19] Article 3.1 of the Proposed Directive
[20] Article 6 of the Proposed Directive.

Sanctions:

Member States shall enact rules on sanctions applicable to infringements of national provisions adopted pursuant to the transposition of the Proposed Directive. The sanctions shall be proportionate, effective and dissuasive.

2.4.2. The Proposed Regulation: European Production and Preservation Orders for electronic evidence in criminal matters

The Proposed Regulation aims at creating a harmonised procedure within the EU for competent authorities of Member States to issue European Production and Preservation Orders for gathering cross-border e-evidence in the context of criminal investigations and prosecutions. While the Directive 2014/41 applies to evidence gathering in general (including but not limited to e-evidence) the Proposed Regulation would solely pertain to the collection and preservation of e-evidence as defined in section 1 of this deliverable.

Necessity of the Proposed Regulation:

Currently, LEAs and judicial authorities who need access to cross-border evidence within the EU rely on the procedure set out in Directive 2014/41 for the issuance of EIOs as described in section 2.2. of this deliverable. Outside the EU, Member States cooperate using mutual legal assistance procedures established in bilateral treaties or cooperation treaties with the EU, or by means of letters rogatory. However, both means of cooperation have proved to be inefficient and cumbersome with the exponential rise of the number of cross-border access requests for e-evidence needed during the investigation and prosecution of criminal matters.

The Proposed Regulation would make it easier for LEAs to secure and gather e-evidence for criminal proceedings stored or held by service providers in another jurisdiction. The Proposed Regulation would not replace the current EIO system for obtaining e-evidence but would provide an additional tool for the authorities.

There may be situations, where the EIO may be the preferred choice for competent authorities and the measures contained in the Proposed Regulation would not supersede those provided in the Directive 2014/41 for the issuance of EIOs.[21] The relevant authorities should be able to choose the tool most convenient on each case with the possibility to issue both an EIO and/or a Production and/or Preservation Order.

Material Scope:

The Proposed Regulation will enable a judicial authority in a Member State to directly obtain e-evidence stored or held by a service provider in another Member State without the involvement of the judicial authority of the executing State.

Service providers are defined in the same way as defined in the Proposed Directive (previous subsection in this deliverable) and in the same way the e-evidence gathering will solely apply to criminal proceedings.

[21] Article 23 and Recital 61 of the Proposed Regulation.

Production Orders refer to orders compelling a service provider to produce electronic evidence. Whereas Preservation Orders compels service providers to preserve electronic evidence in view of a subsequent request for production.

It is established that Production Orders may involve the production of evidence around 'subscriber data', 'access data', 'transactional data' and 'content data' as defined below[22]:

- **Subscriber data** means the identity of subscriber, such as name, date of birth, address, billing and payment, phone and email.
- **Access data** is defined as data related to the commencement and termination of a user access to a service, i.e., date, time, logins and log-offs, IP address, data identifying the interface used and the user ID, including communications metadata.
- **Transactional data** is defined as data related to the provision of a service, such as the source and destination of a message or another type of interaction, data on the location of the device, date, time, duration, size, route, format, the protocol used and the type of compression, unless such data constitutes access data. It includes 'electronic communications metadata' as defined in the E-Privacy Regulation proposal[23], that is: '*data processed in an electronic communications network for the purposes of transmitting, distributing or exchanging electronic communications content; including data used to trace and identify the source and destination of a communication, data on the location of the device generated in the context of providing electronic communications services, and the date, time, duration and the type of communication'*. It is worth noting that by this definition of transactional data would solely include electronic communications metadata, therefore, the content of the communication (text, voice, videos etc) is out of the scope.
- **Content data** means any data stored in digital format, such as text, voice, videos, images, and sound.

Production Orders for **access data** and **subscriber data** and **Preservation Order** can be issued in relation **to all criminal offences.** However, **Production Orders** for **transactional** and **content data**, may only be issued in the context of criminal offences when[24]:

- The offences are punishable in the issuing State for a custodial sentence of a maximum of at least 3 years, or
- for offences wholly or partly committed by means of an information system offence for (1) committing fraud and counterfeiting of non-cash means of payment, (2) sexual abuse and sexual exploitation of children and child pornography, and (3) attacks against information systemsm, and (4) terrorism.

[22] Definitions provided in points 7, 8, 9 and 10 of Article 2 of the Proposed Regulation.
[23] Article 4.3.c) E-Privacy Regulation proposal: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52017PC0010
[24] Article 5.4 of the Proposed Regulation

Preservation Orders to preserve any type of electronic evidence may be issued for **all criminal offences** without distinction (Article 6(2) of the proposed Regulation) and the requirement of a similar measure available for domestic cases does not apply.

Procedure:

European Production and Preservation Orders may be issued by a judge, a court, or any other competent authority as long as it is validated by a judge, court or a prosecutor (subject to the limitations set out below).

When it comes to **European Production Orders for transactional and content data**, the Proposed Regulation does **not** foresee the possibility to be issued **by a prosecutor**.[25] Recital 30 explains that the data involved in Production Orders for subscriber and access data are less sensitive, and they can be issued and validated by competent prosecutors. However, Production orders for transactional and content data shall always be reviewed by a judge. Preservation Orders can be issued and validated by prosecutors. The competences and categories of data are illustrated in the Table 1 below, which has been extracted from the FAQs of the European Commission website. [26]

[25] Article 4.2 of the Proposed Regulation (where the figure of the prosecutor is not contemplated)
[26] European Commission, FAQs: New EU rules to obtain electronic evidence: https://ec.europa.eu/commission/presscorner/detail/el/MEMO_18_3345

Table 1: Types of data and competences. Source: FAQs New EU rules to obtain e-evidence.

Type of data	Definition	Access Rules
Subscriber data	Elements that serve to identify a subscriber or customer such as the name, date of birth, postal address, billing and payment data, telephone number, or email address.	**Prosecutor/judge** in country A can directly ask the service provider or its legal representative in country B to provide the electronic evidence. If request comes from **police**, they have to **ask a prosecutor or judge** in country A to approve the order before transmitting it to the service provider or its legal representative.
Access data	Data elements which in and of themselves cannot identify the user but are strictly necessary as a first step towards identification. This includes data on a user's access to a service, such as the date and time of use or the log-in to and log-off from the service or the IP address allocated by the service provider.	**Prosecutor/judge** in country A can directly ask the service provider or its legal representative in country B to provide the electronic evidence. If request comes **from police**, they have to **ask a prosecutor or judge** in country A to approve the order before transmitting it to the service provider or its legal representative.
Transactional data	Relates to the provision of a service, such as the source and destination of a message, data on the location of the device, date, time, duration, size, route, format, the protocol used and the type of compression.	**Judge** in country A can directly ask the service provider or its legal representative in country B to provide the electronic evidence. If request comes from **police or prosecutor,** they have to **ask a judge** in country A to approve the order before transmitting it to the service provider or its legal representative
Content data	Any stored data in a digital format such as text, voice, videos, images, and sound other than subscriber, access or transactional data.	**Judge** in country A can directly ask the service provider or its legal representative in country B to provide the electronic evidence. If request comes from **police or prosecutor**, they have to **ask a judge** in country A to approve the order before transmitting it to the service provider or its legal representative.

The European Preservation and Production Orders shall be **addressed** directly to an appointed **legal representative** of the service provider (pursuant to the Proposed Directive). Where the legal representative has not been appointed or does not comply with the order, the order may be addressed to any establishment of the service provider in the EU.[27]

The orders may be transmitted by any means capable of producing a written record, or where service providers, Member States or Union bodies have established dedicated platforms or other secure channels for the handling the requests, the issuing authority may also choose to transmit them via these channels.[28] Templates to be used to issue orders are provided in Annexes I, II and II of the Proposed Regulation.

The service providers, recipients of the orders, shall be complied with **within 10 days** from the date of the receipt of the order. In **emergency cases**, the replies shall be transmitted within **6 hours** upon receipt of the order.

When it comes to Preservation orders, service providers shall preserve the data requested for 60 days. After the 60 days, the preservation order shall be ceased unless the issuing authority confirms that the subsequent request for production has been launched.

If the service providers do not comply in a timely manner with the requests, the issuing authority may transfer the orders to the competent authorities in the executing State.

Sanctions:

Without prejudice to existing national laws, pursuant to the Proposed Regulation Member States shall lay down rules on pecuniary sanctions applicable to infringements in relation to the execution of the orders and confidentiality obligations which can range from pecuniary to criminal sanctions. This approach has been widely criticised by experts[29]. Member States having a wide margin of discretion to regulate non-compliance from pecuniary to criminal actions, may leave the door open for service providers to conveniently choose where to appoint their representatives or even establish their headquarters in the EU, and therefore, Member States might choose not to excessive regulate this matter to avoid big tech corporations to leave their country. A measure that ultimately would entail fragmentation and unfairness.

Grounds for refusal: protection of fundamental rights

Article 9 (5) provides for the possibility to object to a Production Order if the service providers believes that it violates the Charter of Fundamental Rights of the EU. In such cases, service providers would have to send a reasoned objection to the issuing authority and inform the authorities on the executing State, either directly, via Eurojust or the European Judicial Network.

[27] Article 7 of the Proposed Regulation
[28] Article 8.2 of the Proposed Regulation
[29] The European Commission's E-evidence Proposal: Toward an EU-wide Obligation for Service Providers to Cooperate with Law Enforcement?, 2018, Vanessa Franssen, European Law Blog https://europeanlawblog.eu/2018/10/12/the-european-commissions-e-evidence-proposal-toward-an-eu-wide-obligation-for-service-providers-to-cooperate-with-law-enforcement/

Effective remedies:

Article 17 of the Proposed Regulation states that suspects and accused persons whose data has been obtained through a Production Order shall have the right to affective remedies during the criminal proceedings without prejudice to those remedies available under the General Data Protection Regulation (GDPR) and the Law Enforcement Directive (LED) . The same applies for persons whose data was obtained and there were no suspects. The right to an effective remedy shall be exercised before a court in the issuing state.

Ireland and Denmark:

With a great deal of the tech giants service providers (Google, Facebook, Microsoft, etc.) headquartered in Ireland for their operations within the EU, Ireland plays an important role in the mutual assistance and cooperation proceedings for gathering e-evidence. Although, Ireland opted-out from Directive 2014/41 (EIO) and nowadays relies on the principle of mutual assistance within the EU Member States, Ireland has notified its wish to take part in the adoption and application of the Proposed Regulation. [30]

On the contrary, Denmark has expressed it will be not taking part in the adoption and implementation of the Proposed Regulation.[31]

2.5. Budapest Convention on Cybercrime – Council of Europe

The Budapest Convention is the first international treaty on crimes committed via the Internet and other computer networks and specifically including crimes around CSA and CSE.

The Convention is opened for signature since November 2001 by member states of the Council of Europe and by non-member States including those which have participated in its elaboration like Canada, Japan, South Africa, and the United States. There are currently 67 parties to the Budapest Convention, including but not limited to the 27 Member States of the EU, countries from Latin America, Africa, Armenia, Azerbaijan and the US.

The Convention provides signing States with:

(1) The criminalization of a list of attacks against and by means of computers

(2) Procedural law tools to make the investigations of cybercrimes and the securing of e-evidence more effective and subject to rule of law safeguards; and

(3) Internal police and judicial cooperation on cybercrime and e-evidence

In November 2021, the Council of Europe adopted a second additional protocol to the Budapest Convention[32] "*Second Additional Protocol to the Convention on Cybercrime on enhanced co-operation and disclosure of electronic evidence*". The text is opened for signature since May 2022. Given that it cannot be signed by the

[30] Recital 64 of the Proposed Regulation.
[31] Recital 65 of the Proposed Regulation.
[32] Second Additional Protocol to the Convention on Cybercrime on enhanced co-operation and disclosure of electronic evidence: https://search.coe.int/cm/pages/result_details.aspx?objectid=0900001680a48e4d

EU as only individual Sates can be parties to the Treaty, the European Commission authorized the EU Member States to sign the protocol in April 2022. [33] The second protocol has been signed by the US along with 23 States, including countries from the EU and Chile, Colombia, Japan and North Macedonia, establishing reciprocal cooperation obligations between those countries.

The second protocol provides enhanced procedures for cross-border requests pertaining to:

- Direct requests to registrars in other jurisdictions to obtain domain name registration information,
- Direct cooperation with service providers in other jurisdiction to obtain subscriber information.
- Expedited mutual assistance procedure, from the judicial authorities of the requesting country to the judicial authorities of the issuing countries in emergency situations, i.e where there is an imminent risk to the life or safety of a natural person.
- Recognition of testimony and statements to be taken from a witness or expert by video conference.

The protocol incorporates the definitions provided in the main body of the Convention for traffic and subscriber data. The scope of the second protocol does not include access to ' content data'.

With the signature of the second protocol of the Budapest Convention, LEAs can contact directly service providers established in another contracting State to acquire certain information without contacting the judicial authorities of that State first. The protocol has been signed by EU and non-EU countries, and it is expected that all countries conforming the EU will sign it. Therefore, while the e-evidence package has not been approved yet based on concerns about privacy and mutual recognition of judicial decisions in criminal matters, direct cooperation with service providers has been implemented by the second protocol around subscriber information and traffic data amongst EU and non-EU countries.

2.6. Data Protection legal framework

2.6.1. Fundamental rights to privacy and data protection

A fundamental right to privacy is laid down by Article 8 of the European Convention for the Protection of Human Rights and Fundamental Freedoms[34]:

> *1. Everyone has the right to respect for his private and family life, his home and his correspondence.*
>
> *2. There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention*

[33] Council of Europe European Convention on Human Rights https://www.consilium.europa.eu/es/policies/e-evidence/
[34] European Convention on Human Rights: https://www.echr.coe.int/documents/convention_eng.pdf

of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others.

In addition, the Charter of Fundamental Rights of the EU[35] establishes the right to respect for private and family life and the right to protection of personal data in its Articles 7 and 8, respectively:

Article 7: ***Respect for private and family life***

Everyone has the right to respect for his or her private and family life, home and communications.

Article 8: ***Protection of personal data***

1. Everyone has the right to the protection of personal data concerning him or her.

2. Such data must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law. Everyone has the right of access to data which has been collected concerning him or her, and the right to have it rectified.

3. Compliance with these rules shall be subject to control by an independent authority.

Both regulatory instruments, the Charter and the Convention are binding for both the EU and its Member States, and thereby affect all legislative acts on privacy matters and, therefore it also affects the legislation around electronic evidence both on a European and on a domestic level.

2.6.2. EU Data Protection secondary law

There are several laws approved by the EU parliament governing the protection of personal data processing:

1. The **General Data Protection Regulation** 2016/679 (GDPR) which came into force in 2018 and repealed Directive 95/46 on the protection of personal data. The GDPR material scope of the GDPR excludes the processing of personal data by competent authorities for the purposes of prevention, investigation, detection or prosecution of criminal offences. Therefore, the GDPR will be out of the scope of this deliverable.
2. Directive 2016/680 on the protection of natural persons with regards to the processing of personal data by competent authorities for the purposes of prevention, investigation, detection or prosecution of criminal offences, also called 'Law Enforcement Directive' (**LED).**

[35] Charter of Fundamental Rights of the European Union: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:12012P/TXT

3. The Regulation 2018/1725 laying down the data protection obligations of EU institutions and bodies when they process personal data, also called **EUDPR.**
4. Regulation 2016/794 which governs the personal data processing carried out by **EUROPOL**, as amended by Regulation 2022/991.

2.6.3. The LED

The LED governs the personal data processing by competent authorities for the prevention, investigation, detection and prosecution of criminal offences. It sets out the same principles collected in the GDPR in its Article 4 whereby personal data shall be:

a) processed lawfully and fairly;
b) collected for specified, explicit and legitimate purposes and not processed in a manner that is incompatible with those purposes;
c) adequate, relevant and not excessive in relation to the purposes for which they are processed;
d) accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay;
e) kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which they are processed;
f) *processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures*.

One of the differences between the GDPR and the LED, is that the LED mandates Member States to provide for the controller to make a clear distinction between personal data of different categories of data subjects, namely:

1) suspects of the commission of a criminal offence or that are about to commit a criminal offence;
2) persons convicted of a criminal offence;
3) victims of criminal offences; and
4) other parties, such as witnesses, persons who can provide information or contacts or associates of suspects or persons who have been convicted.

Scope of application

The LED is applicable when LEAs process personal data for the prevention, investigation, detection and prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security. In this regard, the personal data processing carried out by LEAs when requesting and receiving e-evidence will be always subject to the provisions of the LED.

2.6.4. Data protection safeguards in e-evidence law

Directive 2014/41 establishing the rules around EIOs (as stated in section 2.2 of this document) was passed and came into force while the Council Framework Decision 2008/977 on the protection of personal data in the framework of police and judicial cooperation in criminal matters was also still in force before being repealed by the LED. The LED did not contain any amendments or additions to Directive 2014/41; therefore, the Article 20 still refers that personal data processing in the context of criminal investigations and proceedings shall be carried out in accordance with Council Framework Decision 2008/977 (LED now) and shall be proportionate, necessary and compatible with the original purpose and the right of defence of the data subject. The Directive does not contain any other specific reference to personal data protection.

The overarching objective of the **proposed e-evidence package** is to speed up the process of securing and obtaining e-evidence across borders. The Proposed Regulation for the issuance of preservation and production orders would entail the processing of personal data and limitations on both the right to privacy guaranteed by Article 7 of the Charter and the right to protection of personal data guaranteed by Article 8 of the Charter. To be lawful, such limitations must be "necessary" and "proportionate". To this end the EDPB and the EDPS both submitted separated opinions on the proposed e-evidence package in 2018 and 2019, respectively.

2.6.5. EDPB criticism on the e-evidence package

All 4 data categories as described in the Proposed Regulation, access data, subscriber data, transactional data and content data, fall under the definition of personal data within the EU data protection law. The EDPB recalls that according to "*CJEU case law, to establish the existence of an interference with the fundamental right to privacy, it does not matter whether the information on the private lives concerned is sensitive or whether the persons concerned have been inconvenienced in any way"*[36].

Amongst the various points of criticism raised by the EDPB in its Opinion 3/208 on the proposed e-evidence package, we have selected the following ones for the purposes of this deliverable:

- **New categories of data**: The EDPB highlights once again that the 4 categories of data covered by the e-evidence package are personal data. It analyses that the proposed legislation covers what is being rereferred as non-content data (subscriber data, access data and transactional data) and content data. However, it points out that the CJEU in its judgements C-203/15 and C-698/15 Tele2 Sverige AB hat "*metadata such as traffic data and location data provide the means of establishing a profile of the individuals concerned, information that is no less sensitive, having regard to the right to privacy, than the actual content of communications*"[37]. The EDPB notes that the four categories do not seem to be clearly defined, since, for instance IP addresses may fall under the definition of both, transactional and subscriber data. The EDPB proposes to include a broader

[36] EDPB Opinion 23/2018 on Commission Proposals on European Production and Preservation Orders for electronic evidence in criminal matters, Page 12, para 3: https://edpb.europa.eu/our-work-tools/our-documents/opinion-art-70/opinion-232018-commission-proposals-european-production_en
[37] Ibid page 12, para 4

definition of electronic communication data to cover a technology neutral way in order to ensure the appropriate safeguards to be implemented both for content and non-content data.

- The EDPB considers the abandonment of the **dual criminality principle** and claims it should be maintained, i.e this would for instance prevent a State from requesting data or other measures to another State where the same act is not punished. It is of specific relevance for divergent legislations in the matter of political crimes or opinions and quoting the report literally, the death penalty. However, the report fails to illustrate the practical risks within EU countries (which are bound by the Charter of Fundamental Rights) with real examples, since the death penalty has been long abolished within the EU.
- The EDPB recalls past **CJEU case law** where it is specifically underlined that for traffic and location data, access of the competent authorities shall be restricted solely to fighting serious crime. The EDPD suggests the introduction of additional safeguards by only providing data in the cases of 'serious criminal offences' or for crimes specified in a list and added to the proposal. Furthermore, the EDPB rejects the possibility for orders to be issued or validated by prosecutors in the case of access and subscriber data.
- The EDPB acknowledges that in some instances access requests might be addressed to **processors** (under the definition of the LED and the GDPR), for example, when the service provider is storing the data, and recommends adding a provision whereby processors shall inform the controllers.
- The EDPB emphasises that data protection obligations around **data transfers** shall be complied with when the service providers are based outside the EU, especially when no adequacy decision has been adopted.
- The EDPB strongly suggests abandoning the idea of providing **content data** without any involvement of the competent authorities of the Member State where the data subject is.
- The EDPB regrets the lack of inclusion of a **derogation** where there are substantial grounds for believing that the enforcement of an order would result in a **violation of fundamental rights** of the data subject concerned.
- The time limit of 6 hours to provide data when there is an **emergency request**, i.e., and imminent risk to the life or safety of a natural persons, could violate data protection rights if abused or misused. That is why the EDBP proposes the inclusion of **control mechanisms** even if a posteriori.

2.6.6. EDPS criticism on the e-evidence package

On the 6th of November 2019, the EDPS issued its Opinion 7/2019[38] on the e-evidence proposed package. A summary of the issues is presented below:

- Similarly to the EDPB, the EDPS, highlights the need to have **consistent definitions** of the different **data categories** amongst the Proposed Regulation and applicable data protection laws. The EDPS quotes the definitions provided in the draft ePrivacy Regulation, which would define electronic communications data and distinguish between the two categories of electronic communications content data and electronic communications metadata. The definitions provided for the categories of transactional data and access data are new data categories and lack clarity and may produce overlaps with other data categories that could create difficulties for service providers. For instance, IP address could fall under the categories of transactional data and subscriber data.

- Same as in the EDPB's opinion, the EDPS quotes the **CJEU** and its line of jurisprudence in considering that metadata or data considers 'less sensitive' might produce the same interference with the right to privacy as access to content and making reference to some of the decisions also considered by the EDPB (e.g., Tele2 Sverige).

- The EDPS notes that the **threshold** of a maximum of **three years** of custodial sentence would in practice apply to a large number of offences in national criminal codes, including offences that might not be considered 'serious' and it is recommended that access to content and transactional data shall only be granted in cases of 'serious crimes'[39]. Furthermore, the EDPS acknowledges that in cases were the crime is not 'serious' (without providing a definition for serious crimes) it might still be proportionate to request access to content and transactional data, and suggests doing so using the traditional channels, such as EIOs[40]. In addition, the EDPS suggests including a list of serious crimes in the Proposed Regulation (also suggested by the EDPB). It also acknowledges that this possibility to limit transactional and content data access to serious crimes was discarded at an early stage of the legislative process, but still, it recommends its further consideration and inclusion taking into account the CJEU case law.

- The EDPS highlights the necessity of reassuring **data security** when requesting and providing access to e-evidence, regretting that the Proposed Regulation does not delve enough into this matter. The verification of authenticity of certificates and orders is essential, and the EDPS suggests the use of digital signatures. Article 8(2) of the proposed Regulation would allow, the use of already established dedicated platforms or secure channels to handle requests. However, this remains optional.

[38] EDPS Opinion 7/2019, November 2019: https://edps.europa.eu/sites/edp/files/publication/19-11-06_opinion_on_e_evidence_proposals_en.pdf
[39] Ibid para 28, 29 and 30
[40] Ibid para 29

- Even if the EDPS acknowledges that compliance with fundamental rights would be entrusted primarily to the requesting (issuing) judicial authorities, the EDPS considers that service providers would be entrusted with the task of protecting data subjects' privacy and data protection rights, since there would be not involvement from the judicial authorities of the enforcing (executing) State. Going beyond the recommendation of the EDPB of including at least judicial review of the issuing Sate for content access requests, the EDPS further recommends the **systematic involvement of the judicial authorities** as early as possible in the process[41] and the reinstatement of the dual criminality principle.
- Beyond the general comments and recommendations above listed, the EDPS provides the following additional recommendations, amongst others:
    - Reference to the applicable data protection legal framework. The EDPS recommends adding references to the current e-Privacy Directive 2002/58 with the possibility to replace if with the forthcoming e-Privacy Regulation.
    - The EDPS therefore suggests introducing an obligation to publicly disclose periodically and in an aggregate form the number of production and preservation orders received by services providers under the proposed Regulation, and whether or not these requests were fulfilled.
    - The EDPS recommends adding the right to an effective remedy also when the data has been preserved, as opposed to solely containing a reference to an effective remedy when the data has been obtained.
    - The EDPS suggests incorporating an obligation to introduce judicial review the grounds for immunity by the issuing State when the orders are rejected based on persons benefiting from immunities and privileges.
    - The EDPS suggests incorporating longer time limits than 10 days for the provision of data which would allow to ascertain the authenticity of certificates by service providers.

[41] Ibid para 42

3. Survey on legal considerations affecting data management and information exchange between LEAs and network operators.

In the era of Internet and digital communications and services, most of our actions leave a trace in the digital world. It can be anything, from having an account with a certain provider, to accessing the Internet from a specific IP address and location or sharing illegal files related to CSA/CSE. Police officers need to gather these digital traces, either to pursue a research path (intelligence) or to gather evidence to be presented in Court during criminal proceedings.

In gathering this operational information which can eventually lead to evidence, police forces need to request data to private companies which are often not based in their home State. The cooperation of private actors is needed for the prosecution of crimes and misdemeanours. Without their help, LEAs could not investigate, detect, prevent and prosecute crimes related to CSA/CSE and THB. This cooperation has become increasingly challenging as new providers of digital services emerge and many of them are not covered by the obligations typically set out in the laws of telecommunications. In addition, a great deal of investigative measures and e-evidence need to be requested from private service providers which are based out of the country of the jurisdiction of the LEA, within and without the boundaries of the EU.

For the purposes of this survey, we have compiled a set of questions that had been answered by EU LEA representatives of the HEROES consortium. An interview has been held with these representatives in order to understand what are the difficulties that LEAs face when gathering e-evidence from service providers which are not based in their home State and to analyse how these difficulties can be mitigated with the proposed e-evidence package and the second protocol to the Budapest Convention. A summary of the questions asked and responded can be found in the table 2 below as part of subsection 3.1, the name of the LEAs have been masked with a number for confidentiality purposes. Subsection 3.2 describes the efforts made in contacting representatives of social network operators which are dealing with law enforcement requests.

Following this survey and the research on the current and proposed legal framework elaborated in previous subsection, subsection 3.3 draws preliminary conclusions on how the e-evidence package and the second protocol of the Budapest Convention could change the current landscape on e-evidence, this exercise will continue in the next deliverable of this task (D3.6), due in month 24.

3.1. LEAs status quo and survey on the current challenges

Table 2: Summary of questions and answers provided by LEAs

1	How is e-evidence requested from a service provider which is based in another Member State?
LEA 1	When it comes to big tech providers (including US providers with EU headquarters in Ireland), they have signed collaboration agreements to make the procedure faster and more effective. EIOs are mostly used when they want to request the implementation of an investigative measure in another Member State (e.g., interception of communications), and they issue letters rogatory when the provider is based outside the EU. They also have collaboration agreements with LEAs from third countries.
LEA 2	They have collaboration agreements with different service providers. When they need access to account or subscribers' data, they contact these service providers directly with a police order. They contact US service providers with EU headquarters (usually based in Ireland) via email. They already know who need to contact to and they have their contact details. They also use rogatory letters when service providers are based out of the EU and depending on the case, EIOs are also used.
LEA 3	Information can be requested during criminal proceedings in criminal process. Information is requested through international organizations (Interpol, Europol etc.) Requests are prepared by the international cooperation department, based on the requirements of the investigator. Direct contact with the provider is carried out when there is a cooperation agreement signed between the LEA and the service provider contacted.
LEA 4	Relying on rogatory letters an EIOs mostly. They can also contact service providers directly, when there is a collaboration agreement signed between the LEA and the service provider specifically, this way they can get the information faster than when issuing EIOs.

2	Under what circumstances are EIOs issued?
LEA 1	EIOs are usually used when they would like to have access to content data, when they issue orders for the interception of communications, or when they need banking information for economic crimes.
LEA 2	For instance, in CSA/CSE cases they need to use EIOs and involve judicial authorities of both Member States. When the case falls under the law of the secrecy of communications (for instance when requesting content data), they need judicial authorisation.
LEA 3	EIO can be issued during criminal proceedings in criminal process. Almost always this LEA uses international organizations for information requests. Direct contact is only in those cases when there is a cooperation agreement between the LEA and organization that is contacted. If there is no agreement, only official international organizations are used.
LEA 4	EIOs are used when the police would like to introduce covert investigation in another Member Sate and implement investigative measures such as, intercepting telecommunications, to implement measures to preserve evidence.

3	Regarding the EIOs, would you say that they work efficiently and in a timely manner? What can/needs to be improved?
LEA 1	It depends, when they receive EIOs sometimes they need to perform investigative measures, when they issue EIOs, it depends on the Court and how busy they are. If the matter is urgent, usually takes longer than 24 hours.
LEA 2	In their view, they work efficiently, and service providers are usually cooperative and abide by the deadlines set out by law. Usually, EIOs take longer than contacting the service providers directly but it depends sometimes EIOs are quicker.
LEA 3	Overall, there are no problems with EIOs. Mostly they work efficiently and in a timely manner.
LEA 4	Yes, they work well.

4	In what cases a police order is needed to access the data and in what cases a judicial authorisation is required?
LEA 1	They express that different service providers require different authorisations for the same data, for instance one service provider might require a police order for checking whether a specific individual has an account with the service provider while other service providers might require a judicial authorisation. Under national laws regulating the criminal procedure, telecom law and also data protection laws, police forces have the power to request certain categories of data (ownership of an account, etc) to investigate crimes with a police order and without judicial authorisation. When requesting access to content data they always need judicial authorisation since it falls under the law of the secret of communication.
LEA 2	The direct communication with service providers is provided for by existing national legislation. In particular, the law obliges providers to send data without prosecutorial intervention. When the data to be accessed falls under the national laws around the secrecy of communications (e.g. wiretapping, access to content data) they need to get judicial authorisation. In order to access to subscriber data a police order usually suffices, and it is in compliance with national criminal procedure law.
LEA 3	Judicial authority approval in cases when requested evidence include not only personal data (IP, information about person) but also transcripts of the communication (content data) etc.
LEA 4	The procedure always requires involving the prosecutor or judge in the case; therefore, they always need judicial or prosecutor's authorization.

5	How is data from the EUROPOL requested?
LEA 1	They use the SIRIUS platform within EUROPOL to get information and to check how and whom they need to contact, i.e representatives of the service providers or appointed persons. They use SIENA for the exchange of information between LEAs.
LEA 2	They use SIENA (Secure Information Exchange Network Application) which facilitates information sharing with other police forces within the EU. They do not have access to all the information available in SIENA, it depends on the user permissions given. They consider SIENA a secure way to exchange and request information.
LEA 3	The investigator requests information based on the criminal case, and the international cooperation department prepares the request or EIO and sends it. Received information is forwarded to investigator if such information was available.
LEA 4	They use SIENA to obtain information and contact other LEAs directly if they need to request data for e-evidence.

6	Would you advocate for the creation of a unique single platform amongst LEAs in the EU for the exchange of e-evidence with service providers? Please explain your reasoning.
LEA 1	They use a centralised platform to communicate with all service providers, which was implemented a few years ago and it's used by the police. They think is positive and eases their work, and in addition, it provides more guarantees of security, an also guarantees for the service providers that the requests are truly coming from the LEA, therefore, it is advisable that all police forces use a unique an centralised way to communicate with service providers.
LEA 2	Yes, they think it will be positive and will increase the security of the information shared, given that, at the moment, in the majority of cases, the information is exchanged via email.
LEA 3	They consider that currently there are no problems with the existing system, therefore they cannot argue for necessity of such platform.
LEA 4	Yes, that would facilitate the procedure and the work of the police and it would result in a more efficient and secure data sharing.

7	Would you say that service providers usually comply with e-evidence requests promptly and in a timely manner?
LEA 1	Service providers usually comply but too often the process takes longer than desired. Timelines to respond should be improved. EIOs take even longer.
LEA 2	Yes, in the majority of cases, the information is received in a timely manner. They are not aware of any instances where the service provider did not reply. Sometimes service providers request the issuance of a judicial authorisation as opposed to a police order.
LEA 3	Overall, yes, service providers comply.
LEA 4	Yes, overall, there is compliance and cooperation.

8	Have you ever been required to contact a service provider in the US and how does this process work?
LEA 1	When they request access to content data, usually the companies like Facebook, Google etc which have their European headquarters in Ireland, prompt them to contact the US based company. They usually contact the US company using letters rogatory and it takes a very long time to process, sometimes even 2 years and this seriously affect the investigations.
LEA 2	Yes, sometimes they need to contact service providers in the US, and it is usually done involving the judicial authorities of both countries. The process to access to contact data can be quick or can take a lot of time, sometimes up to 3 years, except when there is a life-threatening risk which is usually quick.
LEA 3	Data access requests with US based entities follow a similar process. The investigator requests the data through the international cooperation department, there is no direct contact with the service(s) provider(s). They believe, there are no problems with the existing system.
LEA 4	For content data, they usually need to contact the entity based in the US, even if the company has its European Headquarters in Ireland. Even companies that are not based in the US but in another third country, for instance, Israel. In these instances, they make use of letters rogatory. To get the information from a third country following this procedure, it usually takes at least 6 months. They claim that they have good contacts with the US authorities and these contacts facilitate the cooperation between both countries.

9	Following Brexit, have you had to request e-evidence from a service provider in the UK? How does this work? Is the process burdensome? How could it be improved?'
LEA 1	As far as they are aware, no requests have been made to service providers in the UK after Brexit. Most of companies that were based in the UK and providing services in different Member States of the EU have moved or registered a new company in Ireland, therefore, they have not had any problems in this regard.
LEA 2	No, they have not had the need to contact service providers based in the UK.
LEA 3	They have made requests to UK based entities following Brexit and found no difficulties in acquiring the data.
LEA 4	To the best of their knowledge, they have not contacted UK based entities following Brexit, since most of the companies operating in the EU which were based in the UK, have transferred to or opened an establishment within one of the Member Sates

3.2. Difficulties faced by social network operators

TRI has made several attempts and contacted different representatives of social network operators which are established within the EU boundaries inviting them to participate in the HEROES project and more specifically to participate in the survey to understand the difficulties social network operators face when dealing with access requests initiated by LEAs outside the country of their main establishment. However, these attempts have been unsuccessful so far. TRI will keep on trying and hope to have input from these service providers on the second iteration of this deliverable, that is D3.6 due in month 24 of the project.

3.3. Preliminary conclusions on how the e-evidence package can resolve the difficulties faced by LEAs in gathering e-evidence and legal analysis of the status quo

- In some instances, and in previous years, LEAs have experienced difficulties in finding the right entity to be contacted and the right person within the service provider when requesting information. Nowadays, they claim it is easier since they already have most of the contacts for each service provider. The proposed Directive obliges service providers which are based in a third country but operate in more than one Member State to appoint a **legal representative** which will function as the point of contact for LEAs and judicial authorities to gather e-evidence data. This appointment will rapidly eliminate any problems that LEAs may have with new service providers that emerge in the market, since they will no longer need search for 'the right contact person'. The obligation to appoint a legal representative serves a two-fold purpose, since not only LEAs will benefit from having a legal representative to contact to, but also it will provide legal certainty to service providers which will no longer have to question what the exact legal process is and whether the appropriate legal safeguards have been implemented.

- When analysing the e-evidence package, we think is positive, that even if LEAs can contact directly the service providers without having to involve the judicial authorities of the issuing Member State, **the role of the issuing (or host) Member Sate** is not passive. The issuing Member State will also need to ensure that legal representatives comply with the provisions of the regulations.

- Certainly, the proposed e-evidence package cannot solve data sharing problems with third-country nationals, regardless of the appointment of a legal representative. For instance, the **US** Stored Communications Act prohibits the **disclosure of content data to foreign authorities**. However, under the Clarifying Lawful Overseas Use of Data (CLOUD) Act, enacted in 2018, service providers could respond positively to such requests. To this effect, the EU is working to sign a bilateral agreement with the US for e-evidence requests and as in the context of that strategy the second protocol to the Budapest Convention was signed. The great benefits of the second protocol of the Budapest convention are unquestionable, primarily because it establishes a reciprocal cooperation amongst the signatory parties (US, Japan, Colombia, EU countries, etc). However, the protocol provides for direct contact with service providers for the exchange of data which does not cover content data. Some of the difficulties expressed by LEAs revolve around the fact, that in order to get access to content data (emails, WhatsApp, etc.), the headquarters in Europe of the service providers require to contact the US based entity holding the data. LEAs claim that this is a lengthy process that can take up to years, and it does jeopardise criminal investigations, prosecutions, and convictions. This problem will not be overcome by the second protocol to the Budapest Convention since it does not contemplate content data access requests. To this effect, an EU-US agreement on cross-border access to e-evidence is being negotiated, but the e-evidence package would, in principle, provide the solution to this problem, since it provides

for data access requests to content data, however, to what extent service providers could refuse the provision of this type of data on the grounds of the servers being located in the US, is still questionable.

- The e-evidence package has received much criticism from the beginning. Legal practitioners and academics have argued that the proposed legislation extra limits the role of service providers. This reasoning is based on the grounds that services providers will be able to object to e-evidence requests if they manifestly violate the Charter of Fundamental Rights, leaving the **assessment of compliance with fundamental rights up to service providers**, hence the criticism.

- Another difficulty that LEAs have expressed is the fact that some providers provide access to some data (never content data) with the issuance of a **police order** while others, for the same data, require the issuance or attachment of a **judicial authorisation**. The proposed legislation if approved, will provide for access requests to be made on the basis of a judicial or prosecutor authorisation, therefore, even if burdensome for LEAs, will provide legal certainty and an extra layer of safeguards to the rights and freedoms of the persons being investigated. However, some domestic criminal procedure laws grant police powers for the obtention of certain categories of data without judicial authorisation, which enable for shorter timelines in getting the data.

- The e-evidence package is still under negotiation, and it is not clear whether it will be ever approved. The e-evidence package, amongst others, provides for LEAs direct requests to service providers established in another EU Member State without the involvement of the judicial authorities of the State where the service provider is established, and giving this way recognition to judicial decisions issued in the soil of other EU country. This **mutual recognition of judicial decisions** amongst EU members is not new, it has been implemented for civil matters for a long time, the novelty here is to apply it to criminal proceedings and investigations. However, while the e-evidence package and thus this mutual recognition of judicial decisions amongst EU member States is still under discussion, the second additional protocol to the Budapest Convention has been signed by several EU and non-EU countries for direct requests to service providers concerning subscriber and traffic data, therefore given effect partially to the e-evidence, which leads to the assumption that direct requests for content and transaction data might be the real point of dissent in the negotiation process.

- In line with the EDPS Opinion 7/2019, we consider that the Proposed Regulation does not effectively address **data security** for the transmission of e-evidence. Only one LEAs of those interviewed have a dedicated internal platform whereby the transmissions and communications with service providers take place, providing, amongst others, reassurance not only in terms of the confidentiality of the data exchanged but also to service providers since they can ascertain that the requests come from authorised LEAs. Article 8(2) of the proposed Regulation would allow the use of already established dedicated platforms or secure channels to handle requests. However, this remains optional. LEAs have expressed that the creation of a unique platform to communicate with service providers would be beneficial in terms of efficiency and data security.

- Having considered the opinions of the EDPS and the EDPB on the proposed legislation, both authorities suggest abandoning the idea of service providers granting access to content data by LEAs in different jurisdictions but within the EU.

4. Identification of practices affecting unregulated cyber investigation such as for example 'observation on the internet' 'infiltration of social media' rules for digital search and seizure.

When it comes to infiltration activities carried out by LEAs for the purposes of investigating, detecting, preventing or prosecuting crimes, this topic has been extensively covered in D4.2 *'Legal and Ethical issues about the use of Special Investigative Methodsto fight THB and CSA/CSE'* submitted at the time of submission of the present deliverable. D4.2 corresponds with Task 4.2 as described in the GA. The aim of this task is to conduct an analysis of the legal and ethical issues surrounding the use of UA and in particular the use of digital tools and strategies to support this activity. Subsequently, the use of infiltrated or under cover agents will not fall under the scope of this deliverable.

In the era of the Internet and Big Data, LEAs around the world are developing their own tools to perform searches on the Internet as part of their investigations. These tools are usually referred to as OSINT (Open Source Intelligence) tools and they have the capacity to collect information from publicly available sources on the Internet that do not require the use of special investigative methods[42] by the police.

Usually, the type of information collected through OSINT serves as 'intelligence' for LEAs, meaning that they can help in supporting lines of investigation, that is, information which leads to another information that allows to follow a line of investigation and in best case scenarios might lead to the reconstruction of the facts. The concept of intelligence should be separated from the concept of 'evidence' the latter only refers to material that can be relied upon during a criminal trial, that can be presented by the different parties that conform the criminal proceedings and ultimately assessed by a judge or jury. Therefore, OSINT data can conform intelligence during a police investigation but can also be admitted as evidence in the course of criminal proceedings.

Evidence and its admissibility in Court, is regulated at a national level by the different laws on criminal proceedings, however, there are some common elements shared by the signatories of the European Convention of Human Rights and all the EU Member States are bound by the EU Charter of Fundamental Rights, for instance, evidence will be open to challenge by the different parties taking place in criminal proceedings, evidence needs to be legally collected and presented during the course of a fair trial, and protection against self-incrimination. In order to be admissible evidence must be relevant to a fact, it needs to have a clear purpose and be fair. When LEAs intend to rely on OSINT material its important it meets these requirements[43].

When searching and seizing computers for the obtention of evidence, investigators also need to abide by domestic criminal laws. Generally, the search and seizure of electronic devices need judicial authorisation or warrant. Accredited investigators need to be aware and trained on their statutory powers to seize, extract and

[42] Intelligent Evidence: Using Open Source Intelligence (OSINT) in criminal proceedings, Fraser Sampson, 2016: https://journals.sagepub.com/doi/abs/10.1177/0032258X16671031
[43] Ibid page 5

retain digital devices from suspects in criminal investigations and their obligations with regards to data protection.

As part of the survey carried out in the previous section, LEAs did not specifically express having difficulties in the use of OSINT technologies or the seizure and search of electronic devices and presenting the information gathered as evidence during criminal proceedings, insofar as they comply with applicable laws, including laws pertaining to the chain of custody of the e-evidence. The chain of custody proves the integrity of a piece of evidence from the moment it is collected, stored, it is authentic and has not been altered. A record of the chain of evidence needs to be maintained at all times otherwise the evidence might be rendered inadmissible.

5. Conclusion

In this deliverable we have explored and analysed the current legal framework around e-evidence and data protection, including the 2 legislative proposals that were presented in 2018 and are still being negotiated amongst the different stakeholders within the EU. A survey has taken placed amongst LEAs to understand the common and specific difficulties that investigators face when trying to obtain e-evidence as part of a criminal investigation. Throughout the analysis performed in this deliverable, we can conclude amongst others, that LEAs need shorter timelines in gathering cross border e-evidence and that the e-evidence package would provide a solution for this problem. However, consensus for the approval of the e-evidence package has not yet been reached and cannot be foreseen in the near future.

The second protocol to the Budapest Convention, which has been recently signed by almost all EU Member States. It makes possible for LEAs of the signatory countries to get in direct contact with service providers for the acquisition of certain categories of data, the obligations therein are reciprocal, meaning that EU Member States will be able to request and receive data but are also obliged to provide data requested from LEAs based in a different Member Sate or a third country. The fact that the second protocol has been approved and signed and the e-evidence package is still under discussion, when both contain similar obligations except for content data – the second protocol does not include the possibility to request content data directly from providers -, suggests that the acquisition of content data without the judicial review and authorisation of the executing State is the real point of dissent of the e-evidence package. Content data is protected in most countries at constitutional level, through the form of the right to the secret to communications. It's a fundamental right that often, amongst others, distinguishes totalitarian states from democratic states.

The approval of the e-evidence package would represent a step forward in the mutual recognition for judicial decisions within the EU Member States. Mutual recognition is not a new concept in the EU, in civil matters it has long been implemented, yet mutual recognition of judicial decisions during the course of criminal proceeding has still a long way to go.

We have contacted representatives of major social network operators in an attempt to understand the difficulties faced when obtaining and compliance with access requests from LEAs from different jurisdictions (within the EU) to the one in which they are established. We will continue our efforts in trying to interview these actors for the purposes of the second iteration of this deliverable (D3.6) which will also contain an analysis of the agreement that the EU is negotiating with the US for the exchange of digital evidence, the agreement which has been recently signed between the US and the UK and the draft of the e-Privacy Regulation.

6. References

[1] European Commission, press release April 2018, FAQs: New rules to obtain electronic evidence: https://ec.europa.eu/commission/presscorner/detail/en/MEMO_18_3345

[2] European Commission, Impact Assessment Accompanying the document "Proposal for a Regulation of the European Parliament and of the Council on European Production and Preservation Orders for electronic evidence in criminal matters and Proposal for a Directive of the EP and the Council laying down harmonised rules on the appointment of legal representatives for the purpose of gathering evidence in criminal proceedings: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=SWD%3A2018%3A118%3AFIN

[3] European Commission, Impact Assessment accompanying the e-evidence package, 2018: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=SWD%3A2018%3A118%3AFIN

[4] Eurojust, November 2021 "Cross-border access to electronic evidence: update and impact of the pandemic on data requests": https://www.eurojust.europa.eu/news/cross-border-access-electronic-evidence-update-and-impact-pandemic-data-requests

[5] Convention established by the Council in accordance with Article 34 of the Treaty on European Union, on Mutual Assistance in Criminal Matters between the Member States of the European Union - Council Declaration on Article 10(9) - Declaration by the United Kingdom on Article 20: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A42000A0712%2801%29

[6] Council Act of 29 May 2000 establishing in accordance with Article 34 of the Treaty on European Union the Convention on Mutual Assistance in Criminal Matters between the Member States of the European Union: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32000F0712%2802%29

[7] Protocol established by the Council in accordance with Article 34 of the Treaty on European Union to the Convention on Mutual Assistance in Criminal Matters between the Member States of the European Union[1] https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A42001A1121%2801%29

[8] Eur- lex, Mutual Assistance in criminal matters between EU Member States: https://eur-lex.europa.eu/EN/legal-content/summary/mutual-assistance-in-criminal-matters-between-eu-countries.html

[9] Directive 2014/41, Article 2 (d): https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32014L0041

[10] Report on Eurojust's casework in the field of the European Investigation Order, November 2020, Page 21: https://www.eurojust.europa.eu/sites/default/files/assets/2020_11_eio_casework_report_corr.pdf

[11] 17 April, 2028, Impact Assessment Accompanying the document Proposal for a Regulation of the European Parliament and of the Council on European Production and Preservation Orders for electronic evidence in criminal matters and Proposal for a Directive of the European Parliament and of the Council laying down harmonised rules on the appointment of legal representatives for the purpose of gathering evidence in criminal proceedings: https://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1524129550845&uri=SWD:2018:118:FIN

[12] Directive of the European Parliament and of the Council laying down harmonised rules on the appointment of legal representatives for the purpose of gathering evidence in criminal proceedings: https://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1524129181403&uri=COM:2018:226:FIN

[13] Regulation of the European Parliament and of the Council on European Production and Preservation Orders for electronic evidence in criminal matters: https://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1524129181403&uri=COM:2018:225:FIN

[14] Explanatory Memorandum: Context of the Proposal, Directive of the European Parliament and of the Council laying down harmonised rules on the appointment of legal representatives for the purpose of gathering evidence in Criminal Proceedings, 2018: https://eur-lex.europa.eu/legal-content/EN/TXT/?LinkSource=PassleApp&uri=CELEX:52018PC0226

[15] 17 April, 2028, Table 4, Impact Assessment Accompanying the document Proposal for a Regulation of the European Parliament and of the Council on European Production and Preservation Orders for electronic evidence in criminal matters and Proposal for a Directive of the European Parliament and of the Council laying down harmonised rules

on the appointment of legal representatives for the purpose of gathering evidence in criminal proceedings: https://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1524129550845&uri=SWD:2018:118:FIN

[16] Article 4.3.c) E-Privacy Regulation proposal: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52017PC0010

[17] European Commission, FAQs: New EU rules to obtain electronic evidence: https://ec.europa.eu/commission/presscorner/detail/el/MEMO_18_3345

[18] The European Commission's E-evidence Proposal: Toward an EU-wide Obligation for Service Providers to Cooperate with Law Enforcement?, 2018, Vanessa Franssen, European Law Blog https://europeanlawblog.eu/2018/10/12/the-european-commissions-e-evidence-proposal-toward-an-eu-wide-obligation-for-service-providers-to-cooperate-with-law-enforcement/

[19] Second Additional Protocol to the Convention on Cybercrime on enhanced co-operation and disclosure of electronic evidence: https://search.coe.int/cm/pages/result_details.aspx?objectid=0900001680a48e4d

[20] Council of Europe European Convention on Human Rights https://www.consilium.europa.eu/es/policies/e-evidence/

[21] Charter of Fundamental Rights of the European Union: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:12012P/TXT

[22] EDPB Opinion 23/2018 on Commission Proposals on European Production and Preservation Orders for electronic evidence in criminal matters, Page 12, para 3: https://edpb.europa.eu/our-work-tools/our-documents/opinion-art-70/opinion-232018-commission-proposals-european-production_en

[23] EDPS Opinion 7/2019, November 2019: https://edps.europa.eu/sites/edp/files/publication/19-11-06_opinion_on_e_evidence_proposals_en.pdf

[24] Intelligent Evidence: Using Open Source Intelligence (OSINT) in criminal proceedings, Fraser Sampson, 2016: https://journals.sagepub.com/doi/abs/10.1177/0032258X16671031

