Intelligence Network & Secure Platform for Evidence Correlation and Transfer

D2.2 Legislative compliance relating to law-enforcement powers and evidence requirements

Document Summary Information

Grant Agreement No	833276	**Acronym**	INSPECTr
Full Title	**Intelligence Network & Secure Platform for Evidence Correlation and Transfer**		
Start Date	01/09/2019	**Duration**	42 months
Project URL	https://inspectr-project.eu		
Deliverable	2.2		
Work Package	2		
Contractual due date	28/02/2023	**Actual submission date**	27/02/2023
Nature	Report	**Dissemination Level**	PU
Lead Beneficiary	RUG		
Responsible Author	Melania Tudorica		
Contributions from	Melania Tudorica, Zuzanna Uba, Jeanne Mifsud Bonnici, Joe Cannataci		

This project has received funding from the European Union's Horizon 2020 research and innovation programme under the Grant Agreement No 833276.

Revision history (including peer reviewing & quality control)

Version	Issue Date	% Complete	Changes	Contributor(s)
v1.0		90	Initial Deliverable Structure	Melania Tudorica
			Edited by	Zuzanna Uba
			Reviewed by	Jeanne Mifsud Bonnici
V2.0		99	Final Deliverable Structure	Melania Tudorica
			Reviewed by	Fabrizio Turchi
			Reviewed by	Joshua Hughes
			Reviewed by	Tony Kavanagh
			Reviewed by	Jeanne Mifsud Bonnici
V3.0		100	Final version for submission	Melania Tudorica
V.3.1		100	Reviewed by	Joe Cannataci

Disclaimer

Copyright message

Table of Contents

Glossary of terms and abbreviations used

Abbreviation / Term	Description
ACPO	Association of Chief Police Officers
AFIS	Automated Fingerprint Identification System
AI	Artificial Intelligence
CDPC	The European Committee on Crime Problems
Charter	Charter of Fundamentals Rights
CSA	Child Sexual Abuse
CSAM	Child Sexual Abuse Material
CSIRTs	Cyber Security Incident Response Teams
Cybercrime Convention	The Council of Europe Convention on Cybercrime
DoA	Description of Action
DSA	Digital Services Act
EAW	European Arrest Warrant
ECHR	European Convention of Human Rights
EECC	EU Electronic Communications Code
eEDES	e-Evidence Digital Exchange System
EEG	Electronic Evidence Guide
EIO	European Investigation Order
EJN	European Judicial Network
ENISA	European Union Agency for Cybersecurity
EU	European Union
GDPR	General Data Protection Regulation
Interpol	International Criminal Police Organisation
JITs	Joint Investigation Teams
LEA Directive	LEA Data Protection Directive
LEAs	Law Enforcement Agencies
LL	Living Labs
MLA	Mutual Legal Assistance
NCMEC	National Center for Missing and Exploited Children
NI-ICS	Number-Independent Interpersonal Communications Services

NIS Directive	The Directive on Security of Network and Information Systems
OLAF	European Anti-Fraud Office
PC-CY	Committee of Experts on Crime in Cyberspace
SERE	Standardization of Evidence Representation and Exchange
SIAs	Security Intelligence Agencies
SIRENE	Supplementary Information Request at the National Entry
SIS	Schengen Information System
TFEU	Treaty on the Functioning of the European Union
UN	United Nations
USA	United States of America
WP	Work Package

List of legislation and documents

Full name and link to full text
Additional Protocol to the European Convention on Mutual Assistance in Criminal Matters [1978] ETS No. 099
Charter of Fundamental Rights of the European Union [2000] OJ C 364/01
Committee of Regions Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace [2013] JOIN(2013) 1 final
Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, *The European Agenda on Security* COM (2015) 185 final
Consolidated version of the Treaty on the Functioning of the European Union [2012] OJ C 326/47
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 [2000] OJ C 197/3
Convention for the Protection of Human Rights and Fundamental Freedoms [1950] ETS No. 005
Convention on Cybercrime [2001] ETS No. 185
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 [2000] OJ C 197/1
Council Decision 2007/533/JHA of 12 June 2007 on the establishment, operation and use of the second generation Schengen Information System (SIS II) [2007] OJ L 205/63
Council Framework Decision of 13 June 2002 on joint investigation teams [2002] OJ L162/1
Council Framework Decision of 13 June 2002 on the European arrest warrant and the surrender procedures between Member States (2002/584/JHA) [2002] OJ L 190/1
Council of Europe Data Protection and Cybercrime Division, Electronic Evidence Guide A basic guide for police officers, prosecutors and judges version 2.1, Strasbourg, France, 6 March 2020
Council of Europe, “Explanatory report to the Convention of Cybercrime” (ETS No 185)
Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union [2016] OJ L 194/1
Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detectio
Directive (EU) 2018/1972 of the European Parliament and of the Council of 11 December 2018 establishing the European Electronic Communications Code [2018] OJ L 321/36
Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications) [2002]
Directive 2013/40/EU of the European Parliament and of the Council of 12 August 2013 on attacks against information systems and replacing Council Framework Decision 2005/222/JHA [2013] OJ L 218

Directive 2014/41/EU of the European Parliament and of the Council of 3 April 2014 regarding the European Investigation Order in criminal matters [2014] OJ L131/1
Directive (EU) 2022/2557 of the European Parliament and of the Council of 14 December 2022 on the resilience of critical entities and repealing Council Directive 2008/114/EC [2022] OJ L 333, p. 164
Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (E
Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data [1995] OJ L 281/31
ENISA, *Cooperation between CSIRTs and Law enforcement: interaction with the Judiciary* [2018]
ENISA, *Electronic evidence - a basic guide for First Responders, Good practice material for CERT first responders* [2014]
ENISA, Identification and handling of electronic evidence – Handbook, document for teachers [2013] September 2013
European Convention on Mutual Assistance in Criminal Matters [1959] ETS No. 030
Proposal for a Regulation of the European Parliament and of the Council on European Production and Preservation Orders for electronic evidence in criminal matters, COM(2018) 225 final
Proposal for a Regulation of the European Parliament and of the Council concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Commu
Proposal for a Regulation of the European Parliament and of the Council laying down rules to prevent and combat child sexual abuse, COM/2022/209 final
Proposal for a Regulation of the European Parliament and of the Council laying down harmonised rules on Artificial Intelligence (Artificial Intelligence Act) and amending certain union legislative acts, COM/2021/206 final
Regulation (EC) No 1986/2006 of the European Parliament and of the Council of 20 December 2006 regarding access to the Second Generation Schengen Information System (SIS II) by the services in the Member States responsible for issuing vehicle registration
Regulation (EC) No 460/2004 of the European Parliament and of the Council of 10 March 2004 establishing the European Network and Information Security Agency [2004] OJ L 77
Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Da
Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market For Digital Services and amending Directive 2000/31/EC (Digital Services Act)
Regulation (EU) 2022/2554 of the European Parliament and of the Council of 14 December 2022 on digital operational resilience for the financial sector and amending Regulations (EC) No 1060/2009, (EU) No 648/2012, (EU) No 600/2014, (EU)

Regulation (EU) 2022/850 of the European Parliament and of the Council of 30 May 2022 on a computerised system for the cross-border electronic exchange of data in the area of judicial cooperation in civil and criminal matters (e-CODEX system), and amendin
Second Additional Protocol to the Convention on Cybercrime on enhanced co-operation and disclosure of electronic evidence [2022] CETS No. 224
The Schengen acquis - Convention implementing the Schengen Agreement of 14 June 1985 between the Governments of the States of the Benelux Economic Union, the Federal Republic of Germany and the French Republic on the gradual abolition of checks at their c

Executive summary

This document reports on the research conducted by WP2 on the INSPECTr Reference Framework for Standardization of Evidence Representation and Exchange. This reference framework to be implemented in the INSPECTr platform will facilitate standard solutions for forensic investigations across LEAs within the EU. The objective of this report is to provide the (final) legislative compliance relating to law-enforcement powers and evidence requirements as it stands at the end of the INSPECTr project. It is important to consider the applicable legal framework considering that LEAs are bound by law in their activities.

This Deliverable is devoted to understanding the legal requirements for law enforcement powers and evidence requirements, i.e. which legal instruments are applicable to investigations and to acquiring evidence, what powers (and restrictions) do law enforcement have to investigate in criminal procedures and share this with their colleagues across Europe, how do LEAs interact with each other and with other parties, which are the relevant data protection implications to be taken into account, etc. This was achieved in D2.1 by an analysis of the overarching European legislation and an analysis of the national legal frameworks of the countries where Living Labs (LL) were taking place. In D2.2 (this deliverable), an update of this applicable legal framework is provided in order to provide a final legal status quo at the end of the INSPECTr project.

There is a lot of fragmentation in the legal framework as regards digital evidence. National, European and international laws and regulations, bilateral agreements and multilateral agreements all play a role in regulating the gathering, analysis and exchange of digital evidence. The applicable legal framework consists of a patchwork of rules on cross-border gathering and transmission of evidence, mutual assistance and cooperation, security of network and information systems, cybercrime and data protection. There are currently several legal instruments in place which allow for the exchange of digital evidence. The use of legal instrument for evidence depends on the Member States involved. Section 2 of this reports shows the status quo of the applicable legal framework as it stands at the end of the INSPECTr project.

From submission of D2.1 mid-2021 until the end of the INSPECTr project there have been a number of legal developments to the applicable legal framework. These developments are discussed in section 3 of this report. This includes:

- A slow progression of the Commission's eEDES system and the launch thereof among Member States which will be used for EIOs and MLAs;
- Adoption of the NIS2 Directive which improves security of network and information systems and allows for CSIRTs to assist LEAs in investigations;
- The political agreement on the e-evidence package which will allow for direct cross-border requests for e-evidence to service providers in another Member State;
- The EU-US agreement negotiations which are likely to be resumed once the e-evidence package is adopted;
- The adoption of the Second Additional Protocol to the Cybercrime Convention (not yet in force) which will allow for enhanced cooperation and disclosure of electronic evidence and direct requests for e-evidence to service providers in another State Party;
- Other areas of developments such as the proposed new CSAM Regulation, the AI Act which is likely to be adopted soon and the DSA which allows for another way of collaboration between LEAs and service providers.

The developments are an improvement considering rapid technological developments, however, challenges and practical realities still remain:

- Cross-border collection and exchange of digital evidence can still be a time-consuming procedure considering differences in law and approach among Member States;
- Cross-border collection and exchange of digital evidence can still be a time-consuming procedure considering that it is not always clear to which competent authority the request needs to be sent;

- Legal, cultural and language differences, nuances of local laws and customs and differences in LEA capacities remain;
- Member States have different procedures and chains of command and currently all have their own systems in place. There is still a long way to go before uniform processing of evidence requests can take place.

The INSPECTr platform will allow an investigator to visualise and bookmark important evidential material, and export it to an investigative report by using various knowledge discovery techniques. This will allow for cross-correlation analysis with existing case data and improve knowledge discovery within a case, between separate cases and between interjurisdictional investigations. The platform will need to be flexible enough to adhere to the applicable legal framework and developments thereof.

1 Introduction

This document – "Legislative compliance relating to law-enforcement powers and evidence requirements" brings together the findings of work carried out in Task 2.1, Subtasks 2.1.1 and 2.1.2 of Work Package 2 – INSPECTr Reference Framework for Standardization of Evidence Representation and Exchange (SERE) – as explained in the Description of Action (DoA) of the INSPECTr project (Grant agreement no 833276).

The main objective of Work Package (WP) 2 – INSPECTr Reference Framework – is to provide a reference framework to be implemented in the INSPECTr platform which will facilitate standard solutions for forensic investigations across Law Enforcement Agencies (LEAs) within the European Union (EU) and internationally. Building such a framework cannot be done without regard for the law as LEAs are bound by law in their activities. As such, an important part of this reference framework is the analysis of the relevant legal status quo.

Task 2.1 was devoted to understanding the legal requirements for law enforcement powers and evidence requirements. These law enforcement powers and evidence requirements included an overview of the legal instruments applicable to investigations and to acquiring evidence, the powers (and restrictions) for law enforcement in investigating criminal procedures and sharing this with their colleagues across Europe, LEAs interaction with each other, Security Intelligence Agencies (SIAs), Computer Security Incident Response Teams (CSIRTs) and third party data owners, and the relevant data protection implications. This was achieved by desktop research of a wide collection of relevant documentation and available information and a questionnaire answered by the LEAs involved within the INSPECTr project in order to identify the existing national legal frameworks.

Subtask 2.1.1 dealt primarily with a legal status quo analysis and aimed at providing a comparative overview of legislation and practises in EU Member States and the resulting deliverable (D)2.1 provided the initial legislative compliance relating to law-enforcement powers and evidence requirements. Subtask 2.1.2 is aimed at providing updates on regulatory developments and supporting project workstreams and the resulting D2.2 (this deliverable) provides the (final) legislative compliance relating to law- enforcement powers and evidence requirements. This deliverable looks at the current status quo of the law and policy by assessing what developments have taken place, in Europe, including in relation to the United States of America (USA). These developments include several ongoing legislative proposals such as the e-evidence package and proposals as regards CSAM and AI as these topics have been specifically discussed within the context of the Living Labs (LL).

Part of subtask 2.1.2 according to the Description of Action (DoA) included supporting legal issues and requirements arising from the LL scenario interactions and a survey of technical issues about the training and technical capabilities with specific reference to LEA partners and recommendation for INSPECTr capacity building programme. However, throughout the lifetime of the INSPECTr project, no legal issues and requirements arose from the LL, meaning that this will be excluded from this deliverable. LLs were monitored throughout the lifetime of the INSPECTr project under WP8. As regards the survey of technical issues, the LEA feedback is focused on technical and investigative issues related to:

- CMS (Case Management System) which is related to The Hive (a scalable Security Incident Response Platform) and CORTEX (an Observable (i.e., elements of probative evidence) Analysis and Active Response Engine);
- GAD (Gadget): tools to process the elements of evidence, for instance the parsers developed to convert the XML report generated by forensic tools in CASE standard;
- CSAM, TERRO, FRAUD: referring to the Use Cases created by the LEAs to understand if the investigators were able to answer specific investigative queries by using the platform;
- GRELLI (Generic Reusable Embeddable Lightweight Widgets etc.): the widgets (table, word cloud, chart, map) developed within the context of the project;

- AI tools: are they used in day-to-day tasks, can tools like Translation, Automatic Speech Recognition (ASR), Optical Character Recognition (OCR) or Named-Entity Recognition (NER) be incorporated into work pipeline, etc.

The feedback received in these surveys is not related to legislative compliance relating to law-enforcement powers and evidence requirements. As a result of this, the input from these surveys will not be included in this deliverable. What will be included is an additional part on legal developments within the field of CSAM and AI considering that this has been addressed in the survey results and legal developments within the field are currently taking place.

As such, this deliverable focusses mainly on updating the work done in D2.1. It was created by reviewing the developments of proposed legislation mentioned in D2.1 and investigating whether additional developments have taken place in the field. This was done by desktop research, by reviewing policy documents, legal instruments, studies, literature, etc. and providing an update of the current legal status quo. As such, this deliverable will consist partly of a repetition of what was written in D2.1 in order to include the (final) legislative compliance document.

The results of this deliverable feed into the reference framework of WP2 and into the EU legislation management tool in WP3.

1.1 Mapping INSPECTr Outputs

The purpose of this section is to map INSPECTr Grant Agreement commitments, both within the formal Deliverable and Task description, against the project's respective outputs and work performed.

Table 1: Adherence to INSPECTr GA Deliverable & Tasks Descriptions

INSPECTr GA Component Title	INSPECTr GA Component Outline	Respective Document Chapter(s)	Justification
DELIVERABLE			
D2.2 Legislative compliance relating to law-enforcement powers and evidence requirements	*Provide updates on regulatory developments and support project workstreams [RUG, CNR, CCI] (m18-m42) a. Periodic reviews of regulatory developments in Europe and United States. There are several legislative proposals e.g. at a European level (such as the electronic evidence regulation and the e-privacy regulation) that may come into effect only in the later years of the project. Perform reviews to ensure that the legal*	*All components addressed throughout this Deliverable where relevant. Legal issues of LLs have not been reported.*	*Legal analysis of relevant legislation addressed from a national and European perspective. Survey of technical issues about the training and technical capabilities with specific reference to LEA partners and recommendation for INSPECTr capacity building programme.*

	baseline remains up-to-date with legislative developments throughout the life-time of the project. *b. Support legal issues and requirements arising from the Living Labs' scenario interactions* *c. Survey of technical issues about the training and technical capabilities with specific reference to LEA partners and recommendation for INSPECTr capacity building programme.*		
TASKS			
T2.1 Understanding, assessing and meeting legislative compliance relating to law-enforcement powers and evidence requirements. *ST2.1.2 Provide updates on regulatory developments and support project workstreams*	*a. Periodic reviews of regulatory developments in Europe and United States. There are several legislative proposals e.g. at a European level (such as the electronic evidence regulation and the e-privacy regulation) that may come into effect only in the later years of the project. Perform reviews to ensure that the legal baseline remains up-to-date with legislative developments throughout the life-time of the project.* *b. Support legal issues and requirements arising from the Living Labs' scenario interactions* *c. Survey of technical issues about the training and technical capabilities with specific reference to LEA partners and recommendation for INSPECTr capacity building programme.*	*All components addressed throughout this Deliverable where relevant.*	*Legal analysis of relevant legislation addressed from a national and European perspective. Survey of technical issues about the training and technical capabilities with specific reference to LEA partners and recommendation for INSPECTr capacity building programme.*

1.2 Scope

In criminal investigations, LEAs can use a variety of free and commercial digital forensic tools. The INSPECTr platform intends to reduce complexity by offering one platform with extended options for multi-level and cross-border collaboration, for reactive and preventative policing which, in turn, will facilitate the detection and prediction of cybercrime operations as well as crime trends. The INSPECTr project aims to develop a shared intelligent platform and a novel process for gathering, analysing, prioritising and presenting key data to facilitate this process by using forensic tools. The platform will allow an investigator to visualise and bookmark important evidential material, and export it to an investigative report by using various knowledge discovery techniques. This will allow for cross-correlation analysis with existing case data and improve knowledge discovery within a case, between separate cases and between inter-jurisdictional investigations. The gathering, analysis, prioritisation and sharing of data across jurisdictions for criminal investigations is regulated by law. To be able to investigate criminal matters, LEAs need a variety of powers to gather, preserve and exchange evidence such as search and seizure of stored computer data, real-time collection of traffic data and interception of content data, as evidence may come in the form of computer files, logs, transmissions, metadata, computer data, etc. The platform therefore, needs to be in line with relevant legislation, including fundamental rights.

Task 2.1.1 focused on law and practices in the EU Member States as regards digital evidence, including privacy and data protection. Following this legal assessment two things became clear: 1. the legal framework is fragmented, meaning that there is no uniform regulation and 2. there are many actors involved in the field. The actors involved in the field include LEAs, such as police forces on local, regional and national level, cybercrime units and specialised forces, CSIRTs, prosecution, the judiciary, national contact points and international and European agencies and bodies such as Interpol, Europol, Eurojust, and ENISA. This scattered landscape of legal instruments and actors involved in the field makes uniform investigation and sharing across Europe a challenge. This scattered landscape is also visible in the way information and evidence is shared by using the various secure channels operated by international and European agencies and bodies, including Europol's Secure Information Exchange Network Application (SIENA), the Camden Asset Recovery Inter-agency Network (CARIN) for more informal requests, the Schengen Information System (SIS) and the e-CODEX platform which will operate the e-Evidence Digital Exchange System (eEDES) for European Investigation Orders (EIOs) and the INSPECTr platform which will be used for ongoing investigations.

In task 2.1.2 the legal framework is re-assessed in order to provide an up-to-date status quo of the legal framework at the end of the INSPECTr project. As the INSPECTr project focusses mainly on a European solution and the countries involved in a LL are all European (EU Member States and United Kingdom), this deliverable focuses mainly on EU and Council of Europe legal instruments applicable to digital evidence.

As regards the connection between the legal compliance and the LL, no legal issues were reported throughout the lifetime of the project within the context of the LL. LLs were monitored throughout the lifetime of the INSPECTr project under WP8. Therefore, the legal issues and requirements from the LL scenario interactions will not be further elaborated upon in this deliverable. As regards the feedback received in the survey of technical issues, the replies did not relate to legislative compliance relating to law enforcement powers and evidence requirements. As a result of this, the input from these surveys will not be included in this deliverable. What will be included is an additional part on legal developments within the field of CSAM and AI considering that this has been addressed in the survey results and legal developments within the field are currently taking place.

2 The applicable legal framework

In D2.1 the initial legislative compliance relating to law-enforcement powers and evidence requirements was presented. This report discussed the European legal framework on digital evidence, privacy and data protection regulation and national legislation and practices and provided a reference framework from a legal perspective to be implemented in the INSPECTr platform, which will facilitate standard solutions for forensic investigations across LEAs within the EU. This legal analysis is highly important considering that LEAs are regulated and constrained by law in their activities. Considering that the law is dynamic, always changing, in particular in view of technological developments it is important to keep track of legal developments in the field. This deliverable presents the final status quo on the law as it stands at the end of the INSPECTr project.

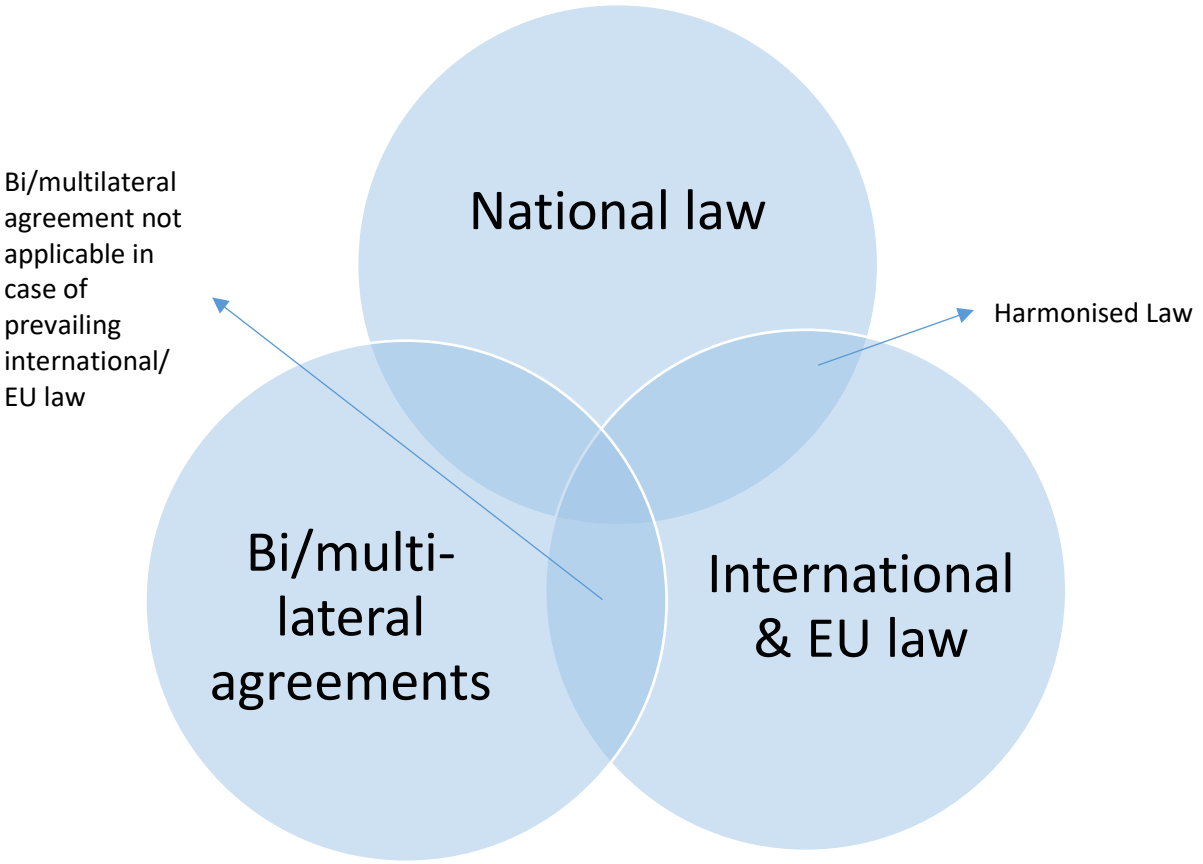
One of the most important conclusions as seen in D2.1 is that there is a lot of fragmentation in the area of law relating to law enforcement powers and evidence requirements. This fragmentation is caused by the fact that criminal law is based on the national laws and traditions of the Member States, including bilateral and multilateral agreements of collaboration between countries. As can be seen in section 4 of D2.1, the national laws and traditions in Ireland, Estonia, France, Belgium, Latvia and Romania (the six countries where the Living Labs are taking place) vary immensely. In spite of these differences, similarities can also be observed. Similarities are mainly caused by the fact that national law may be inspired by international instruments (and, as such, reflect the spirit of international instruments in national laws) or may implement international instruments. Within the context of the EU the competence to legislate in the field of criminal matters was traditionally left to the different Member States, however the power to harmonise some aspects of criminal procedural laws and to facilitate cooperation among states falls within the EU's competence[1]. With the creation of the Area of Freedom, Security and Justice, the EU can add important value to existing national criminal laws within the limits of its competence. There is however no comprehensive EU legal framework regarding criminal law that regulates law enforcement powers and evidence requirements. On an international level there is also no comprehensive legal framework, only several legal instruments that are relevant to law enforcement powers and evidence requirements, such as the Cybercrime Convention.

Taking this into consideration one can say that the applicable legal framework can be found in:

- national laws and traditions;
- bi/multilateral agreements;
- harmonised international and European law;
- international and European law.

This is visually simplified in the image below:

[1] Article 82 Treaty on the Functioning of the European Union (TFEU).



The added complexity in determining the applicable legal framework is that not all countries are participating in all legal instruments. Even on a European level, not all Member States participate in all EU legal instruments as can be seen for example by the fact that Ireland and Denmark have opted out of the European Investigation Order (EIO) Directive, which is currently the main legal instrument when it comes to sharing evidence across the EU. This means that there is no one size fits all when it comes to describing the applicable legal framework, but that it needs to be assessed on a case by case basis which legal instrument needs to be used in cross-border collaboration.

2.1 List of legislation

The list below shows the status quo of the applicable legal framework as it stands at the end of the INSPECTr project. This list is extracted from D2.1 and includes only the international and European legal framework. More detailed information on each legal instrument can be found in D2.1. Updates will be provided in section 3 of this deliverable. Legislation that has been approved, but which is not yet in force can be found in grey in the list below. National law will not be included in this deliverable as there has not been an inquiry on national legal updates within the INSPECTr project. The national legal framework (including bilateral and multilateral agreements) applicable to the countries participating in the Living Labs is reflected in D2.1.

1. European Investigation Order (EIO)

Regime	European Union
Type of instrument	Directive
Link to full text	https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32014L0041&from=EN
Status	In force
Focusses on	Cross-border investigation
Relevance	Cross-border gathering and transmission of evidence
Additional comments	Does not apply in Ireland and Denmark[2]

2. EU 2000 Convention

Regime	European Union
Type of instrument	Convention
Link to full text	https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:42000A0712(01)&from=EN
Status	In force
Focusses on	Mutual assistance in criminal matters
Additional comments	The EIO Directive replaces the corresponding provisions of this Convention for the Member States bound by the EIO Directive

3. Schengen Implementing Convention and SIS

Regime	European Union
Type of instrument	Convention
Link to full text	https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:42000A0922(02)&from=EN
Status	In force
Focusses on	External borders, police cooperation

[2] See Recitals 43 – 45 EIO Directive.

Relevance	Police cooperation, secure Schengen Information System (SIS)
Additional comments	The EIO Directive replaces the corresponding provisions of this Convention for the Member States bound by the EIO Directive[3]; Bulgaria, Romania and Cyprus not yet part of the Schengen Area; Does not apply in Ireland; SIS operated by Bulgaria, Romania and Ireland

4. European Arrest Warrant

Regime	European Union
Type of instrument	Decision
Link to full text	https://eur-lex.europa.eu/resource.html?uri=cellar:3b151647-772d-48b0-ad8c-0e4c78804c2e.0004.02/DOC_1&format=PDF
Status	In force
Focusses on	Extradition
Relevance	May be used in combination with EIO or mutual assistance requests and includes the handing over of evidence in connection with the extradition

5. Decision on exchange of information and intelligence

Regime	European Union
Type of instrument	Decision
Link to full text	https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32006F0960&from=EN
Status	In force
Focusses on	Exchange of information and intelligence
Additional comments	Replaces related provisions of the Schengen implementing Convention as regards exchange of information and intelligence for the purpose of criminal investigations

[3] Article 24 EIO Directive.

6. e-CODEX Regulation

Regime	European Union
Type of instrument	Regulation
Link to full text	https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX%3A32022R0850
Status	In force
Focusses on	Legal framework for the technological backbone of digitisation of EU judicial cooperation
Additional comments	The e-CODEX platform runs the eEDES system which is currently being deployed by the Commission and Member States for EIOs and MLAs

7. Joint investigation teams

Regime	European Union
Type of instrument	Council Framework Decision
Link to full text	https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32002F0465&from=EN
Status	In force
Focusses on	Joint Investigation Teams
Additional comments	The EIO Directive does not apply to the gathering of evidence in JITs

8. NIS2 Directive

Regime	European Union
Type of instrument	Directive
Link to full text	https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32022L2555&from=EN
Status	In force
Focusses on	Security of network and information systems
Relevance	CSIRTs

Additional comments	Replaced the NIS Directive (https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016L1148&from=EN) in January 2023 Network and Information Security is further strengthened by the: • Critical Entities Resilience (CER) Directive[4] https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32022L2557 • Digital Operational Resilience Act (DORA) Regulation https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32022R2554

9. Digital Services Act

Regime	European Union
Type of instrument	Regulation
Link to full text	https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32022R2065
Status	In force
Focusses on	Safe digital space
Relevance	Exchange of information between providers of hosting services and LEAs or judicial authorities, notification of suspicions of criminal offences by providers of hosting services
Additional comments	Is part of the Digital Services Act package which also includes the Digital Markets Act which is more focussed on EU competition and antitrust.

10. European Convention on Mutual Assistance in Criminal matters

Regime	Council of Europe
Type of instrument	Convention
Link to full text	https://www.coe.int/en/web/conventions/full-list/-/conventions/rms/09000016800656ce
Status	In force
Focusses on	MLA
Relevance	Cross-border gathering of evidence

[4] Directive (EU) 2022/2557 of the European Parliament and of the Council of 14 December 2022 on the resilience of critical entities and repealing Council Directive 2008/114/EC [2022] OJ L 333, p. 164.

Additional comments	The EIO Directive replaces the corresponding provisions of this Convention for the Member States bound by the EIO Directive

11. Cybercrime Convention

Regime	Council of Europe
Type of instrument	Convention
Link to full text	https://www.coe.int/en/web/conventions/full-list/-/conventions/rms/0900001680081561
Status	In force
Focusses on	Cybercrime
Relevance	Also applies to digital evidence
Additional comments	Legally binding, large number of signatories beyond the EU

12. Second Additional Protocol to the Cybercrime Convention

Regime	Council of Europe
Type of instrument	Protocol
Link to full text	https://rm.coe.int/1680a49dab
Status	Not yet in force, is likely to enter into force in 2023. Needs 5 State ratifications to come into force. As of February 2023, Serbia only had ratified the Second Additional Protocol.
Focusses on	Enhanced cooperation and disclosure of electronic evidence
Relevance	Requests for e-evidence directly to service providers in another State Party
Additional comments	Large number of signatories beyond the EU

13. General Data Protection Regulation (GDPR)

Regime	European Union
Type of instrument	Regulation
Link to full text	https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679&from=EN

Status	In force
Focusses on	Data protection
Relevance	General data protection rules, directly applicable

14. Law Enforcement Directive

Regime	European Union
Type of instrument	Directive
Link to full text	https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016L0680&from=EN
Status	In force
Focusses on	Data protection in the context of law enforcement
Relevance	Specific harmonising LEA data protection rules

15. European Production and Preservation Orders

Regime	European Union
Type of instrument	Regulation
Link to compromise text	https://data.consilium.europa.eu/doc/document/ST-5448-2023-INIT/en/pdf
Status	Not yet force, is likely to enter into force in 2023. Agreement on compromise text reached in January 2023. Council and European Parliament are expected to vote on the compromise text during 2023.
Focusses on	European Production and Preservation Orders for electronic evidence in criminal proceedings and for the execution of custodial sentences following criminal proceedings, direct cross-border requests for e-evidence to service providers in another Member State
Relevance	Gathering electronic evidence

16. Legal representatives Directive

Regime	European Union
Type of instrument	Directive

Link to compromise text	https://data.consilium.europa.eu/doc/document/ST-5449-2023-INIT/en/pdf
Status	Not yet in force, is likely to enter into force in 2023
Focusses on	Rules on the designation of designated establishments and the appointment of legal representatives for the purpose of gathering electronic evidence in criminal proceedings within the context of European Production and Preservation Orders
Relevance	Gathering electronic evidence

3 Developments in the field

Considering that the law is dynamic and constantly in need of change in particular due to technological developments, this section is aimed at providing updates on regulatory developments in order to provide the (final) legislative compliance relating to law- enforcement powers and evidence requirements. This section looks at the developments that have taken place in order to provide an up to date legal status quo.

3.1 EIO and the eEDES system

The European Investigation Order (EIO) Directive is a comprehensive system that allows EU Member States to obtain evidence in criminal cases at all stages of criminal proceedings in other Member States and aims to simplify and speed up cross border criminal investigations in the EU. This is important considering that cross-border collection and exchange of digital evidence can still be a time-consuming procedure, which is challenging considering the volatile nature of digital evidence which is easily altered or deleted. The EIO Directive as such has not been updated and is currently still in effect as was described in D2.1. However, it is worth mentioning that training within the EIO context is currently ongoing by the TREIO project[5]. TREIO is one of the key projects aiding in the EU-wide deployment of the e-Evidence Digital Exchange System (eEDES). This platform for exchanging EIOs is an improvement considering the differences between Member States in exchanging evidence. While there is a certain level of harmonisation and digitisation in place, some authorities still rely on 'regular' post to send requests for evidence. Especially if it is not exactly clear to which competent authority the request needs to be sent it may take longer than necessary for a request to arrive at its correct destination. The eEDES system, operated on the e-Codex platform, will improve the process of exchanging evidence and tackle this challenge.

By way of the e-CODEX Regulation[6] which entered into force in 2022, the e-CODEX system has become the technological backbone of the digitisation of EU judicial cooperation in both civil and criminal matters for which the Regulation established the legal framework. e-CODEX consists of a package of software products that allow for secure digital communication between courts, and between citizens and the courts, in particular enabling the secure exchange of judicial documents. The e-CODEX platform is currently used for communications as regards European order for payment procedure, European small claims procedure, mutual recognition of financial penalties procedure and EIOs and MLAs.

eEDES is the core service platform (run on e-CODEX) for electronic evidence that manages the EIO and MLA procedures on a European level that is being developed by the e-Evidence project led by the European Commission (Directorate General (DG) Justice and Consumers). The system is under continuous development and the rollout among the Member States is currently taking place. The TREIO project provides an all-round cross-border training on the EIO, including demo and video tutorials on the use of the eEDES system. Both the e-Evidence project and the TREIO project are delayed considering that in the implementation the project timeline and the system's deployment need to be aligned. Member States all have their own pace and roll-out within their national projects, meaning that the trainings can only take place when Member States are ready for this. Several national trainings have taken place within the context of the TREIO project where the TREIO project trained national master trainers and offered further support to these master trainers for further training within their national institutions dealing with the EIO. Apart from these national training the TREIO project will also develop an e-learning course and organise international online sessions with representatives from other Member States. In the international sessions Member States are paired upon completion of trainings and will thus get a chance to train with their international colleagues. These trainings are important considering that the EIO is

[5] <https://treio.eu>.

[6] Regulation (EU) 2022/850 of the European Parliament and of the Council of 30 May 2022 on a computerised system for the cross-border electronic exchange of data in the area of judicial cooperation in civil and criminal matters (e-CODEX system), and amending Regulation (EU) 2018/1726 [2022] OJ L 150, p. 1.

currently the leading legal instrument for exchanging evidence within the EU. The EIO Directive replaces the corresponding provisions of many of the other MLA legal instruments for the Member States bound by the EIO Directive as discussed in D2.1.

3.2 Cybersecurity of network and information systems

The Directive on Security of Network and Information Systems[7] (NIS Directive) was described in D2.1 and provides legal measures for a high level of cybersecurity in the EU to respond to cybersecurity challenges.[8] Article 23 of the Directive determines that the Commission needs to periodically review the functioning of the NIS Directive and report to the European Parliament and to the Council. Following the review of the NIS Directive in 2020, the Commission identified 3 weaknesses due to differences in implementation of the Directive:

- low level of cyber resilience of businesses operating;
- inconsistent resilience across Member States and sectors;
- low level of joint situational awareness and lack of joint crisis response.[9]

Differences in implementation are for example visible in the healthcare sector, where in some Member States hospitals do fall within the scope of the NIS Directive and in others they do not. In order to address these weaknesses and to modernise the Directive following increased digitisation of the internal market and evolving cybersecurity threats, amplified by COVID-19, a legislative proposal for the new (NIS2) Directive was presented in December 2020.[10] On 30 May 2022, a political agreement was reached between the European Parliament and the Council, which was subject to formal approval.[11] On 27 December 2022, the new NIS2 Directive was published in the Official Journal of the European Union.[12] It entered into force on the twentieth day following this publication and Member states will have 21 months from the entry into force of the Directive to implement the provisions into their national law. The NIS2 Directive replaced the NIS Directive and aims to improve the system of cybersecurity risk management, in light of the European Commission's Work Program for 2023, under the area of 'A Europe fit for the Digital Age'.

In order to increase the level of cybersecurity within the EU, the NIS2 Directive obliges more entities and sectors to take cybersecurity risk management measures by including medium and large entities from more sectors that are critical for the economy and society within the scope of the Directive. Critical sectors include for example providers of public electronic communications services, digital services, waste water and waste management, manufacturing of critical products, postal and courier services and public administration.[13] The Directive also covers more broadly the healthcare sector, for example by including medical device manufacturers. The NIS2 Directive thus extends the scope of application to provide for a comprehensive coverage of some of the most essential and important economic sectors, such as energy, transport, banking, but also food production,

[7] Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union [2016] OJ L 194/1.

[8] See recital 4 and 5 Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union [2016] OJ L 194/1.

[9] See Proposal for a Directive of the European Parliament and of the Council on measures for a high common level of cybersecurity across the Union, repealing Directive (EU) 2016/1148, COM(2020) 823 final, para. 1, under Reasons for and objectives of the proposal.

[10] Proposal for a Directive of the European Parliament and of the Council on measures for a high common level of cybersecurity across the Union, repealing Directive (EU) 2016/1148, COM(2020) 823 final.

[11] See <https://ec.europa.eu/commission/presscorner/detail/en/ip_22_2985>.

[12] Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 [2022] OJ L 333, p. 80.

[13] See Proposal for a Directive of the European Parliament and of the Council on measures for a high common level of cybersecurity across the Union, repealing Directive (EU) 2016/1148, COM/2020/823 final.

processing and distribution and digital providers.[14] Network and Information Security is further strengthened by the Critical Entities Resilience (CER) Directive[15] and by the Digital Operational Resilience Act (DORA) Regulation[16] which entered into force simultaneously with the NIS2 Directive. The CER Directive strengthens the resilience of critical entities in a number of sectors (such as energy, transport, health, drinking water, waste water and space) and the DORA Regulation strengthens the IT security of financial entities such as banks, insurance companies and investment firms.

The NIS2 Directive is divided into nine chapters which include general provisions as regards scope and minimum harmonisation requirements, coordinated security frameworks, rules on cooperation, cybersecurity risk-management measures and reporting obligations, jurisdiction and registration, provisions relating to information sharing, security and enforcement, provisions on delegated and implementing acts and final provision. As opposed to NIS Directive, the NIS2 Directive established uniform rules on which entities are operators of essential services in order to eliminate the current divergences between the assessments by individual MS. The specific criteria include the cap-size rule, where all medium and large enterprises, as defined in the Commission Recommendation 2003/361/EC[17], operating within the sectors of the Directive, fall within its scope.[18] Regardless of the size of the entity, the NIS2 will also apply to public administration entities of central and local governments, regarded as such in accordance with national law and pursuant to more specific rules in Annex I of the Directive.[19] According to Article 2 (7 – 9), the NIS2 Directive does not apply to public administration entities in the areas of defence, national or public security, or law enforcement, including the investigation, detection and prosecution of criminal offences.[20]

When it comes to cybersecurity risk management measures, the NIS2 Directive imposes the requirement of implementing appropriate and proportionate technical and organisational measures to manage the risks posed to the security of network and information systems which those entities make use of, to prevent or minimise the risks of impacts on the recipients of their services. Article 18 outlines a list of minimum measures to be adopted by the entities, such as incident handling and business continuity management.[21] The Directive also amends the incident reporting requirements, by introducing a system of notification in phases, including an initial notification within 24 hours of becoming aware of a potential risk or incident, followed by an 'intermediate' and 'final' reporting obligations to the Computer Security Incident Response Teams (CSIRTs) or other relevant authority.[22] The designation of CSIRTs is an important aspect within the INSPECTr project considering their supporting role in investigations. The tasks and competences of CSIRTs have expanded following the more elaborate scope of the NIS2 Directive and include monitoring cyber threats, vulnerabilities and incidents at national level, providing early warning, responding to incidents, providing dynamic risk and incident analysis, providing a proactive scanning of the network and information systems and participating in the CSIRTs network. While they do not have the same powers as LEAs, CSIRTs play an important role in supporting investigations and work closely with

[14] Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 [2022] OJ L 333, Art. 1(2, b).

[15] Directive (EU) 2022/2557 of the European Parliament and of the Council of 14 December 2022 on the resilience of critical entities and repealing Council Directive 2008/114/EC [2022] OJ L 333, p. 164.

[16] Regulation (EU) 2022/2554 of the European Parliament and of the Council of 14 December 2022 on digital operational resilience for the financial sector and amending Regulations (EC) No 1060/2009, (EU) No 648/2012, (EU) No 600/2014, (EU) No 909/2014 and (EU) 2016/1011 [2022] OJ L 333, p. 1.

[17] Commission Recommendation of 6 May 2003 concerning the definition of micro, small and medium-sized enterprises [2003] OJ L 124, p. 36.

[18] Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 [2022] OJ L 333, p. 82.

[19] Ibid, Art. 2.

[20] Ibid, Art. 2-3(a).

[21] Ibid, Art. 21(b)-(c).

[22] Ibid, Art. 23.

LEAs considering that incidents can be the result of criminal activities. CSIRTs can for example discover suspicious activity of which they can inform LEAs, but they can also play a role in the investigation by providing technical expertise, support the gathering and preservation of evidence and sharing the information they have or have access to. In case of a formal involvement of CSIRTs in criminal investigations, the prosecutor is often consulted who needs to give consent for the involvement of the CSIRT in gathering, handling and analysing evidence.[23]

3.3 E-evidence package

In 2018, the Commission proposed a Regulation[24] and a Directive[25] (the e-evidence package) with the aim to make the exchange of digital evidence easier and faster for police and judicial authorities. The Regulation introduces a European Production Order and a European Preservation Order for digital evidence in criminal matters and the Directive introduces harmonised rules for legal representatives for gathering evidence in criminal proceedings. These new legal instruments will not replace the EIO Directive, but will provide an additional tool for authorities. A production order is an instruction from an issuing authority, such as LEAs, to a service provider, to deliver or make available certain information which is considered to be digital evidence. A preservation order requires the service provider to preserve the digital evidence in view of the subsequent request for production.[26] These tools are considered to be necessary due to the fact that network-based services can be provided from anywhere in the world. As a consequence, the digital evidence is often stored outside of the jurisdiction of the Member State investigating a crime. As such, the investigating authority needs to request the Member State where the service provider is based for mutual assistance. In view of the growing number of digital evidences, these requests through the official channels can take a long time. Combining this with the lack of a clear framework for cooperation with service providers makes it challenging for service providers to comply with LEA requests, in particular LEAs from another country. The new Regulation will allow LEAs to approach the service providers directly, without the involvement of a judicial authority in another Member State. Considering that the choice of legal instrument is a Regulation, the EU is making it clear that it does not want implementation issues negatively affecting the effectiveness of the new tools.[27] In addition to this, the Directive will lay down harmonised rules, obliging service providers in the EU to designate at least one legal representative for the receipt of, compliance with and enforcement of production and preservation orders and any other orders issued in the context of gathering evidence in criminal proceedings. Having legal representatives means that LEAs will have a clear point of access to address service providers.

This e-evidence package has been criticised from the onset by lawyers, media and journalists associations, civil society groups, internet companies and also by the European Parliament. Several articles, open letters and consultation papers have been published demanding for stronger safeguards for fundamental rights.[28] In its opinion[29], the European Data Protection Supervisor (EDPS) stressed that the definitions of data categories in the

[23] See for more information on the roles of CSIRTs and LEAs and their cooperation: ENISA, *Cooperation between CSIRTs and Law enforcement: interaction with the Judiciary* [2018], available at <https://www.enisa.europa.eu/publications/csirts-le-cooperation>.

[24] Proposal for a Regulation of the European Parliament and of the Council on European Production and Preservation Orders for electronic evidence in criminal matters, COM (2018) 225 final.

[25] 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, COM (2018) 226 final.

[26] See Article 2 of the Proposed Regulation.

[27] See also A. Tinoco-Pastrana, *The Proposal on Electronic Evidence in the European Union*, EUCRIM 1/2020, p.46.

[28] See for example <https://www.ebu.ch/files/live/sites/ebu/files/News/Position_Papers/open/2021_05_18_EevidenceJointLetter_18May2021.pdf> and <https://www.fairtrials.org/app/uploads/2022/02/E-evidence-position-paper-February-2019.pdf>.

[29] European Data Protection Supervisor, Opinion 07/2019, EDPS Opinion on Proposals regarding European Production and Preservation Orders for electronic evidence in criminal matters, 6 November 2019, available at <https://edps.europa.eu/sites/default/files/publication/19-11-06_opinion_on_e_evidence_proposals_en.pdf>.

proposed Regulation should be clarified and consistent with other definitions of data categories in EU law and makes specific recommendations including the authenticity and confidentiality of orders and data transmitted, the limited preservation under European Preservation Orders, the data protection framework applicable, the rights of data subjects, data subjects benefiting from immunities and privileges, the legal representatives, the time limits to comply with European Production Orders and the possibility for service providers to object to orders.

Negotiations in the political trilogue between the Council, European Parliament and the Commission had been taking place since 2018. The European Parliament initially produced a draft report[30] on the subject with 267 amendments to the proposal, while the different political groups introduced a total of 841 amendments[31]. Statewatch reported on 6 July 2022 that there has been a turning point in the negotiations and that both legislators have confirmed their willingness to finalise soon.[32] On 25 January 2023, a press release was issued confirming that agreement has been reached on the e-evidence package.[33] On 20 January 2023, the Council's Permanent Representatives Committee (COREPER) was invited to analyse and confirm the final compromise text of the e-evidence package.[34] Assuming that the text will be confirmed and that the European Parliament will adopt its position at first reading, the Council will approve the European Parliament's position after which the e-evidence package will be adopted in the wording which corresponds to the European Parliament's position. At the time of writing this deliverable on the eve of closing the INSPECTr project, the e-evidence package has thus not yet been adopted. However, with these developments the e-evidence package is likely to come into force within the course of 2023. Once it comes into force, the e-evidence package's alternative mechanism to the existing international cooperation and MLA tools will allow LEAs to address judicial orders for electronic evidence directly to service providers in another Member State which will speed up cross-border requests for e-evidence considerably.

3.4 Cooperation with third countries

Considering that crimes do not stop at EU borders and digital evidence can be stored anywhere in the world, it is not enough to regulate the exchange of digital evidence only within a European context. As a consequence, the Council authorised the Commission to negotiate an agreement on behalf of the EU with the United States of America (USA)[35] and to participate in negotiations with the Council of Europe on a second additional protocol to the Cybercrime Convention[36]. These international negotiations aim at improving cooperation with third (non-EU) countries.

[30] Available at <https://www.europarl.europa.eu/doceo/document/A-9-2020-0256_EN.html#title3>.
[31] See <https://www.europarl.europa.eu/doceo/document/LIBE-AM-644870_EN.pdf>.
[32] See <https://www.statewatch.org/news/2022/july/eu-end-game-approaching-for-e-evidence-negotiations-says-french-presidency/>.
[33] <https://www.consilium.europa.eu/en/press/press-releases/2023/01/25/electronic-evidence-council-confirms-agreement-with-the-european-parliament-on-new-rules-to-improve-cross-border-access-to-e-evidence/>.
[34] Council of the European Union, Interinstitutional File: 2018/0108(COD), Brussels 20 January 2023, 5448/23, available at < https://data.consilium.europa.eu/doc/document/ST-5448-2023-INIT/en/pdf> and Council of the European Union, Interinstitutional File: 2018/0107(COD), Brussels 20 January 2023, 5449/23, available at <https://data.consilium.europa.eu/doc/document/ST-5449-2023-INIT/en/pdf>.
[35] Council of the European Union, Brussels, 21 May 2019, 9114/19, available at <https://data.consilium.europa.eu/doc/document/ST-9114-2019-INIT/en/pdf>; Recommendation for a Council Decision authorising the opening of negotiations in view of an agreement between the European Union and the United States of America on cross-border access to electronic evidence for judicial cooperation in criminal matters, COM(2019) 70 final. See for the negotiating directive: <https://data.consilium.europa.eu/doc/document/ST-9666-2019-INIT/en/pdf>.
[36] Council of the European Union, Brussels, 21 May 2019, 9116/19, available at <https://data.consilium.europa.eu/doc/document/ST-9116-2019-INIT/en/pdf>; Recommendation for a Council Decision authorising the participation in negotiations on a second Additional Protocol to the Council of Europe Convention on

3.4.1 EU-US agreement

In 2018, the USA enacted the Clarifying Lawful Overseas Use of Data (CLOUD) Act in order to improve procedures for investigators in obtaining access to electronic information held by service providers. This Act allows LEAs in the USA in certain cases access to extraterritorially located data, meaning that European companies may fall within the scope of the CLOUD Act. This Act was highly criticized, both within the USA and outside the USA, including by civil rights groups for reasons of fundamental rights. Due to the extraterritorial nature of the CLOUD Act, it may conflict or interfere with laws in other countries. Recent research of the Dutch National Cybersecurity Centre has shown that European companies and European-based data storage are not immune to non-European legislation such as the CLOUD Act.[37] In its joint legal assessment, the EDPS and the European Data Protection Board (EDPB) found a possible conflict between the CLOUD Act and the GDPR.[38] Following the entry into force of the CLOUD Act, the Commission adopted a Recommendation for a Council Decision to authorise the opening of negotiations in view of an international agreement between the EU and the USA on cross-border access to electronic evidence for judicial cooperation in criminal matters.

The objective of the EU-US agreement is to set common rules and address conflicts of law regarding orders for obtaining electronic evidence, to allow for a transfer of electronic evidence by a service provider to a requesting authority and to ensure respect for the fundamental rights, freedoms and general principles of EU law.[39] Service providers in the USA currently collaborate with European LEAs on a voluntary basis or through MLA procedures. However, laws in the USA do not always allow service providers to respond to European requests directly. An agreement between the EU and the USA will thus facilitate cooperation, while ensuring safeguards.[40] In particular a strong protection mechanism was emphasised by the European Data Protection Supervisor (EDPS) in its opinion on the negotiating mandate.[41]

Negotiations with the United States to facilitate cross-border access to e-evidence for judicial cooperation in criminal matters started in September 2019 and are currently still ongoing. The Commission periodically informs the Council about the state of play of these negotiations. In June 2022, a meeting was held in Washington between the EU's commissioner for justice and US Attorney General which did not progress negotiations between the EU and the USA as the EU's e-evidence package was still being negotiated within the EU.[42] In December 2022 in a press speaking point, Commissioner Reynders said that it was decided to re-launch EU-USA negotiations on electronic evidence after final adoption of the e-evidence package.[43] The e-evidence package is likely to come into force within the course of 2023 as described above, meaning that negotiations between the EU and the USA are likely to also restart within the course of 2023, unfortunately not within the lifetime of the INSPECTr project.

Cybercrime (CETS No. 185), COM(2019) 71 final. See for the negotiating directive: <https://data.consilium.europa.eu/doc/document/ST-9664-2019-INIT/en/pdf>.

[37] See <https://www.ncsc.nl/actueel/weblog/weblog2022/de-werking-van-de-cloud-act-bij-dataopslag-in-europa>.

[38] EDPB-EDPS Joint Response to the LIBE Committee on the impact of the US Cloud Act on the European legal framework for personal data protection (annex), available at <https://edpb.europa.eu/sites/default/files/files/file2/edpb_edps_joint_response_us_cloudact_annex.pdf>.

[39] Annex to the Recommendation for a Council decision authorising the opening of negotiations in view of an agreement between the European Union and the United States of America on cross-border access to electronic evidence for judicial cooperation in criminal matters, Article 1.

[40] Annex to the Recommendation for a Council decision authorising the opening of negotiations in view of an agreement between the European Union and the United States of America on cross-border access to electronic evidence for judicial cooperation in criminal matters, Article 3.

[41] European Data Protection Supervisor, Opinion 2/2019, EDPS Opinion on the negotiating mandate of an EU-US agreement on cross-border access to electronic evidence, 2 April 2019. See also: Summary of the Opinion of the European Data Protection Supervisor on the negotiating mandate of an EU-US agreement on cross-border access to electronic evidence [2019] OJ C 186, p. 17.

[42] See for example <https://www.lawfareblog.com/has-time-eu-us-agreement-e-evidence-come-and-gone>.

[43] <https://ec.europa.eu/commission/presscorner/detail/en/STATEMENT_22_7784>.

3.4.2 Second Additional Protocol to the Cybercrime Convention

Apart from the negotiations between the EU and the USA, the Commission was also authorised to participate in negotiations on a second Additional Protocol to the Cybercrime Convention. The second Additional Protocol[44] aims at more effective MLA, including for example direct cooperation with service providers in other jurisdictions which are parties to the Convention. It provides for a framework and safeguards for cross-border requests, which include data protection requirements. The advantages of having the Cybercrime Convention and its protocols in place is that the reach of the Council of Europe's regime extends beyond the EU.[45]

The Second Additional Protocol was adopted by the Council of Europe on 17 November 2021 and opened for signature on 12-13 May 2022. Since only states can sign the Protocol, the EU authorised Member States to sign it in the interest of the EU.[46] The Protocol enters in to force when five countries have ratified it. Currently 33 countries have signed the Protocol, one country, Serbia has ratified the Protocol in February 2023.[47] This means that it is not likely that the Protocol will enter into force within the lifetime of the INSPECTr project, but that it will soon after.

The Protocol consists of common provisions, measures for enhanced cooperation, conditions and safeguards and final provisions. It applies to criminal investigations or proceedings concerning criminal offences related to computer systems and data, and to the collection of evidence in electronic form of a criminal offence.[48] Measures for enhanced cooperation include procedures enhancing direct cooperation with providers and entities in other State Parties (chapter 2, section 2), procedures enhancing international cooperation between authorities for the disclosure of stored computer data (chapter 2, section 3), procedures pertaining to emergency mutual assistance (chapter 2, section 4) and procedures pertaining to international co-operation in the absence of applicable international agreements (chapter 2, section 5). Much like the EU's e-evidence package, the Protocol will facilitate direct requests to service providers in other countries which will speed up requests for cross-border electronic evidence considerable.

3.5 Other relevant areas of regulation

There are many developments going on in the digital sphere. While this report discusses the legal framework applicable to digital evidence and LEA powers, there are other area of law which may not necessarily regulate digital evidence and LEA powers as such, but which do influence digital evidence regulation and approach following technological developments. The most important developments are highlighted in this section, which includes developments in the field of online Child Sexual Abuse (CSA), Artificial Intelligence (AI) and digital services. Child Sexual Abuse Material (CSAM) is per definition digital evidence and the INSPECTr project is using

[44] Second Additional Protocol to the Convention on Cybercrime on enhanced co-operation and disclosure of electronic evidence [2022] CETS No. 224.

[45] Currently 66 countries have ratified the Cybercrime Convention, two countries have signed the Cybercrime Convention; ten have been invited to accede and more than 140 countries are working with the Council of Europe to reinforce their legislation and capacity to address cybercrime. See <https://search.coe.int/directorate_of_communications/Pages/result_details.aspx?ObjectId=0900001680a48ca6>.

[46] <https://www.consilium.europa.eu/en/press/press-releases/2022/04/05/access-to-e-evidence-council-authorises-member-states-to-sign-international-agreement/>.

[47] See: <https://www.coe.int/en/web/conventions/full-list?module=signatures-by-treaty&treatynum=224>, last checked 10 February 2023. The Council (of the European Union) has authorized EU Member States to ratify the Protocol. Signatories so far includes some, but not all, EU Member States and the USA. Ireland and Denmark, the Member States who have opted out of the EIO Directive, have not yet signed the Protocol.

[48] Article 2 (1) Second Additional Protocol. See also the Explanatory Report to the Second Additional Protocol to the Convention on Cybercrime on enhanced co-operation and disclosure of electronic evidence, Strasbourg, 12.V.2022, available at <https://rm.coe.int/1680a49c9d> for more on application and scope of the Protocol.

CSA as a use case. Developments in the field of AI are rapidly ongoing and has also been addressed in the LLs, reason for which to include this relevant area of regulation in this section.

3.5.1 CSAM

In our increasingly digital world, online Child Sexual Abuse Material (CSAM) continues to increase. The COVID-19 pandemic has contributed to the increase in occurrence of CSA online. With children spending more time online, their vulnerability to the online forms of sexual abuse has consequently increased. As follows from the Interpol's report on Threats and Trends Child Sexual Exploitation and Abuse COVID-19 Impact, both the amount of CSAM as well as the illegal consumption thereof has increased, making online CSA an increasing concern for LEAs. At the same time, the resources of LEAs across Europe have been significantly impacted by the COVID-19 pandemic.[49] Especially in the area of cross-border cooperation, the long delays for MLA processes continue to be the main challenge for LEAs in view of the volatile nature of electronic evidence which is easily altered or deleted.[50] The amount of CSAM that has been created or that is in circulation online cannot be quantified in absolute terms, because new content is constantly being added and only a proportion of older content has been identified and taken down. These emerging threats call for a coordinated legislative response which is effective and compliant with the developments in the areas of privacy, data protection and human rights online.

LEAs, national authorities, safer internet hotlines or reporting mechanisms and service providers or industry all work together in the fight against CSAM. Industry has been called upon to take down CSAM materials from their services. Over the last decade, industry has set up reporting mechanisms for materials to be taken down once notified and adopted more automated systems to detect and take down CSAM. Microsoft for example developed 'PhotoDNA', software that creates a unique digital signature of an image (a hash) which can then be compared against the database of other hashes in order to identify illegal content. The main database of hashes of CSAM is held by the National Center for Missing and Exploited Children (NCMEC), a USA based non-profit organisation. PhotoDNA detects, disrupts and reports CSA and is freely available. Apart from images, Microsoft also developed a grooming detection technology, which scans chat conversations for potentially problematic conversations. Other service providers have also shown similar initiatives. While these technologies were not developed to assist LEAs *per se*, it is sometimes used to report a CSA case. These voluntary practices of detecting, reporting and removing CSAM have however come into a new light by recent legal developments.

The 2002 e-Privacy Directive[51] regulates confidentiality of communications and the rules regarding tracking and monitoring online. With the entry into force of the General Data Protection Regulation (GDPR), the e-Privacy Directive required updating and is likely to be replaced by the e-Privacy Regulation[52] proposed in 2017.[53] A year later, the EU Electronic Communications Code (EECC)[54], a new Directive which reforms the framework for the regulation of electronic communications services and networks, was introduced. With the entry into force of the EECC, the definition of 'electronic communications service' changed and now includes the so-called 'number-independent interpersonal communications services' (NI-ICS), i.e. services using numbers as a mere identifier,

[49] Interpol, 'Threats and Trends Child Sexual Exploitation and Abuse COVID-19 Impact' (2020), available at <https://www.interpol.int/en/content/download/15611/file/COVID19%20-%20Child%20Sexual%20Exploitation%20and%20Abuse%20threats%20and%20trends.pdf>.

[50] SIRIUS, 'SIRIUS EU Digital Evidence Situation Report' (2021) p. 15.

[51] Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications) [2002] OJ L 201/37.

[52] Proposal for a Regulation of the European Parliament and of the Council concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications) COM (2017) 010 final.

[53] The e-Privacy Regulation is meant to update the current rules on cookies, data retention, e-marketing and telecom privacy. In particular data retention is a problematic issue.

[54] Directive (EU) 2018/1972 of the European Parliament and of the Council of 11 December 2018 establishing the European Electronic Communications Code [2018] OJ L 321/36.

such as instant messaging. As of the entry into force of the EECC, this definition will also be applied to the e-Privacy Directive. As a result of this NI-ICS providers will be legally required to be in compliance with the e-Privacy Directive, which will interfere with the voluntary anti-CSAM activities. To 'fix' this, the Commission proposed a Regulation[55] for the temporary derogation, valid until 2024, from certain provisions of e-Privacy Directive as regards the use of technologies by NI-ICS for the processing of personal and other data for the purpose of combatting CSA online, in line with the 2020 EU strategy for a more effective fight against CSA.

Regulation (EU) 2021/1232 provides for a temporary regulatory framework which allows voluntary monitoring of communication by derogation from Article 5 (1) (confidentiality of communication) and Article 6 (1) (traffic data) of the e-Privacy Directive. This derogation thus allows service providers to continue their monitoring practices on a voluntary basis, by using technologies which detect CSAM. Such voluntary activities are an important means in reducing the spread of CSAM online, and a valuable tool in the detection, identification, prevention, investigation, and prosecution of CSA offences.[56] However, these activities also entail some degree of interference with a number of fundamental rights of service users. This quick 'fix' by the Commission has thus been the subject of scrutiny by the European Parliament.[57] Following lengthy debates, the European Parliament and the Council compromised and found a political agreement with a more narrow scope for a temporary and strictly limited derogation.[58] Following the compromise, the Regulation entered into force and sets out the framework as regards the scope and conditions for exercising voluntary activities by service providers in order to ensure that the voluntary practices do not affect fundamental rights, such as the rights to privacy and family life, data protection, beyond what would be considered a necessary limitation under article 52 (1) of the Charter for the purposes of investigating crime and CSA.

As follows from paragraph 10 of the Regulation's recitals, with regards to the scope of the Regulation, it

> "*does not provide for a legal ground for the processing of personal data by providers for the sole purpose of detecting online child sexual abuse on their services and reporting it and removing online child sexual abuse material from their services, but it provides for a derogation from certain provisions of Directive 2002/58/EC*",

and lays down "*additional safeguards which are to be respected by providers if they wish to rely on it*". Voluntary activities within the framework of the Regulation are furthermore subject to the safeguards as set out in GDPR and the Regulation specifies that the technologies used for voluntary activities should be the least privacy intrusive in accordance with the state of art, and ensure as much accuracy and reliability as possible in order to reduce the number of false positives to a maximum extent possible. As regards grooming detection technologies which scans chat conversations for potentially problematic conversations, the Regulation determines that the technologies used should

> "*not be used to systematically filter and scan text in communications unless it is solely to detect patterns which point to possible concrete reasons for suspecting online child sexual abuse, and they should not be able to deduce the substance of the content of the communications*".[59]

[55] Regulation (EU) 2021/1232 of the European Parliament and of the Council of 14 July 2021 on a temporary derogation from certain provisions of Directive 2002/58/EC as regards the use of technologies by providers of number-independent interpersonal communications services for the processing of personal and other data for the purpose of combating online child sexual abuse [2021] OJ L 274, p. 41.
[56] Ibid p. 42.
[57] <https://www.europarl.europa.eu/RegData/etudes/STUD/2021/662598/EPRS_STU(2021)662598_EN.pdf>.
[58] See <https://www.europa-nu.nl/id/vliec7g9hxzh/nieuws/fighting_sexual_abuse_of_children?ctx=vim2bx14ecsu&s0e=vifdkm1d06kk>.
[59] Regulation (EU) 2021/1232 of the European Parliament and of the Council of 14 July 2021 on a temporary derogation from certain provisions of Directive 2002/58/EC as regards the use of technologies by providers of number-independent interpersonal communications services for the processing of personal and other data for the purpose of combating online child sexual abuse [2021] OJ L 274, Art. 3 and paras. 16 and 18.

The Regulation furthermore establishes certain duties on the service providers, such as the duty to ensure human oversight[60], and rules pertaining to storing of data gathered in the course of suspected CSAM gathering[61].

Regulation 2021/1232 is temporary in nature and will be applicable until the 3 August 2024 (Article 10). The status of the e-Privacy Regulation is, to date, undecided following political disagreement[62], meaning that the e-Privacy Regulation will not be able to provide an answer in the near future. In May 2022 the Commission proposed a Regulation to regulate CSAM.[63] This CSAM Regulation will help rescue children from further abuse, prevent material from reappearing online and bring offenders to justice by obliging service providers to do a mandatory risk assessment to assess the risk that their services are misused for CSAM and/or grooming and putting in place risk mitigation measures if necessary. Member States will need to designate national authorities for reviewing the risk assessments. In case of a significant risk, a detection order will be issues to the service provider, obliging them to detect CSAM and grooming by targeting specific type of content on a specific service with strong safeguards put in place. If CSAM is detected, the service provider will have reporting obligations and the CSAM will need to be effectively removed. A new EU centre, similar to NCMEC will be put in place which will verify reports of potential online CSA made by providers before sharing them with LEAs and Europol. In their joint opinion, the EDPB and the EDPS raise their concerns regarding the necessity and proportionality of the interferences and limitation to the protection of fundamental rights considering that the measures could potentially significantly impact all users of interpersonal communications services and that it is questionable whether the proposed measures are genuinely effective and the least harmful to fundamental rights at stake.[64] The legislative procedure for this new CSAM Regulation is still ongoing[65] and being heavily debated between the EU legislators[66]. Unfortunately, the outcome of how CSAM will be regulated after 3 August 2024 remains unclear within the lifetime of the INSPECTr project.

3.5.2 AI

AI is the simulation of human intelligence processes by machines and is a technology which is rapidly gaining interest, for example due to the impact it may have, for example on education. Programmes like ChatGPT have sparked controversy as they have the ability to write entire papers. These 'machine learning' technologies may seem innocent, however, they have the capacity to also be used for crimes such as deepfakes, cyberattacks and disruption of systems by using AI. As AI per definition is a digital technology, it may impact digital evidence regulation and approach. It is therefore relevant to briefly discuss the legal development in the field to keep in mind when developing an INSPECTr platform for gathering, analysing, prioritising and presenting key data in criminal investigations.

In April 2021 the Commission proposed a Regulation[67] for harmonised rules as regards AI, known as the AI Act which aims to regulate the high-risk use of AI. The AI Act is applicable to a number of different actors (such as service providers, AI users, importers and distributors of AI systems) and lays down rules on a number of key

[60] Ibid, Art. 3(g).
[61] Ibid, Art. 3(h).
[62] Member States do not want far-reaching restrictions on requiring telecom companies to retain telecoms metadata for law enforcement purpose while the EU Parliament wants more protection of privacy and data protection.
[63] Proposal for a Regulation of the European Parliament and of the Council laying down rules to prevent and combat child sexual abuse, COM/2022/209 final.
[64] EDPB-EDPS Joint Opinion 4/2022 on the Proposal for a Regulation of the European Parliament and of the Council laying down rules to prevent and combat child sexual abuse, 28 July 2022, available at <https://edps.europa.eu/system/files/2022-07/22-07-28_edpb-edps-joint-opinion-csam_en.pdf>.
[65] <https://eur-lex.europa.eu/legal-content/EN/HIS/?uri=COM:2022:209:FIN>.
[66] See for example the European Parliament's Initial Appraisal of a European Commission Impact Assessment, available at <https://www.europarl.europa.eu/RegData/etudes/BRIE/2022/734703/EPRS_BRIE_APIN_734703_CSA-final.pdf>.
[67] Proposal for a Regulation of the European Parliament and of the Council laying down harmonised rules on Artificial Intelligence (Artificial Intelligence Act) and amending certain union legislative acts, COM/2021/206 final.

issues regarding AI. It established the rules relating to the placing of the AI systems on the market, as well as putting them into service and use in the EU[68]. It also lists certain prohibited AI practices, as well as issues specific requirements for AI systems classified as 'high-risk' and operators of such systems.[69] It furthermore harmonises certain transparency rules[70], rules on market monitoring and market surveillance[71], as well as measures in support of innovation[72]. The proposal introduces the concept of high-risk AI systems, meaning AI systems in predefined areas (Annex 3) that can be classified as high risk if they pose a high risk of harm to the health and safety or the fundamental rights of persons.[73] High-risk systems include for example AI systems in the area of biometric identification, critical infrastructures and law enforcement. The high-risk systems and their use are subject to a number of regulatory provisions and obligations in Chapter 2 of the AI Act. Such obligations include for example, the implementation of a suitable risk management system[74], and certain data and data governance principles[75]. High-risk AI systems used for specific purposes, inter alia law enforcement, are exempted from complying with a number of requirements mentioned in the AI Act, such as the registration obligation under Article 51, testing of high-risk AI systems in real world conditions outside AI regulatory sandboxes[76], as well as the conformity assessment procedure in some situations[77]. When it comes to the technology specific provisions of the Regulation, considering the high-risk systems, the proposal, lays down more specific rules as regards the use of 'real time' remote biometric identification systems, in accordance with the legislation currently in force, such as the GDPR and the Law Enforcement Directive. As a general rule, the proposal prohibits the use of 'real-time' remote biometric identification systems in publicly accessible spaces by law enforcement authorities or on their behalf unless strictly necessary for some of the reasons mentioned in Article 5 (1, d, i - iii).[78]

In December 2022, the Council adopted its common position on the AI Act.[79] At the time of writing this deliverable, the AI Act is at the stage of first reading by the European Parliament[80], meaning that it is still being debated in the European Parliament and that the plenary vote is expected in March 2023. Following that vote, the draft will be part of the trilogue discussions. Depending on how smooth the discussions will progress, the AI Act is likely to be adopted within the course of 2023. In January 2023 Euractiv reported that a new compromise amendments were circulated to finalise the classification of high-risk AI systems[81] and that the EU and the USA are also starting formal cooperation on AI[82]. Unfortunately, the outcome of how AI will exactly be regulated remains unclear within the lifetime of the INSPECTr project.

[68] Ibid, Art. 1(a).
[69] Ibid, Art. 1(b)-1(c).
[70] Ibid, Art. 1(c).
[71] Ibid, Art. 1(d).
[72] Ibid.
[73] Ibid, para. 32.
[74] Ibid, Art. 9.
[75] Ibid, Art. 10.
[76] Ibid, Art. 54(a).
[77] Ibid, Art. 47.
[78] Ibid, Art. 5.
[79] See: <https://www.consilium.europa.eu/en/press/press-releases/2022/12/06/artificial-intelligence-act-council-calls-for-promoting-safe-ai-that-respects-fundamental-rights/> and <https://www.rijksoverheid.nl/actueel/nieuws/2022/12/07/eu-akkoord-over-sterke-goedwerkende-markt-voor-kunstmatige-intelligentie>.
[80] See: <https://eur-lex.europa.eu/legal-content/EN/HIS/?uri=celex:52021PC0206>, last checked 30 January 2023.
[81] <https://www.euractiv.com/section/artificial-intelligence/news/ai-act-co-rapporteurs-seek-closing-high-risk-classification-sandboxes/>.
[82] <https://www.euractiv.com/section/artificial-intelligence/news/eu-us-step-up-ai-cooperation-amid-policy-crunchtime/>.

3.5.3 Digital Services Act

In 2022, the EU adopted the Digital Services Act[83] (DSA) which aims at creating a safer digital space, which includes protection of fundamental rights of users. With the emerging and increasing role of the digital sphere, some elements of older EU legislation, such as the 2000 E-Commerce Directive, had become outdated and in need of revision in order to effectively tackle some of the new emerging challenges around online platforms and intermediaries.[84] Digital sphere users are exposed to online risks which seriously prejudice their rights and interests under EU law. With the largely uncoordinated and fragmented responses on the side of the online platforms, the need for harmonisation became even more pressing. The DSA thus aims to harmonise those responses and provide a framework for addressing the cross-border digital space threats by conferring responsibilities on two main groups: online intermediaries and platforms, which represent a variety of actors, such as social networks (Ops, VLOPs), hosting services, ISPs, and online marketplaces.

The DSA also establishes a number of rules as regards the exchange of information between providers of hosting services and LEAs or judicial authorities. This includes orders to act against illegal content, orders to provide information and the notification of suspicions of criminal offences. The suspicion of criminal offences obliges providers of hosting services to inform LEAs or judicial authorities if it becomes aware of any information giving rise to a suspicion that a criminal offence involving the threat to the life or safety of a person(s) has taken place, is taking place or is likely to take place.[85] The DSA does however not provide for a legal basis for profiling the recipients of platform's services for this purpose. The platforms are under the duty to respect the fundamental rights and freedoms of individuals when informing the relevant LEAs on certain activities of the recipient of the service.[86]

Cross-border enforcement of the DSA is coordinated by the relevant Digital Services Coordinator (DSC), an authority designated by a Member State that is responsible for the application and enforcement of the DSA.[87] For the purpose of maintaining the efficiency of cross-border communication, the DSCs of Member States need to cooperate with each other and other national competent authorities. Interestingly, the request for initiation of the cross-border enforcement in one Member State may also be submitted by a DSC or the Board for Digital Services, an independent advisory group of DSCs,[88] from another Member States, which is an important instrument in facilitating the efficiency of cross-border investigations.[89]

[83] Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market For Digital Services and amending Directive 2000/31/EC (Digital Services Act) [2022] OJ L 277, p. 1.
[84] Executive Summary of the Impact Assessment Report Accompanying the document Proposal for a Regulation of the European Parliament and of the Council SWD(2020) 349 on a Single Market For Digital Services (Digital Services Act) and amending Directive 2000/31/EC
[85] Art. 18 DSA.
[86] Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market For Digital Services and amending Directive 2000/31/EC (Digital Services Act) [2022] OJ L 277, para 48, Art. 21.
[87] Ibid, Art. 38.
[88] Ibid, Art. 47.
[89] Ibid, Art. 45.

Conclusions

This Deliverable provides a reference framework from a legal perspective to be implemented in the INSPECTr platform, which will facilitate standard solutions for forensic investigations across LEAs within the EU. This legal analysis is highly important considering that LEAs are regulated and constrained by law in their activities. This report reflects the current legal status quo as it stands at the end of the INSPECTr project. When the INSPECTr platform will be eventually implemented, the legal framework will need to be re-assessed in order to include the latest updates at that point in time considering the rapid developments in the field.

In this Deliverable, the legal requirements for law enforcement powers and evidence requirements as discussed in D2.1 were updated by re-assessing the relevant legal instruments on an international and European level and the updates that have taken place since submitting D2.1. One of the most important conclusions as seen in D2.1 is that there is a lot of fragmentation in the area of law relating to law enforcement powers and evidence requirements. This fragmentation is caused by the fact that criminal law is based on the national laws and traditions of the Member States considering that the competence to legislate in the field of criminal matters was traditionally left to the Member States. The EU does however have the power to harmonise some aspects of criminal procedural laws and to facilitate cooperation among states falls within the EU's competence. With this competence over the years came a patchwork of legislation slowly covering certain aspects of criminal procedural law. As such, quite a large number of (national and international) legal instruments and agreements are applicable to investigations, gathering evidence and, cross-border collaboration. These laws regulate what powers and restrictions LEAs have and how they interact with other agencies and parties on a national and on an international level. The applicable legal framework can be found in:

- national laws and traditions;
- bi/multilateral agreements;
- harmonised international and European law;
- international and European law.

The international and European legal framework consists of EU and Council of Europe legal instruments and consists of rules on cross-border gathering and transmission of evidence, mutual assistance and cooperation, security of network and information systems, cybercrime and data protection.

Since the submission of D2.1 mid-2021, there have been some legal developments which are relevant within the context of the INSPECTr project:

- As regards the EIO, the current leading legal instrument for exchange of digital evidence, the developments of the eEDES system are slowly progressing. The eEDES system will be used as the main platform for sending and receiving EIOs in the EU and eventually also likely for MLA requests. Once the system is fully implemented and used by all EU Member States for EIOs and MLAs, the system is likely to speed up procedures and to facilitate the process.
- The NIS2 Directive entered into force and obliges more entities and sectors to take cybersecurity risk management measures in order to increase the level of cybersecurity within the EU. CSIRTs are designated within the context of the NIS2 Directive and have a supporting role in investigations and work closely with LEAs considering that incidents can be the result of criminal activities.
- It can be cautiously said that e-evidence package is likely to be adopted in 2023 considering that it was confirmed that agreement has been reached between the legislators. The aim of the e-evidence package is to make the exchange of digital evidence easier and faster for police and judicial authorities by introducing the European Production Order and a European Preservation Order for digital evidence in criminal matters and by designating legal representatives. These additional tools for authorities will significantly speed up certain requests for cross-border evidence.
- Within a broader, international, context the Commission has been negotiating on behalf of the EU with the USA and in the Council of Europe considering that crimes do not stop at EU borders and digital evidence can be stored anywhere in the world. Negotiations on the EU-US agreement have not really

progressed but are likely to restart once the e-Evidence package will be adopted. Negotiations within the Council of Europe were more successful, the Second Additional Protocol to the Cybercrime Convention has been adopted and will enter into force once at least five countries ratify it. The Second Additional Protocol aims at more effective MLA, including for example direct cooperation with service providers in other jurisdictions which are parties to the Convention. It provides for a framework and safeguards for cross-border requests which include data protection requirements.

Apart from these developments which directly impact the way that digital evidence is exchanged across borders, there are many other legal developments within the field of technology law which are interesting within the context of the INSPECTr project:

- LEAs, national authorities, safer internet hotlines or reporting mechanisms and service providers or industry all work together in the fight against CSAM. Industry has been called upon to take down CSAM materials from their services and to report incidents to LEAs. These practices currently find their legal basis in a temporary Regulation, derogating from standing legislation while final CSAM legislation is being awaited. CSAM is a use case within the context of the INSPECTr project and online CSAM is per definition digital evidence. The outcome of these developments need to be taken into account when eventually implementing the INSPECTr platform.
- AI is a digital technology which may be used for certain crimes and can thus impact digital evidence regulation and approach. The proposed AI Act is aimed at harmonising rules as regards AI and will regulate the high-risk use of AI. The proposal at the time of writing this deliverable seems to be at its final stages within the legislative process and is expected to be adopted within the course of 2023.
- The DSA, which aims at creating a safer digital space, was adopted in 2022. The DSA establishes a number of rules as regards the exchange of information between online platforms and LEAs. Online platforms are obliged to inform competent LEAs or judicial authorities of suspicions that a service recipient is likely to commit a serious criminal offence involving a threat to life and safety of a person. The DSA is thus another way for LEAs to collaborate with service providers, facilitating the investigation of crimes.

Although the developments within the area are a great improvement to the gathering and sharing of digital evidence, in particular as regards speed and efficiency, the practical reality is that there are still challenges:

- Cross-border collection and exchange of digital evidence can still be a time-consuming procedure, which is challenging considering the volatile nature of digital evidence which is easily altered or deleted. While there is a certain level of harmonisation and digitisation in place, some authorities still rely on 'regular' post to send requests for evidence. Especially if it is not exactly clear to which competent authority the request needs to be sent it may take longer than necessary for a request to arrive at its correct destination.
- While there is increasingly more attention to setting common standards for gathering and exchange of digital evidence, there are still differences in national enforcement legislation and approach. Legal, cultural and language differences, nuances of local laws and customs and differences in LEA capacities can also challenge cross-border cooperation. A simple example of this is that some countries write elaborate explanations in their request for mutual assistance, while others write short explanations. For the authorities who write short explanations it is sometimes difficult to filter the elaborate explanations from their peers abroad.
- The eEDES system for the exchange of digital evidence that is being put in place by the Commission is promising, however, all Member States have different procedures and chains of command and currently all have their own systems in place. There is still a long way to go before uniform processing of evidence requests can take place.

The INSPECTr platform will allow an investigator to visualise and bookmark important evidential material, and export it to an investigative report by using various knowledge discovery techniques. This will allow for cross-correlation analysis with existing case data and improve knowledge discovery within a case, between separate

cases and between interjurisdictional investigations. The platform will need to be flexible enough to adhere to the applicable legal framework and developments thereof.

References

Legislation and treaties

Additional Protocol to the European Convention on Mutual Assistance in Criminal Matters [1978] ETS No. 099

Additional Protocol to the European Convention on Mutual Assistance in Criminal Matters [1978] ETS No. 099

Charter of Fundamental Rights of the European Union [2000] OJ C 364/01

Consolidated version of the Treaty on the Functioning of the European Union [2012] OJ C 326/47

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 [2000] OJ C 197/3

Convention for the Protection of Human Rights and Fundamental Freedoms [1950] ETS No. 005

Convention on Cybercrime [2001] ETS No. 185

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 [2000] OJ C 197/1

Council Decision 2007/533/JHA of 12 June 2007 on the establishment, operation and use of the second generation Schengen Information System (SIS II) [2007] OJ L 205/63

Council Framework Decision 2006/960/JHA of 18 December 2006 on simplifying the exchange of information and intelligence between law enforcement authorities of the Member States of the European Union [2006] OJ L 386/89

Council Framework Decision of 13 June 2002 on joint investigation teams [2002] OJ L162/1

Council Framework Decision of 13 June 2002 on the European arrest warrant and the surrender procedures between Member States (2002/584/JHA) [2002] OJ L 190/1

Council Framework Decision of 13 June 2002 on the European arrest warrant and the surrender procedures between Member States (2002/584/JHA) [2002] OJ L 190/1

Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union [2016] OJ L 194/1

Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA [2016] OJ L 119/89

Directive (EU) 2018/1972 of the European Parliament and of the Council of 11 December 2018 establishing the European Electronic Communications Code [2018] OJ L 321/36

Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications) [2002] OJ L 201/37

Directive 2013/40/EU of the European Parliament and of the Council of 12 August 2013 on attacks against information systems and replacing Council Framework Decision 2005/222/JHA [2013] OJ L 218

Directive 2014/41/EU of the European Parliament and of the Council of 3 April 2014 regarding the European Investigation Order in criminal matters [2014] OJ L131/1

Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 [2022] OJ L 333, p. 80

Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data [1995] OJ L 281/31

European Convention on Mutual Assistance in Criminal Matters [1959] ETS No. 030

Regulation (EC) No 1986/2006 of the European Parliament and of the Council of 20 December 2006 regarding access to the Second Generation Schengen Information System (SIS II) by the services in the Member States responsible for issuing vehicle registration certificates [2006] OJ L 381/1

Regulation (EC) no 1987/2006 of the European Parliament and of the Council of 20 December 2006 on the establishment, operation and use of the second generation Schengen Information System (SIS II) [2006] OJ L 381/4

Regulation (EC) No 460/2004 of the European Parliament and of the Council of 10 March 2004 establishing the European Network and Information Security Agency [2004] OJ L 77

Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) [2016] OJ L 119/1

Second Additional Protocol to the European Convention on Mutual Assistance in Criminal Matters [2001] ETS No. 182

Regulation (EU) 2021/1232 of the European Parliament and of the Council of 14 July 2021 on a temporary derogation from certain provisions of Directive 2002/58/EC as regards the use of technologies by providers of number-independent interpersonal communications services for the processing of personal and other data for the purpose of combating online child sexual abuse [2021] OJ L 274, p. 41

Regulation (EU) 2022/2554 of the European Parliament and of the Council of 14 December 2022 on digital operational resilience for the financial sector and amending Regulations (EC) No 1060/2009, (EU) No 648/2012, (EU) No 600/2014, (EU) No 909/2014 and (EU) 2016/1011 [2022] OJ L 333, p. 1

Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market For Digital Services and amending Directive 2000/31/EC (Digital Services Act) [2022] OJ L 277, p. 1

Regulation (EU) 2022/850 of the European Parliament and of the Council of 30 May 2022 on a computerised system for the cross-border electronic exchange of data in the area of judicial cooperation in civil and criminal matters (e-CODEX system), and amending Regulation (EU) 2018/1726 [2022] OJ L 150, p. 1

Second Additional Protocol to the Convention on Cybercrime on enhanced co-operation and disclosure of electronic evidence [2022] CETS No. 224

The Schengen acquis - Convention implementing the Schengen Agreement of 14 June 1985 between the Governments of the States of the Benelux Economic Union, the Federal Republic of Germany and the French Republic on the gradual abolition of checks at their common borders [2000] OJ L 239/19

Treaty of Lisbon amending the Treaty on European Union and the Treaty Establishing the European Community [2007] OJ C 306/01

Policy documents

Annex to the Recommendation for a Council decision authorising the opening of negotiations in view of an agreement between the European Union and the United States of America on cross-border access to electronic evidence for judicial cooperation in criminal matters

Commission Recommendation of 6 May 2003 concerning the definition of micro, small and medium-sized enterprises [2003] OJ L 124, p. 36

Council of the European Union, Brussels, 21 May 2019, 9114/19, available at <https://data.consilium.europa.eu/doc/document/ST-9114-2019-INIT/en/pdf>

Council of the European Union, Brussels, 21 May 2019, 9116/19, available at <https://data.consilium.europa.eu/doc/document/ST-9116-2019-INIT/en/pdf>

Council of the European Union, Interinstitutional File: 2018/0107(COD), Brussels 20 January 2023, 5449/23, available at <https://data.consilium.europa.eu/doc/document/ST-5449-2023-INIT/en/pdf>

Council of the European Union, Interinstitutional File: 2018/0108(COD), Brussels 20 January 2023, 5448/23, available at < https://data.consilium.europa.eu/doc/document/ST-5448-2023-INIT/en/pdf>

EDPB-EDPS Joint Opinion 4/2022 on the Proposal for a Regulation of the European Parliament and of the Council laying down rules to prevent and combat child sexual abuse, 28 July 2022, available at <https://edps.europa.eu/system/files/2022-07/22-07-28_edpb-edps-joint-opinion-csam_en.pdf>

EDPB-EDPS Joint Response to the LIBE Committee on the impact of the US Cloud Act on the European legal framework for personal data protection (annex), available at <https://edpb.europa.eu/sites/default/files/files/file2/edpb_edps_joint_response_us_cloudact_annex.pdf>

European Data Protection Supervisor, Opinion 2/2019, EDPS Opinion on the negotiating mandate of an EU-US agreement on cross-border access to electronic evidence, 2 April 2019

Explanatory Report to the Second Additional Protocol to the Convention on Cybercrime on enhanced co-operation and disclosure of electronic evidence, Strasbourg, 12.V.2022, available at <https://rm.coe.int/1680a49c9d>

European Parliament's Initial Appraisal of a European Commission Impact Assessment, available at <https://www.europarl.europa.eu/RegData/etudes/BRIE/2022/734703/EPRS_BRIE_APIN_734703_CSA-final.pdf>

Joint communication to the European Parliament, the Council, the European Economic and Social Committee and the Committee of Regions Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace [2013] JOIN(2013) 1 final

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, COM (2018) 226 final

Proposal for a Regulation of the European Parliament and of the Council laying down harmonised rules on Artificial Intelligence (Artificial Intelligence Act) and amending certain union legislative acts, COM/2021/206 final

Proposal for a Regulation of the European Parliament and of the Council laying down rules to prevent and combat child sexual abuse, COM/2022/209 final

Proposal for a Directive of the European Parliament and of the Council on measures for a high common level of cybersecurity across the Union, repealing Directive (EU) 2016/1148, COM(2020) 823 final

Proposal for a Regulation of the European Parliament and of the Council on European Production and Preservation Orders for electronic evidence in criminal matters, COM(2018) 225 final

Proposal for a Regulation of the European Parliament and of the Council concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications) COM (2017) 010 final

Recommendation for a Council Decision authorising the opening of negotiations in view of an agreement between the European Union and the United States of America on cross-border access to electronic evidence for judicial cooperation in criminal matters, COM(2019) 70 final

Recommendation for a Council Decision authorising the participation in negotiations on a second Additional Protocol to the Council of Europe Convention on Cybercrime (CETS No. 185), COM(2019) 71 final

Summary of the Opinion of the European Data Protection Supervisor on the negotiating mandate of an EU-US agreement on cross-border access to electronic evidence [2019] OJ C 186, p. 17

Guidelines

Council of Europe Data Protection and Cybercrime Division, Electronic Evidence Guide A basic guide for police officers, prosecutors and judges version 2.1 [2020]

ENISA, *Electronic evidence - a basic guide for First Responders, Good practice material for CERT first responders* [2014], available at <https://www.enisa.europa.eu/publications/electronic-evidence-a-basic-guide-for-first-responders>.

ENISA, *Identification and handling of electronic evidence – Handbook, document for teachers* [2013] September 2013, available at <https://www.enisa.europa.eu/topics/trainings-for-cybersecurity-specialists/online-training-material/documents/identification-and-handling-of-electronic-evidence-handbook/view>.

European Data Protection Supervisor, Opinion 07/2019, EDPS Opinion on Proposals regarding European Production and Preservation Orders for electronic evidence in criminal matters, 6 November 2019, available at <https://edps.europa.eu/sites/default/files/publication/19-11-06_opinion_on_e_evidence_proposals_en.pdf>

Literature and other sources

A. McQuinn and D. Castro, 'How law enforcement should access data across borders', *Information Technology & Innovation Foundation*, July 2017

A. Tinoco-Pastrana, The Proposal on Electronic Evidence in the European Union, EUCRIM 1/2020, p.46

Chalmers, D., Davies, G., Monti, G., *European Union Law*, Cambridge: University Press, 2010

D.J.B. Svantesson and L. van Zwieten, 'Law enforcement access to evidence via direct contact with cloud providers – identifying the contours of a solution', *Computer law & Security Review* 32 (2016)

D.J.B. Svantesson, 'Law enforcement cross-border access to data', *Preliminary Report* November 2016

J.A. Espina Ramos, *The European Investigation order and its relationship with other judicial cooperation instruments*, EUCrim 1/2019

ENISA, Cooperation between CSIRTs and Law enforcement: interaction with the Judiciary [2018], available at <https://www.enisa.europa.eu/publications/csirts-le-cooperation>

Websites (news articles, press releases, legislative procedure)

https://treio.eu

https://ec.europa.eu/commission/presscorner/detail/en/ip_22_2985

https://www.ebu.ch/files/live/sites/ebu/files/News/Position_Papers/open/2021_05_18_EevidenceJointLetter_18May2021.pdf

https://www.fairtrials.org/app/uploads/2022/02/E-evidence-position-paper-February-2019.pdf

https://www.europarl.europa.eu/doceo/document/A-9-2020-0256_EN.html#title3

https://www.europarl.europa.eu/doceo/document/LIBE-AM-644870_EN.pdf

https://www.statewatch.org/news/2022/july/eu-end-game-approaching-for-e-evidence-negotiations-says-french-presidency/

https://www.consilium.europa.eu/en/press/press-releases/2023/01/25/electronic-evidence-council-confirms-agreement-with-the-european-parliament-on-new-rules-to-improve-cross-border-access-to-e-evidence/

https://data.consilium.europa.eu/doc/document/ST-9666-2019-INIT/en/pdf

https://data.consilium.europa.eu/doc/document/ST-9664-2019-INIT/en/pdf

https://www.ncsc.nl/actueel/weblog/weblog/2022/de-werking-van-de-cloud-act-bij-dataopslag-in-europa

https://www.lawfareblog.com/has-time-eu-us-agreement-e-evidence-come-and-gone

https://ec.europa.eu/commission/presscorner/detail/en/STATEMENT_22_7784

https://search.coe.int/directorate_of_communications/Pages/result_details.aspx?ObjectId=0900001680a48ca6

https://www.consilium.europa.eu/en/press/press-releases/2022/04/05/access-to-e-evidence-council-authorises-member-states-to-sign-international-agreement/

https://www.coe.int/en/web/conventions/full-list?module=signatures-by-treaty&treatynum=224

https://www.europarl.europa.eu/RegData/etudes/STUD/2021/662598/EPRS_STU(2021)662598_EN.pdf

https://www.europanu.nl/id/vliec7g9hxzh/nieuws/fighting_sexual_abuse_of_children?ctx=vim2bx14ecsu&s0e=vifdkm1d06kk https://www.consilium.europa.eu/en/press/press-releases/2022/12/06/artificial-intelligence-act-council-calls-for-promoting-safe-ai-that-respects-fundamental-rights/

https://www.rijksoverheid.nl/actueel/nieuws/2022/12/07/eu-akkoord-over-sterke-goedwerkende-markt-voor-kunstmatige-intelligentie

https://eur-lex.europa.eu/legal-content/EN/HIS/?uri=celex:52021PC0206

https://www.euractiv.com/section/artificial-intelligence/news/ai-act-co-rapporteurs-seek-closing-high-risk-classification-sandboxes/

https://www.euractiv.com/section/artificial-intelligence/news/eu-us-step-up-ai-cooperation-amid-policy-crunchtime/

https://eur-lex.europa.eu/legal-content/EN/HIS/?uri=COM:2022:209:FIN