Kyriaki Dionysopoulou

Considerations of fundamental rights and lawyers' ethics regarding digitalization

Training of Lawyers in various areas of EU law 2 **#TRAVAR2**

Co-funded by the EU

Digitalisation as an EU Priority

- **European Declaration on Digital Rights and Principles 2022**
  - A Human-Centric Digital Transition
  - EU Charter of Fundamental Rights
  - The Rule of Law
- **Digitalisation Regulation 2023/2844**
  - Interoperability of justice systems
  - Access to Justice
- **Digitalisation Directive 2023/2843**
- **e-CODEX Regulation**

Digitalisation of Judicial Cooperation in the EU

Key EU Legislative Instruments

Regulation (EU) 2023/2844

- Establishes the core legal framework for the digitalisation of judicial cooperation
- Introduces:
  - electronic communication channels
  - digital exchange of documents
  - videoconferencing tools
- Applies directly in all EU Member States

Directive (EU) 2023/2843

Complements the Regulation

Aligns existing instruments of judicial cooperation in criminal matters with the new digital framework

Requires transposition into national law by Member States

Digitalisation in Criminal Law: Setting the Scene

Digitalisation Regulation 2023/2844

- "Digital by Default" Principle

Strategic EU Goal:

- Fully functional area of freedom, security and justice
- Equal Digital Capacity within the EU
- Access to justice
- The Regulation recognises the importance of reducing existing disparities in the digitalisation of judicial systems across Member States

Digitalisation in Criminal Law: Setting the Scene

Key Priorities

- Harmonised digital development
- Equal access to technological infrastructure
- Effective use interoperability between national systems
- Digitalisation of Judicial Cooperation and Fundamental Rights Safeguards
- Facilitation of cross-border judicial proceedings through digital tools and technologies
- Efficiency, accessibility and interoperability of justice systems
- Safeguarding EU values, rule of law and fundamental rights

Central Principle

- Digital transformation must be inclusive and coherent throughout the European judicial area

Safeguarding EU Values and the Rule of Law

Nevertheless, as criminal lawyers, we must bear in mind that every step towards digitalisation of judicial proceedings must:

- serve and protect the values and acquis of the European Union,
- strengthen mutual trust among Member States,
- uphold the rule of law,
- preserve fundamental procedural rights.
- Essential Safeguards

Digital justice must always remain:

- human-centric,
- transparent,
- fair,
- accountable,
- respectful of fundamental rights.

Fundamental Rights in Criminal Proceedings: a Cornerstone of the rule of law

New Challenges

At the same time, digitalisation raises important concerns regarding:

- procedural safeguards,
- cybersecurity,
- protection of personal data,
- equal access to technology,
- preservation of fair trial guarantees
- Right to privacy
- Freedom of expression and access to information
- Right to a fair trial and access to justice
- Equality and non-discrimination in digital systems

Security, Legal Aid and Access to Justice

Protection of Sensitive Data

- Competent authorities handle sensitive information in cross-border proceedings.
- Therefore:
- security of communication systems must be ensured,
- reliability and integrity of data exchange are essential,
- confidentiality must be protected at all stages.

Legal Aid and Legal Assistance

- The right to:
- legal aid,
- effective access to justice

Access to Information

- Natural and legal persons should be able to:
    - access relevant legal information,
    - use the e-Justice Portal,
    - benefit from simplified digital access mechanisms.

Videoconference and Fundamental Rights: Procedural Safeguards

Safeguards in Remote Hearings - Requirements of the Regulation

Videoconferencing or other distance communication technology must:

- allow verification of the identity of participants,
- ensure visual, audio and oral communication,
- enable effective participation during the hearing.

Important Clarification

- A mere telephone call **is not considered sufficient** for oral hearings.

Videoconference and Fundamental Rights: Fair Trial Concerns

Fundamental Rights Concerns – The technology used must comply with:

- personal data protection standards,
- confidentiality of communications,
- data security requirements.

Why This Matters

Remote hearings directly affect:

- the right to a fair trial,
- effective participation of the accused,
- defence rights,
- credibility
- equality of arms.

Videoconference and Fundamental Rights

Fundamental Rights Perspective:

✓ The criminal procedure preserves its **directness** and **immediacy**

✓ Physical judicial presence remains central in core adjudication

Key Safeguard:

✓ Protection of the right to fair trial

✓ Effective judicial immediacy

✓ Proper assessment of evidence and credibility

✓ Respect for defence rights

Videoconference and Fundamental Rights: Consent and Participation

Fundamental Guarantee

General Rule

- Use of videoconferencing requires **consent** of:
  - suspect
  - accused or convicted person
  - affected persons (Regulation (EU) 2018/1805)

Exceptional Derogation

Consent may be bypassed only if:

- there are **serious threats to public security or public health**
- threats are **genuine, present, or foreseeable**
- the derogation is **strictly necessary**

Effective Remedy in Remote Hearings

Right to an Effective Remedy (Article 47 Charter)

- Applies where rights are violated during videoconferencing or other remote hearings
- Ensures access to judicial protection in the digital justice context

Core Guarantee

•Right to challenge procedural violations
•Right to seek judicial review before a competent authority
•Full compliance with the Charter of Fundamental Rights

Key Principle

Digitalisation of justice must strengthen, not limit, access to effective judicial protection and the right to a fair trial.

Confidentiality of Lawyer–Client Communication

Obligation of Competent Authorities
•Ensure full confidentiality of communication
•Apply relevant national law in line with EU standards

Key Purpose
•Protect the right of defence
•Preserve legal professional privilege
•Guarantee effective and fair participation in proceedings

Fundamental Principle
Remote justice must not compromise the confidential relationship between lawyer and client

Core Procedural Rights Explicitly Protected

Key Rights Guaranteed

- Right to interpretation (Directive 2010/64/EU)
- Right of access to a lawyer (Directive 2013/48/EU)
- Right to information and case file access (Directive 2012/13/EU)
- Presumption of innocence (Directive (EU) 2016/343)
- Special safeguards for children (Directive (EU) 2016/800)
- Right to legal aid (Directive (EU) 2016/1919)
- Right to be present at trial

Legal Framework

- EU Charter of Fundamental Rights
- EU Procedural Rights Directives

Core Message

- Digital justice must operate within a **fully rights-based system**, where competent authorities actively guarantee and protect defence rights in practice.

Lawyers' Ethics in the Context of Digitalisation

The Professional Role of Lawyers in Digital Justice

- Digitalisation of justice systems raises important questions regarding the ethical duties of lawyers, particularly in criminal proceedings where fundamental rights are at stake.

Core Ethical Dimension

- Lawyers remain guardians of:
  - the right to a fair trial
  - the rights of defence
  - equality of arms
  - procedural fairness

Digital tools must never weaken professional independence or confidentiality.

Fundamental Ethical Principles

Key Ethical Duties in the Digital Era

- Confidentiality
  - Protection of lawyer–client communications in digital environments
- Professional secrecy
  - Secure handling of electronic files and evidence
- Independence
  - No external interference through digital systems or platforms
- Competence
  - Adequate understanding of digital tools and procedures
- Diligence
  - Ensuring effective defence in remote and hybrid proceedings

Balancing Efficiency and Fundamental Rights

- Confidentiality and Professional Secrecy

Where does legal protection end when data are stored on third-party servers?

Key notes

- Protection of lawyer-client communications
- Risks linked to cloud services and online platforms
- Cybersecurity obligations for lawyers
- Ensuring national law
- Maintaining trust in digital legal services

Balancing Efficiency and Fundamental Rights

Ethical Tension in Practice?

- algorithmic tools & defence strategy
- remote hearings vs effective client consultation time
- unequal digital capacity between lawyers

➢ **Digitalisation in criminal justice reconfigures the procedural architecture of defence rights, requiring a reconceptualisation of both fair trial guarantees and the ethical duties of legal professionals**

Balancing Efficiency, Fundamental Rights and Ethics

Closing Remarks

- Digitalisation of EU justice is rooted in the ***acquis communautaire*** and the rule of law
- Guided by the ***principle of "Digital by Default"*** in judicial cooperation
- Must fully respect procedural safeguards and judicial independence
- Aim: a ***human-centred*** justice system where technology enhances fairness and access to justice

Alexis Anagnostakis

Videoconferencing in Greek criminal proceedings: Promise, practice and the protection gap

Training of Lawyers in various areas of EU law 2 **#TRAVAR2**

Co-funded by the EU

The First Remote Criminal Trial in Greece

January 2026 — Mixed Jury Court of Syros

Three witnesses testifying live from the Greek Embassy in Dublin.

Press cameras. Excitement. A palpable sense of history.

Then the link started.

The smiles froze.

The image froze.

" We sat in that courtroom watching a screen that told us nothing, and calling it evidence. "

— Alexis Anagnostakis

SECTION 2 — THE LEGAL FRAMEWORK: ARTICLE 238A CCP

What the Law Says

Article 238A formalises videoconferencing in criminal proceedings — a sixth chapter in Book II of the CCP titled 'Procedure by Video Teleconference.'

Physical attendance remains the default.

Videoconference is the exception.

Who Can Order It

The prosecutor or the court may order examination of witnesses and participants by videoconference where physical attendance is difficult or impossible.

A threshold must be met.

→ This is where the protection gap begins.

What Has Changed in Practice

Post-COVID, videoconferencing has become not the exception but the expectation.

For witnesses abroad, detained defendants, and logistically complex cases — the screen has replaced the courtroom.

SECTION 3 — THE PROTECTION GAP

Four Concrete Vulnerabilities

1. No Mandatory Notification to the Defendant
2. No Defence Counsel at the Remote End
3. Poor Technical Quality — and No Procedural Remedy
4. The Translation Compound Problem

1 Vulnerability 1 — The Defendant Is Not Notified

The Problem

Under current practice, when a court orders witness examination by videoconference, the defendant is not always specifically notified that this is how the hearing will proceed. There is no mandatory advance warning requiring the defendant to be told: ***'Your accuser will testify from a screen, not from this room.'***

Why It Matters

The right to prepare your defence is contingent on knowing what form the evidence will take. A cross-examination of a witness testifying via a shaky embassy connection requires different preparation — different tactics — than a live confrontation.

In Practice

If defence counsel learns only on the day of hearing that the prosecution's key witness will appear via videolink — there is no time to request a test connection, no prior review of technical arrangements.

2 Vulnerability 2 — No Lawyer at the Remote End

Article 238A does not require — and Greek courts do not systematically ensure — that defence counsel is present at the remote location where the witness testifies.

When the Syros witnesses testified from the Dublin Embassy, there was no defence lawyer in that room, no independent observer, no verification of the conditions under which the testimony was given.

Who ensures the witness is not being prompted?

Who guarantees confidentiality?

Who observes the demeanour that a jury has the right to assess?

ECtHR Standard

Effective participation via videoconference requires:

- Ability to follow proceedings
- Ability to be heard without technical obstacles
- Confidential communication with counsel
- Counsel presence at the remote location — flagged as 'of paramount importance'

3 Vulnerability 3 — Poor Technical Quality & No Remedy

The most insidious problem. When video quality is poor — pixelated witness, broken audio, inadequate translation — there is no effective procedural remedy within the current CCP framework.

You cannot stop the hearing. You cannot demand rescheduling merely because the connection is poor. **The decision to proceed or adjourn lies entirely with the presiding judge, and the standard is not defined.**

'Poor quality' is not a ground of nullity under Article 171 CCP. It does not trigger an absolute procedural defect.

⚠ The Syros Case

Three witnesses testified. Translation was inadequate. Defence counsel raised quality issues on the record. The court noted the objection and proceeded. The testimony was counted. The defendant was convicted.

There is no consistent doctrine on what level of technical failure constitutes a fair trial violation.

4 Vulnerability 4 — The Translation Compound Problem

The Compound Failure

When witnesses testify from abroad via videoconference, interpretation is done in real-time over the connection.

Poor audio quality degrades the already difficult task of simultaneous interpretation.

The interpreter hears an incomplete signal and translates an incomplete signal.

Article 233 CCP & Article 6(3)(e) ECHR

Article 233 CCP requires appointment of an interpreter when a witness does not adequately speak Greek.

But the article sets no minimum technical standards for remote interpretation:

- No dedicated interpretation channels
- No separate audio feed requirement

The result: the right to an interpreter, guaranteed by Article 6(3)(e) ECHR, is formally satisfied but substantively hollow.

“I’m sorry. *This was my fault.*”

He said nothing.

What I did

Did not check the file. Did not check the connection.

My instinct

Blame others. The prosecutor. The local lawyers.

The truth

He was asking about me. Not them.

That silence stayed with me longer than any argument I have ever lost.

Good lawyers should not have to be perfect to deliver a fair trial. That is what safeguards are for.

Article 6 ECHR — The Three-Part Test

Justified Case

Use of videoconference must be justified in the individual case — not a default convenience.

Legitimate Aim

The technology must serve a legitimate purpose: witness protection, distance, incapacity, or similar.

Effective Participation

The defendant must be able to follow proceedings, be heard, communicate confidentially with counsel, and have demeanour assessed.

The Deeper Constitutional Question

When the law creates a mechanism for videoconferencing but provides no minimum technical standard, no mandatory notification right, no right to counsel at the remote end, and no enforceable remedy for failure — is that mechanism compliant with Article 6?

SECTION 5 — CONCLUSION

What Justice Requires

Technology is not neutral in a criminal trial. Every choice about how a witness appears, how their words are transmitted, how their face is seen — or not seen — is a choice about evidence, about credibility, about the real possibility of injustice.

Article 238A has created a framework. But a framework without mandatory advance notification to the defendant, without a right to defence counsel at the remote location, and without an effective remedy when the technology fails —

That framework is not a guarantee of a fair trial. It is a performance of one.

What we need is not less videoconferencing.

What we need is videoconferencing done with the rigour that justice demands.

The first trial was historic. The frozen smiles were a warning. Five months later, we owe our clients better than that.

Christodoulos Derdemezis

E-Evidence procedures: Lessons from child abuse cases

Training of Lawyers in various areas of EU law 2 **#TRAVAR2**

Co-funded by the EU

The Modern Definition of CSA crimes – New forms of CSA crimes - Legal TOOLS

- **Eu Directive 2011/93**
- Child Pornography (article 2 of the Directive)
- Other cyber related crimes include Revenge Porn (the act of distributing sexual containing material without the consent of the party) + On line Child grooming (the proposal by means of information and communication technology by an adult to meet a child for the purpose of committing a sexual offence)
- **New challenges → Proposal of the Commission (6/2/2024)** on combatting child sexual abuse which covers also offences as **livestreaming of child sexual abuse** and **intentional access** and **dissemination of child sexual abuse deepfakes**
- **Convention on Cybercrime of the Council of Europe**
- **Resolution of the UN 79/243**
- **Interim regulation** adopted on the 14 July 2021 → until 3/4/2026 EXPIRED
- 11/5/2022 : **A proposal** on permanent rules from the Commission → obligation to the providers to detect, report and remove CSA material

The use of e – evidence in the “more conventional” CSA crimes

- **Crime recordings**
- **Communication** between the offender and the victim

❖Mobile phones : An ally when the perpetrator is someone close to home…

❖**Areios Pagos 2081/2018: Text messaging revealed that the offender knew that the rape victim was a minor**

- **Location data** → the scene of the crime
- **Areios Pagos 101/2021** : The disclosure of the encrypted code by the accused is not a mitigating factor at sentencing
- Could the voluntary disclosure of the password by the accused be considered a mitigating factor at sentencing?
- Regulation 2022/2065 of the European Parliament and of the Council

Investigating tools

- **Undercover investigation with a court order**
- **A concealed identity on the Internet**
- Open Sources Intelligence – Mom takes action! (Judicial Council of Athens 4533/2016)
- **Even a simple body search** → leads to another suspect (Judicial Council of Rhodes 39/2021)
- Deposition by means of electronic devises = Evidence only if combined with other evidences
- House searches
- Profiling of the suspect

Report on digital data on child pornography – usual questions

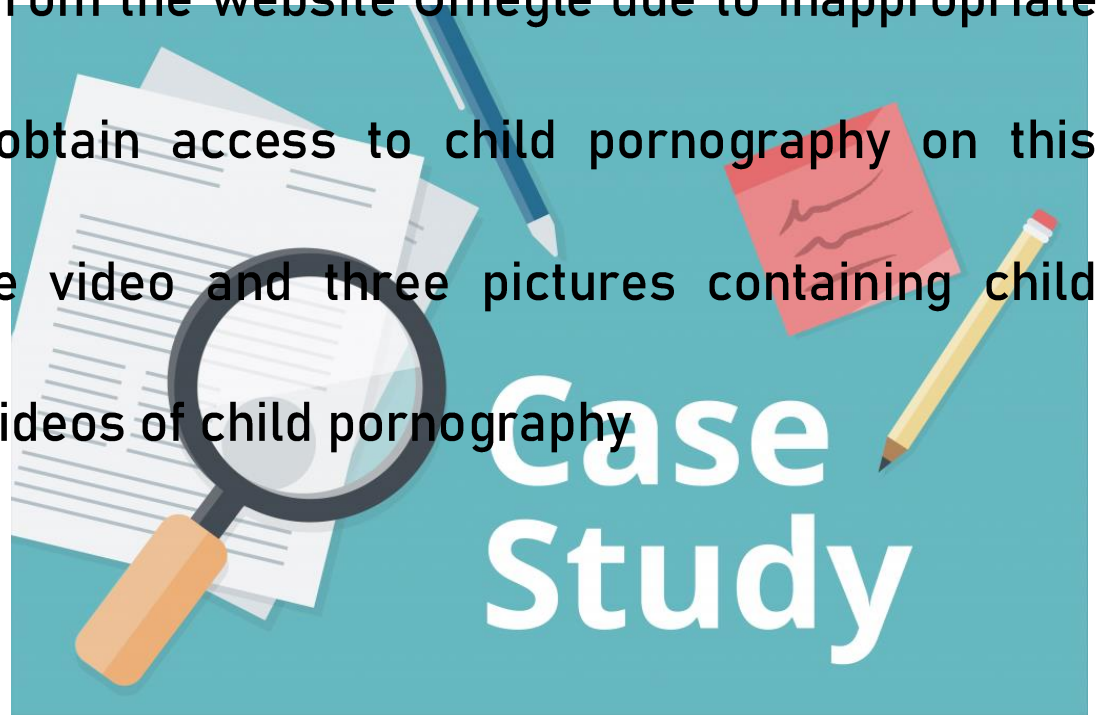
- Is there any child pornography material on the device?
- When was the material produced/downloaded?
- What is the percentage of child pornography compared with the one of adult pornography?
- How many times did the offender access the child pornography material?
- Where deleted files are retrieved, the date and time must be recorded
- Has the offender produced any child pornography material?
- Did the offender have access to websites containing such a material? Did the offender have accounts on these websites?
- Are there any p2p systems?
- Did the offender use any online applications such as Messenger, Chat and What's Up?
- Is there any child pornography material stored in the cloud?

Case law – importance of the investigation on e – evidence

- **The non bis in idem argument** : Prosecution for 150 pictures on 13/7/2016. Another Prosecution for 338 pictures The non bis in idem argument. **Judicial Council of the Court of Appeals of Thessaloniki 831/2019** = Different DATE, Different PICTURES, TWO devices = DIFFERECT ACT OF POSSESSION →
- **The case of the Military Academy :** LACK of proper report on the matter of confiscation + LACK of investigation on the hard drive = ACQUITAL
- **Court of Appeals of Dodecanisa 3/2019 :** Not a single file was found indicating there was a communication and/or file sharing between the accused and the victim. + The examination and analysis of the laptop revealed that the conversations didn't take place originally at the accused's laptop. The communication and multimedia files in question auto synced between the accused's laptop and another device + There was no digital evidence of sharing, obtaining and distributing child pornography = ACQUITAL

Case study

- A hard drive was confiscated.
- A visual check of the suspect's laptop showed that the program ManyCam was downloaded.
- IE history check: the suspect was banned from the website Omegle due to inappropriate behavior.
- However, on 16-3-2016 he was able to obtain access to child pornography on this website.
- On the file "Downloads", there were one video and three pictures containing child pornography material.
- The hard drive of the suspect contained 5 videos of child pornography



Claims of the accused

- Chat on Omegle with unknown users who sent him hyperlinks
- Not many files
- The files were downloaded automatically without his knowledge.
- Poor IT knowledge (Most common argument : WATCH OUT for the downloading of elaborated applications, access to the darkweb, use of keywords and symbols associated with content depicting child pornography)

❖**Areios Pagos 643/2020 : 1) Visible Files, 2)** The existence of other files essential to the accused' s profession in the same drive prove that he had knowledge of the child pornography material, **3) Encrypted Files**

❖**Court of Appeals of Piraeus :** No distribution + Deletion + no proof that he had opened the files + at the same time music files were downloaded → **ACQUITAL**

The Ruling

- Poor IT knowledge? It was a fact that he did install ManyCam and used it to watch a child pornography video.
- NOT many files? Still there are files containing CSA material
- Shift of burden of proof → It was he who had to prove that he lacked the knowledge to retrieve the pictures from the unallocated space
- He had access to DEEPWEB.
- He used signals and symbols associated with content depicting child pornography
- He visited OMEGLE many times until he was banned from the site.

Indictment of the accused before the **Mixed Jury Court of First Instance of Corinth**

- He was found guilty
- He was sentenced to 4 years of imprisonment
- The hard disc containing child pornography material was SEIZED

"I'd say Guilty, but, hey, who am I to judge?"

PICTURE 1

Good morning, ladies and gentlemen. Let me take this opportunity to welcome you to this beautiful city. My name is Christodoulos Derdemezis and I am a lawyer here in Athens.

First of all, I would like to thank the coordinators of the event for inviting me to speak to such an interesting seminar

In my years of serving as a lawyer I have come up with various crimes related to child sexual abuse cases and have come to realize the importance of e – evidence.

PICTURE 2

Eu Directive 2011/93 sets forth a thorough definition of offences concerning sexual abuse and sexual exploitation and includes in these definitions the act of causing a child to witness sexual activities or sexual abuse, engaging in sexual activities with a child and coercing, forcing or threatening a child into sexual activities with a third party.

Technology and especially the internet have created more forms of child sexual abuse. Among the latter, we have come to see the increasing prevalence of internet child pornography.

Article 2 of the of the Directive 2011/93/ EU includes a thorough definition of child pornography According to Article 2 of the Directive 2011/93/EU "child pornography" means:

(i) any material that visually depicts a child engaged in real or simulated sexually explicit conduct;

(ii) any depiction of the sexual organs of a child for primarily sexual purposes;

(iii) any material that visually depicts any person appearing to be a child engaged in real or simulated sexually explicit conduct or any depiction of the sexual organs of any person appearing to be a child, for primarily sexual purposes; or

(iv) realistic images of a child engaged in sexually explicit conduct or realistic images of the sexual organs of a child, for primarily sexual purposes;

In Greece, child pornography also means any virtual depiction of sexual organs or act.

Other cyber related crimes include:

1) REVENGE PORN

In 23-6-2022, after the disclosure that a well-known television co-host engaged in revenge porn acts, a law was voted that punishes the act of distributing sexual containing material without the consent of the other party/ parties.

2. ON LINE CHILD GROOMING

On line child grooming could be described as the proposal, by means of information and communication technology, by an adult to meet a child who has not reached the age of sexual consent, for the purpose of committing a sexual offence against the child who has not reached the age of sexual consent (in Greece 15 years old), where that proposal was followed by material acts leading to such a meeting.

In addition, in Greece a special crime is provisioned when an adult by means of information and communication technology offends the child by gestures or indecent proposals regardless of whether the perpetrator meets the child in person or not. (Meeting the minor is an aggravating factor).

On 6 February 2024 the European Commission published a proposal on combatting child sexual abuse which covers also offences as livestreaming of child sexual abuse and intentional access and dissemination of child sexual abuse deepfakes. Deepfake technology is used to create images or videos of people doing or saying things which they did not do or say. Although a child may not be physically harmed, the creation of CSAM deepfakes is a form of sexualization of the child.

Other special legislation includes the Convention on Cybercrime of the Council of Europe that helps facilitate the detection, investigation and prosecution both at domestic and international levels. Among other, the Convention facilitates the expeditious preservation of specified computer data

(article 16), the search and seizure of stored computer data (19) and real time collection of traffic data (20).

Furthermore, on December 2024 the General Assembly adopted the United Nations Convention against Cybercrime; Strengthening International Cooperation for Combating Certain Crimes Committed by Means of Information and Communications Technology Systems and for the Sharing of Evidence in Electronic Form of Serious Crimes.

The European Commission on 10 September 2020 presented a first legislative proposal containing an interim regulation allowing a number of independent interpersonal communications services, such as webmail, messaging services and internet technology to derogate from the privacy rules contained in the ePrivacy Directive to enable them to detect and report child sexual abuse material online on a voluntary basis. The act was adopted on 14 July 2021 and entered into force on 2 August 2021. It was limited until 3 August 2024. However, on 15 February Council and Parliament reached a provisional agreement to extend the interim regulation on a temporary derogation from certain provisions of the e – privacy directive for voluntary detection of online CSA until 3 April 2026. Derogation allowed streaming and video media applications to voluntarily detect, report and remove child sexual abuse material. After failed negotiations on an extension, the EU's interim ePrivacy derogation expired on 3 April 2026.

In addition to that, together with its new European strategy for a Better Internet for Kids, the Commission published on 11 May 2022 a proposal on permanent rules which are intended to replace the interim regulation. The proposed rules will oblige providers to detect, report and remove child sexual abuse material on their services.

PICTURE 3

In the more "conventional" types of child sexual abuse crimes that existed even before the internet era the use of e – evidence may come as a surprise. Ordinary evidence, such as medical examination of the victim, psychological evaluation, DNA analysis, and testimonies seem to be enough to prosecute someone for this type of crimes. But, sometimes, the combination of e – evidence with physical evidence is quite fruitful. For instance:

- The modern offender often isn't "satisfied" with just the sexual engagement with a minor. He/she also takes pleasure in really humiliating his/her victim by taking pictures or videos during the crime. In a well-known case in Greece a group of adolescents raped a minor repeatedly and had the "habit" of recording it on video. The videos were found on the mobile phone of one of the perpetrators and led to the identification of other perpetrators as well. The identification was possible because their faces and voices were shown and heard in the videos.
- Another thing is that criminals brag. They show off their acts and post them online. In one case in Greece, the identity of an offender was tracked simply by spotting his spots.

- The perpetrator often (especially if he/she is a friend, a relative or in general someone the minor trusts) is engaged in conversations with his/her victim by the means of sms or social media before or even after the crime is committed. Even if the actual facts of the crime itself aren't mentioned in these messages, usually the conversation is evaluated in combination with other more "traditional" evidence. Let's take this case as an example: N who is a minor had created a false account on Facebook pretending she was a 16 years old boy. K, born in 1977 began to have conversations with her until he convinced her to meet him. When they met, he raped her. The perpetrator argued that he didn't know her age. The Prosecutor using e – evidence and, specifically, the conversations from FACEBOOK between the victim and the perpetrator was able to prove that that wasn't the case and that the perpetrator knew her age. In another case the victim, who was 16 at the time, had engaged in a sexual relationship with her karate instructor. The defendant argued that the relationship had started after his student reached the age of 18. However, the messages and the time they were sent between the defendant and the victim revealed the truth. We must point out that there have been cases where even if text messages (or even MSN messages) were presented at court without a court order, they would be admissible. This occurred in two occasions: 1) the messages were handed to the authorities by one of the interlocutors, 2) the messages were found without the need to "open" the

phone, the laptop and the application using a password or special decryption. The data found on e – mails is also admissible without a court order if they were already printed or were found without the need to turn on the phone, the laptop and the application using a password or special decryption. The data found on a hard drive is admissible without a court order especially if they are on a work computer. However, it should be noted that the legal investigation of data in the cloud requires a court order for it to be conducted

- The new techniques also allow the tracking of mobile devices, especially smartphones. The location data of the smartphone can reveal the whereabouts of the suspect at the time of the offence. In a murder case the phone of the perpetrator gave away the fact that the husband was walking and going about in the house at a time when he was supposed to be tight by the murderers having lost his consciousness.

In these more “conventional” types of crime the perpetrator can use the e – evidence for his benefit as well.

In a case the perpetrator presented this argument to the Supreme Court (Areios Pagos): The perpetrator, a teacher of music, was condemned to 14 and a half years of imprisonment by the Mixed Court composed of regular judges and jurors of Athens for having sex with one of his students under 12 years of age. At the court hearing before the Mixed Court e – evidence was presented. The defendant had taken a picture of his act with a digital camera. He later stored the file in an encrypted form in a hard drive using “VERACRYPT”.

The defendant claimed that a mitigating factor at sentencing should be considered. That is the fact that he disclosed to the police the code to unlock his phone. The Mixed Jury Court rejected his claim reasoning that the decryption could take place even without the help of the defendant. The Court reasoned in addition that the defendant was caught by surprise by the house search and that was why he didn’t have the time to hide or destroy his device. Instead, he chose to pretend to cooperate with the investigation by handing over the code. The Supreme Court approved the reasoning and rejected the defendant’s petition. However, if the decryption was in no other way possible,

the voluntary disclosure by the accused could be considered a mitigating factor at sentencing.

A question is raised concerning the obligation of a third party (for example the IT of a company like Apple) to cooperate with the authorities. According to Regulation 2022/2065 of the European Parliament and of the Council providers are forced to provide suscribers' data if a formal legal order is issued by a court. This usually includes Account details and technical data.

PICTURE 4

Child pornography is among the crimes that the Greek law permits **undercover investigation with a court order**. The Court considers two principal tests when granting a court order. First, there must be sufficient evidence that the crime took place. Second, the detection of the crime would otherwise be impossible or extremely difficult.

Effective investigatory tools should include the possibility for law enforcement authorities to use **a concealed identity on the Internet**.

In the case of the rape of the girl named N the conversations between the perpetrator and the undercover investigator could be later retrieved by the false account. If the suspect has deleted the incriminating e – evidence on his/her mobile device or if the device is encrypted, the investigator could prior to that take photos of the messages and store the communication data on their own device.

In another case it was the mother who did the investigation herself! The perpetrator approached the victim on Facebook and offended her by gestures and indecent proposals. He also convinced his victim to send him naked pictures. The mother of the victim found the naked pictures on the victim's phone.

The offender claimed that he didn't know the age of the victim. However, our dear mom used some **Open Sources Intelligence** and found out that the offender had taken a female name on Facebook. She even took photos and printed the conversations between the victim and the offender and gave them to the authorities. So, the Judicial Council rejected the argument by saying among other things that the perpetrator was using a female name so that he could easily gain the trust of young girls.

In one case, the investigators found the mobile phone of a suspect on a **body – search**. It was confiscated and the analysis showed that 659 video and picture files were stored in it, containing child pornography material. Nevertheless, the investigators were not satisfied with finding that e – evidence. They analysed the device further. They found out he surfed the internet searching for child pornography related webpages. Most importantly, they found out on his phonebook keywords containing child pornography connotations. After that, he revealed to the investigators that he had met an Iranian on line who “shared the same interests with him”. So, the investigation of the phone book led to another suspect as well.

It should be mentioned that in this type of case, the victim testifies digitally i.e by means of electronic devises. The witness statement is stored in a digital file and is viewed in Court. The defendant is entitled to ask questions in writing but the deposition takes place without him/her or his/her lawyers. This deposition is considered to be evidence. Therefore, the defendant has the right to an electronic copy of it. Nevertheless, the Court cannot depend solely on this evidence in order to condemn the accused. The judges can however use this evidence together with other type of evidences as well (AP 878/2019).

In another case, a search of the suspect’s professional cabinet (the suspect was a lawyer) revealed that there were many files containing child pornography at his PC. However, the accused claimed that everyone in the office had access to that PC. Nevertheless, a house search was also conducted. The personal laptop of the accused was confiscated revealing the existence of the same files in it as well.

Information is derived by the profiling of a suspect as well. Once his/her mobile phone, laptop, tablet is seized, an analysis of the IE history file by visit or hit count is conducted. If the frequency of URLs to the Hit Count for each pornography type show that the suspect accesses child porn, chat rooms and pictures profiles (i.e. from Facebook) more often than adult porn and neutral websites, then it is more likely that the suspect is in fact a child pornography user and not someone that seeks adult porn. This type of profiling is frequently used by prosecutors in order to dismiss the accused persons claims that they were searching for adult porn and the child pornography material just happened

to pop out while navigating in the internet. It is included in the expert opion/ report of the analysts.

PICTURE 5

This report addresses some of these questions

1) Is there any child pornography material on the device?
2) When was the material produced/ downloaded? The answer to this question would be useful for establishing the time of the crime
3) What is the percentage of child pornography compared with the one of adult pornography?
4) How many times did the offender access the child pornography material?
5) Where deleted files are retrieved, the date and time of the deletion must be recorded
6) Has the offender produced any child pornography material (digital cameras, videos, skype etc)
7) Did the offender have access to websites containing child pornography material? Did the offender have accounts on these websites?
8) Are there any p2p systems?
9) Did the offender use any online applications such as Messenger, Chat and What's Up?
10) Is there any child pornography material stored on the Cloud?

PICTURE 6

Case about report

In fact, in a case the expert opinion had an enormous impact on the outcome of the trial.

The defendant, residing in Thessaloniki, was prior to the investigation of the case in question convicted by the Mixed Jury Court of First Instance of

Thessaloniki for possessing 150 pictures of child pornography on his computer on 13-7-2016. Nevertheless, he was prosecuted once more for the possessing of 338 files containing child pornography material. The defendant used the non bis in idem argument. The expert report solemnly explained that this was a different act of possession. It took place on 12-7-2016, the files were completely different and they were stored in two devices, the P/C and one usb stick. The argument was dismissed.

The lack of proper investigation led to the acquittal of another accused. He was accused for the possession of three external hard drives containing child pornography material. He was a student at the Hellenic Military Academy.

On two occasions his hard drives were not in his possession (the first one for 15 days) due to a non-scheduled inspection at the dorms of the school and the intervention of a fellow student who had taken one of them and had never returned it. In addition to that, there was no proof that the 3 hard drives that were initially confiscated by the inspectors of the Military Academy were the ones confiscated by the proper authorities that is the police. Moreover, there was no examination of the internal hard drive. If there had been, there would have been some findings on whether the accused visited webpages related to child pornography and downloaded the files that were found in the three external hard drives.

In another case the accused was prosecuted for communicating on the internet with a 13-year-old girl and for convincing her to send him naked pictures and a video showing her genitals.

The accused claimed that he had participated at the online game Travian for several months. In order to communicate with other players, he used msn messenger and some email addresses. Therefore, he claimed that another player was communicating with the minor without him knowing. So, what happened was this: The other player's account "synchronized" with the device of the accused. The files were downloaded in his device without him knowing.

The accused was acquitted based on this evidence: 1) Not a single file was found indicating there was a communication and/or file sharing between the accused and the victim. 2) The examination and analysis of the laptop revealed that the conversations didn't take place originally at the accused's laptop. The communication and multimedia files in question auto synced between the

accused's laptop and another device. 3) There was no digital evidence of sharing, obtaining and distributing child pornography.

PICTURE 7

Europol received information on child pornography from the National Center for Missing and Exploited Children. Digital trace led to Greece and after a court order was issued the police were able to identify one suspect living in Nafplio.

A house search was conducted. A hard disc was seized. While searching his mobile devices the policemen noticed that the Program ManyCam was downloaded on his laptop. Manycam uses a webcam or video camera as input for the software itself as an alternative source of input.

On his hard drive 5 video files were found depicting children under 15 years of age engaging in sexual activities. Furthermore, it was established that on 16-3-2016 he had access to child pornography on the free online chat website Omegle and that on the same day he had distributed one video file of child pornography.

The investigators also did a little of IE history check. They found out that the suspect was banned from the website Omegle due to inappropriate behavior.

Furthermore, on the file "Downloads" on his laptop one video and three pictures containing child pornography material were found.

Further investigation established the fact that on the 15-6-2016 he had distributed two similar videos again on the website Omegle. It also revealed that he had searched internet and visited websites using keywords with child pornography connotations. He had also used many times the program Dropbox using yet again keywords containing child pornography connotations. Finally, it was discovered that he had watched a video regarding the Dark Web.

PICTURE 8

The suspect was arrested and was prosecuted for a child pornography felony. He claimed that while visiting Omegle unknown users sent him hyperlinks with child pornography material without him knowing. He had a poor IT knowledge and on top of that: he wasn't aware of the downloading.

Lack of IT knowledge and of the actual downloading are the most common arguments of the accused persons. In another case, the court (Areios Pagos 643/2020) rejected the argument because of the following facts: 1) The files were visible to the driver. 2) Furthermore, the suspect had legal professional files in the same driver as well, files that he often used. So, he couldn't have missed the existence of the criminal files. 3) In addition to that, in another driver there were files encrypted. This encryption couldn't be done without the accused's knowledge. Finally, 4) the expert testified that there was no proof of some strange "invader".

However, in another case the Court accepted the argument. At an external hard drive 158 pictures of child pornography were able to be retrieved by the investigators. Nevertheless, there was no proof that the accused had distributed the pictures. Moreover, the files were deleted and there was no proof that he had opened them. The Court accepted the claim of the accused that the files were downloaded at the same time as some music files he wanted to download. Once he realized that the files contained child pornography material, he erased them. However, there remained the cookies and the investigators were able to retrieve the files.

In general, indications such as the downloading of elaborated applications, access to the darkweb and use of keywords and symbols associated with content depicting child pornography lead to the condemnation of the accused in question.

PICTURE 9

However, in our case, the Judicial Council of Nafplio dismissed his claims stating that the accused did not have a poor IT knowledge and he knew perfectly well what he was doing.

First of all, it was a fact that he did install ManyCam and used it to watch a child pornography video.

Secondly, he had access to the darkweb.

Thirdly, he used keywords and symbols with child pornography connotations.

Finally, he had visited OMEGLE many times until 2-3-2017 when he was banned from the site.

The accused was indicted before the Mixed Jury Court of First Instance of Corinth. There he made the same claims adding that he didn’t even know that the files from Omegle were downloaded to his laptop. He confessed though that he opened some of them out of curiosity.

In addition, he claimed that the act was not a felony but a misdemeanor. The Mixed Court rejected all his claims, appreciated the evidence, including the cd where all the digital evidence were copied and stored, and sentenced the accused to 4 years of imprisonment. The hard drive remains seized.

Paola Berta

Digital evidence in Spanish and EU legal practice: Legal framework, admissibility risks and reliability

Training of Lawyers in various areas of EU law 2 **#TRAVAR2**

Co-funded by the EU

PURPOSE OF THIS DECK

Training of Lawyers on various areas of European Union Law 2

Co-funded by the European Union

#TRAVAR2

- Legal framework, admissibility risks and reliability issue

- Map the main Spanish, EU and international instruments relevant to digital evidence

Focus: criminal procedure, electronic communications data, forensic preservation, cooperation and platform/service-provider evidence.

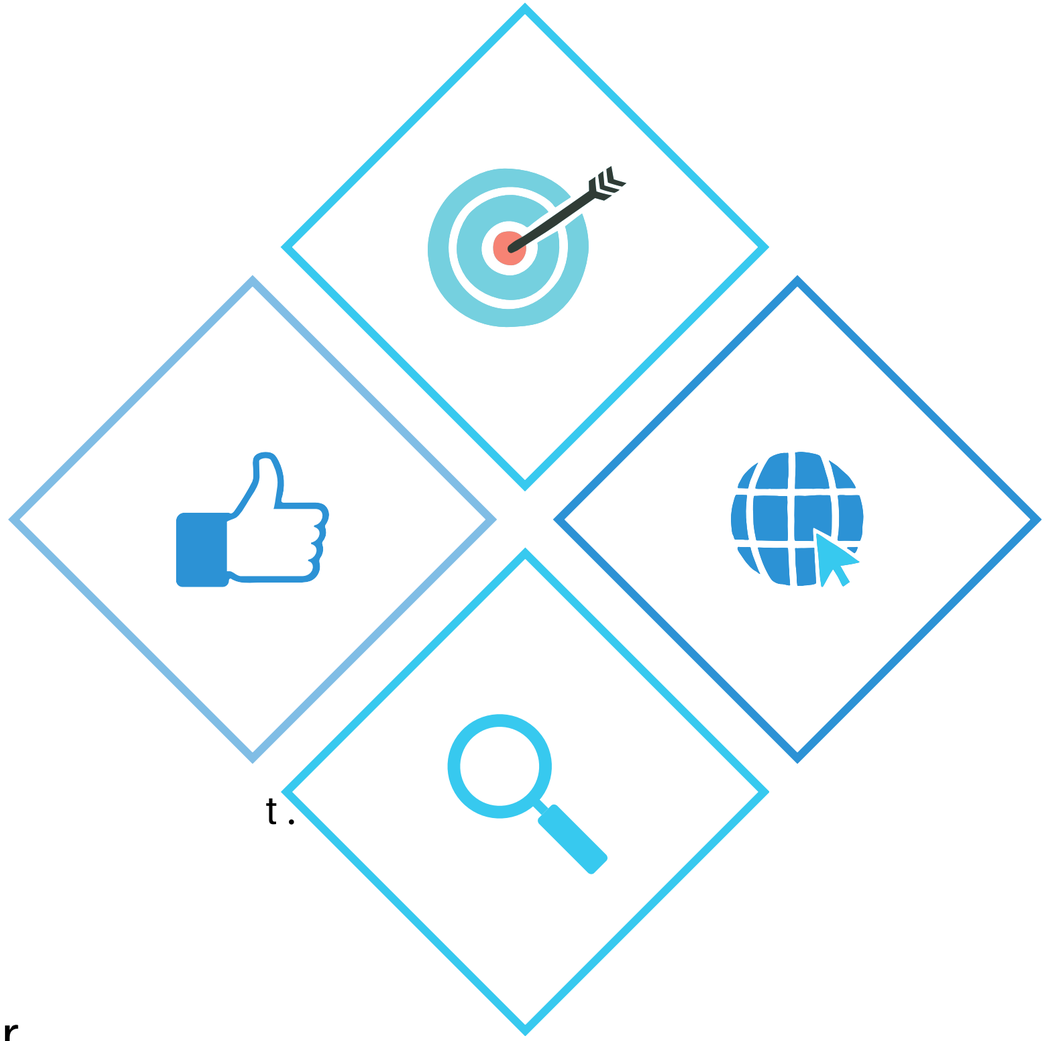
- Compare exclusionary rules and doctrines affecting unlawfully obtained evidence.

- Provide a practical checklist for assessing legality, reliability and litigation risk.

Digital evidence: core idea

Training of Lawyers on various areas of European Union Law 2
Co-funded by the European Union
#TRAVAR2

- Digital evidence is information stored, processed or transmitted in electronic form.



t .

- it normally requires hardware/software to make binary data perceptible as text, image, audio, video or metadata.

Courts assess both:

- Lawfulness: was the evidence obtained without violating fundamental rights or procedural safeguards?
- Reliability: can identity, integrity, authenticity and continuity of custody be demonstrated?

Practical lifecycle of digital evidence

1. **Identification of the source:** **device, account, platform, provider, network or cloud service.**
2. **Legal authority: consent, judicial authorisation, prosecutorial/police power, civil production mechanism or international cooperation.**
3. **Preservation: sealing, rapid preservation, Budapest preservation, chain-of-custody record.**
4. **Verification**: hash values, forensic report, logs, metadata, expert validation.
5. **Presentation: procedural filing, technical reproduction in court, adversarial scrutiny**
6. **Challenge: fundamental-rights objections, authenticity, manipulation, broken custody, derivative evidence.**

Training of Lawyers on various areas of European Union Law 2

Co-funded by the European Union

#TRAVAR2

SPAIN Normative Framework

Training of Lawyers on various areas of European Union Law 2
Co-funded by the European Union
#TRAVAR2

LOPJ ART.11,1

Exclusion of evidence obtained in violation of fundamental rights.

Basis for nullity/exclusion of unlawfully obtained digital evidence and, where applicable, derivative evidence.

LECRIM ART. 588 TER J-M ART. 588 OCTIES

Access to communications-related data, IP addresses, device identifiers and subscriber/device identification.

Preservation orders for data.

Criminal investigations involving providers, communications data, IP, IMSI/IMEI and ownership identification.

Determines when judicial authorisation is required and when police/prosecutors may act directly.

LAW 25/2007, ART. 3

Retention of electronic communications data.

Operators providing publicly available electronic communications services or public networks.

Identifies retained traffic/location data categories; access generally requires judicial authorisation.

LECRIM, ARTO282 BIS. 6-7

Undercover computer/online agents.Criminal investigations involving online undercover activity.

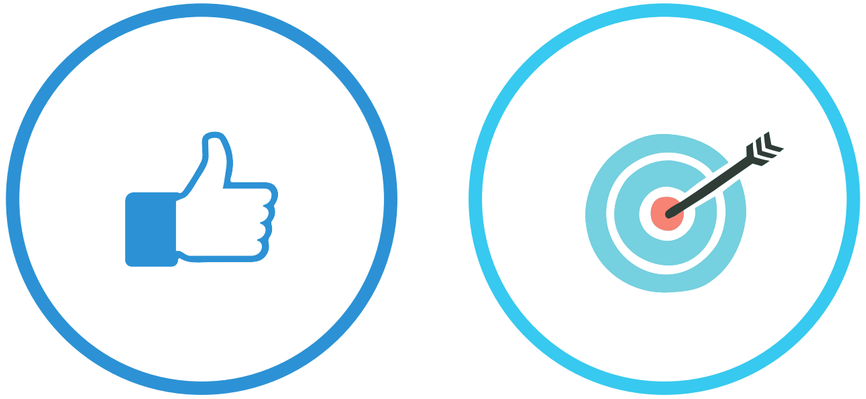
Supports controlled online operations and, in certain cases, exchange or analysis of illicit files.

Training of Lawyers on various areas of European Union Law 2
Co-funded by the European Union
#TRAVAR2

Spanish procedural law: LECrim access to data

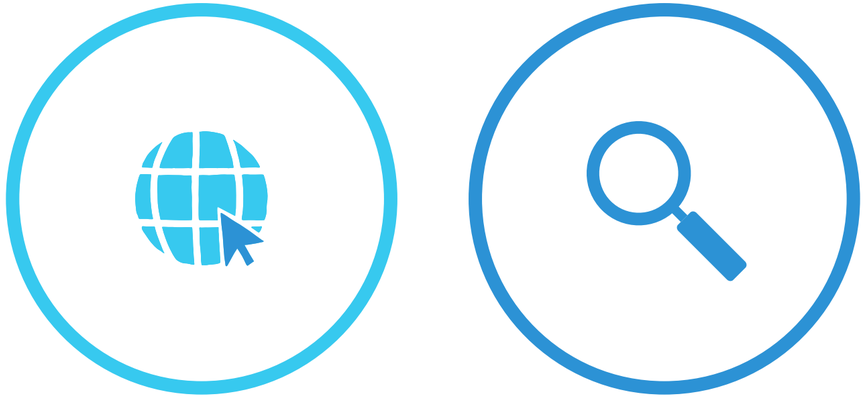
ART.588 TER J LECRIM

- communications-related data held by providers may require judicial authorisation.



ART.588 TER M LECRIM

- .prosecutor or judicial police may directly request certain ownership/device identification data.



• ART. 588 TER K LECRIM

- police may obtain IP address by their own means, but linking the IP to a subscriber/device via provider data requires judicial authorisation.

• ART. 588 TER L LECRIM

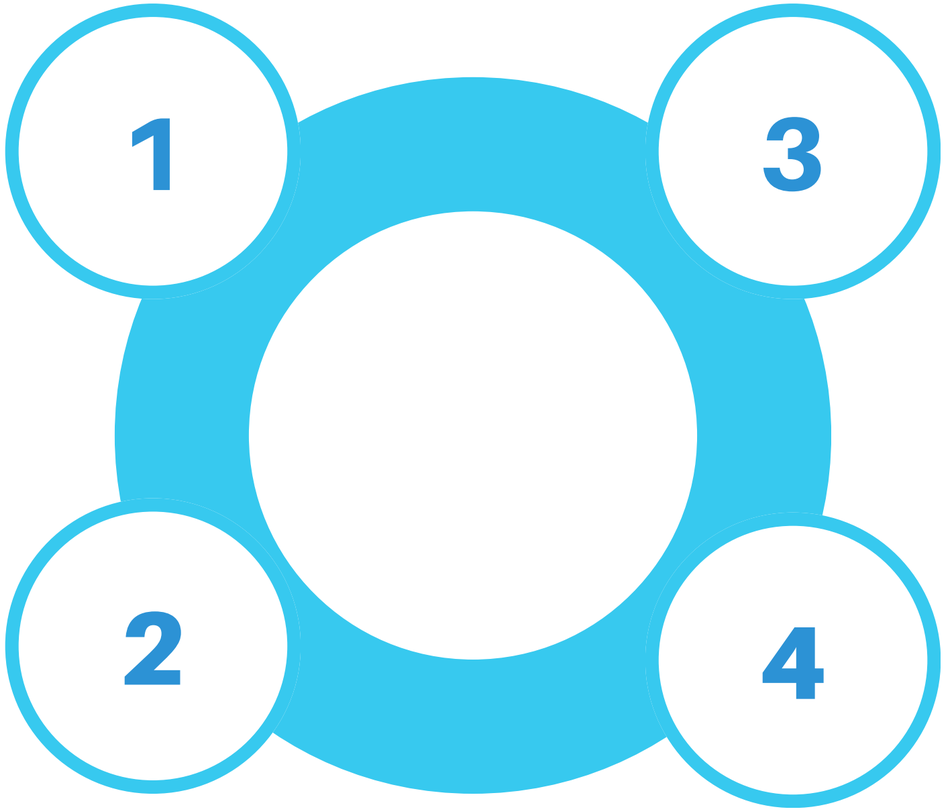
- police may obtain IMSI/IMEI-type identifiers, but linking them to line/subscriber data or intercepting communications requires the appropriate judicial authorisation. (Auto)

Training of Lawyers on various areas of European Union Law 2
Co-funded by the European Union
#TRAVAR2

EU COOPERATION: European Investigation Order

- The EIO is the main EU mutual-recognition tool for investigative measures in criminal matters.

- It can be used to request preservation of evidence, production of evidence, real-time measures, location/tracking or access to computer systems, depending on the measure and national implementation.

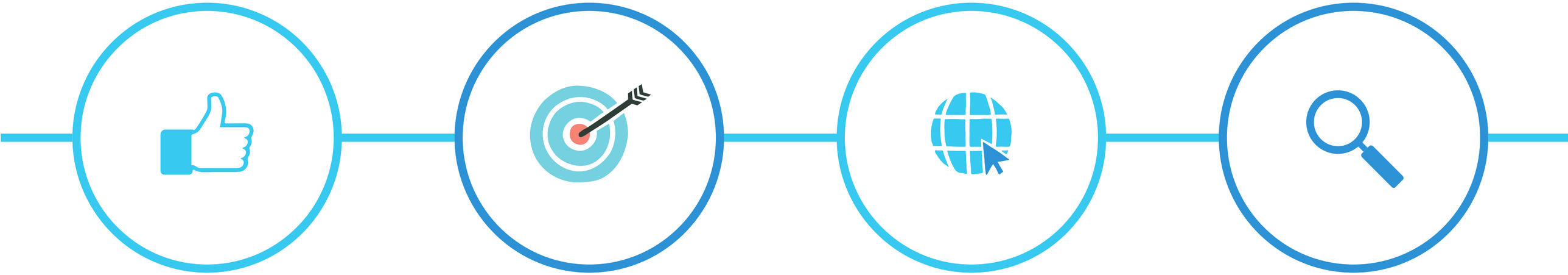


- Directive 2014/41/EU Art. 32.1 allows provisional measures to prevent destruction, transformation, movement, transfer or disposal of an item that may be used as evidence.

- Spanish Law 23/2014 implements issuance and execution rules, including urgent decisions on preservation measures.

Training of Lawyers on various areas of European Union Law 2
Co-funded by the European Union
#TRAVAR2

EU E-EVIDENCE SYSTEM FROM 2026



- Regulation (EU) 2023/1543 applies from 18 August 2026.

It introduces:

- European Production Order Certificate (EPOC): production of electronic evidence.
- European Preservation Order Certificate (EPOC-PR): preservation of electronic evidence.

- Orders are sent directly to the provider's designated establishment or legal representative.

- Preservation must occur without delay; delivery is generally within 10 days, or 96 hours in urgent cases.
- Grounds for refusal/notification issues include privilege/immunity, press/freedom of expression rules, manifest fundamental-rights breach, non bis in idem and certain double-criminality issues.

BUDAPEST CONVENTION IN CYBERCRIME

First international treaty focused on cybercrime and electronic evidence

Training of Lawyers on various areas of European Union Law 2
Co-funded by the European Union
#TRAVAR2

1

- Provides a global cooperation framework for cybercrime and digital evidence.

Key tools:

- Rapid preservation of stored computer data.
- Subsequent mutual-assistance requests for search/access, seizure or disclosure.
- Rapid disclosure of enough data to identify the provider and transmission route.
- Emergency direct authority-to-authority channels in urgent cases.

2

3

- Preservation normally lasts at least 60 days to allow a formal request to follow.

4

- Denial may be possible for political offences or threats to sovereignty, security, public order or essential interests.

DSA AND INTEMEDIARY-SERVICE PROVIDERS

Training of Lawyers on various areas of European Union Law 2
Co-funded by the European Union
#TRAVAR2

- Intermediaries include access providers, hosting services, platforms, socia networks and online marketplaces.

1

- The DIGITAL SERCICE ACT is directly applicabl in Spain and includes cooperation duties.

2

3

- Art. 10 DSA: orders to provide information.
- Art. 18 DSA: notification of suspected criminal offences.
- Practical relevance: platform information, illegal-content investigations, account/data identification and escalation to public authorities.

4

Training of Lawyers on various areas of European Union Law 2
Co-funded by the European Union
#TRAVAR2

EXCLUSIONARY RULE: UNLAWFUL EVIDENCE

- Under Spanish law, evidence obtained in violation of fundamental rights may be null and without evidential effect.

Purpose of exclusion:

- deter fundamental-rights violations in criminal investigations;
- avoid aggravating the original rights violation through use at trial;
- protect the integrity and fairness of the process.

- Digital evidence is especially exposed to exclusion arguments where access to devices, accounts, communications or retained data lacks authority or exceeds scope.

FALCIANI DOCTRINE

STS 116/2017 OF 23 FEBRUARY, AUTHORED BY JUDGE MARCHENA:

THE CONSTITUTIONAL COURT'S FALCIANI DOCTRINE REJECTS AUTOMATIC NULLITY IN EVERY CASE OF RIGHTS INFRINGEMENT.

Training of Lawyers on various areas of European Union Law 2

Co-funded by the European Union

#TRAVAR2

- **COURTS MUST PERFORM A BALANCING ANALYSIS:**

1

- Internal control:
- Was the violation instrumentally aimed at obtaining evidence outside constitutional channels?
- Was the violation so intense that it affected the core values of the fundamental-rights system?

2

- External control:
- Are there general prevention or deterrence needs that require exclusion to protect future rights effectiveness?

3

- Practical effect:
- unlawfulness does not always equal exclusion, but serious or instrumental violations remain high-risk

STS 116/2017, of 23 February, is the landmark judgment of the Spanish Supreme Court that, for the first time in Spain, upheld the use of the 'Falciani list' as incriminating evidence in tax-related criminal proceedings. This ruling established doctrine on illegally obtained evidence by private individuals and its admissibility in criminal procedure.

FRUIT OF THE POISNOUS TREE

DOCTRINE

DERIVATIVE EVIDENCE OF A NULL ORIGINAL EVIDENCE

1

- Derivative evidence may be excluded if it has a natural connection with null original evidence.

2

- Key question: is there a sufficient causal and legal connection between the unlawful source and the later evidence?
- If yes, the general rule is exclusion of the derivative evidence.

3

- Possible litigation arguments may focus on independence, attenuation, inevitability or absence of relevant connection, depending on the facts and applicable case law.

Training of Lawyers on various areas of European Union Law 2

Co-funded by the European Union

#TRAVAR2

RECORDINGS MADE BY PRIVATE INDIVIDUALS

1

- **Exclusion can apply where a private individual's purpose is to obtain evidence unlawfully or to gain a procedural advantage through rights infringement.**

2

- **Recordings of out-of-court confessions by one participant may be admissible only where they are spontaneous and produced in a good-faith communicative context.**

3

- **If the recording is obtained through trickery, deception or a scheme to obtain evidential material, it may violate the integrity principle supporting exclusion**

4

Evidence obtained through torture or treatment radically compromising trial fairness must be excluded even if the infringer is a private individual and even if the conduct was not process-driven.

Training of Lawyers on various areas of European Union Law 2

Co-funded by the European Union

#TRAVAR2

COMPARATIVE MATRIX: EXCLUTION DOCTRINES:

Training of Lawyers on various areas of European Union Law 2
Co-funded by the European Union
#TRAVAR2

UNLAWFUL EVIDENCE ART. 11.1 LOPJ	FALCIANI DOCTRINE	FRUIT OF THE POISONOUS TREE DOCTRINE	PRIVATE RECORDINGS
Fundamental-rights violation in obtaining evidence.	Evidence obtained with a rights infringement, especially by a private actor or non-state route.	Later evidence derives from null original evidence.	Recording by a participant or private person.
Was the evidence obtained directly or indirectly in violation of fundamental rights? Requires identification of the infringed right and connection with evidence. **EFFECTS:** Nullity/exclusion; judgment cannot rely on it.	Balancing: instrumental purpose, intensity of violation, deterrence/prevention needs Not automatic; contextual and rights-sensitive. **EFFECTS:** May allow or exclude evidence depending on balancing.	Natural/causal connection between null source and derivative evidence. Challenge may fail if connection is broken or evidence is genuinely independent **EFFECTS:** Exclusion of derivative evidence where connection persists.	Spontaneity and good faith vs trickery, deception or process-oriented evidence gathering. Torture or radical unfairness always strongly triggers exclusion. **EFFECTS:** Admission if spontaneous/good faith; exclusion if integrity/fairness compromised.

Training of Lawyers on various areas of European Union Law 2
Co-funded by the European Union
#TRAVAR2

Reliability: chain of custody

Chain of custody is the documented procedure proving identity, integrity and authenticity from seizure/discovery to court production.

A generic allegation is not enough: the challenger should identify when, how and to what extent continuity was broken.

- HASH VALUE:
A hash is a mathematical result produced by a standard algorithm such as MD5, SHA-1, SHA-256 or SHA-512.
- If even one bit changes, the resulting hash changes.
- Practical uses:
- verify that original and forensic copy are identical;
- detect later manipulation;
- document integrity in minutes, police reports, notarial records or internal-investigation records;
- support expert testimony.

CORE STAGES:

SEIZURE/IDENTIFICATION;

SEALING;

TRANSFER;

STORAGE;

OPENING/UNSEALING;

FORENSIC COPY/CLONING;

HASH RECORDING;

EXPERT ANALYSIS;

COURT FILING AND PRESERVATION.

FORENSISC COPY/CLONING

A forensic copy should capture all data from the source while keeping the original unaltered.

FORENSISC COPY

- A physical clone is preferable to a merely logical copy when deleted files or full device state matter

BEST PRACTICE

- use tools and methods that avoid altering the source;
- document witnesses, public certifier/notary or court officer presence where appropriate.
- preserve the original as evidence;
- work on the forensic clone;
- consider a second copy for business continuity where the data owner must keep operating;

Training of Lawyers on various areas of European Union Law 2
Co-funded by the European Union
#TRAVAR2

PRACTICAL LITIGATION STRATEGY

Training of Lawyers on various areas of European Union Law 2

Co-funded by the European Union

#TRAVAR2

BEFORE RELYING ON DIGITAL EVIDENCE

- map the legal route used to obtain it;
- identify every person/entity who handled it;
- verify original, clone, hash and custody record;
- isolate potentially tainted evidence from independent evidence;
- prepare a proportionality and necessity explanation;
- prepare for authenticity and manipulation objections.

BEFORE CHALLENGING DIGITAL EVIDENCE

- identify the precise right or procedural rule infringed;
- explain the causal link between infringement and evidence;
- specify the custody break or technical defect;
- identify derivative evidence affected by the same taint.

KEY TAKEAWAYS

- Digital evidence is not just a technical object; it is a procedural and fundamental-rights issue.
- Spanish law combines exclusionary rules, procedural authorisation regimes and evidential reliability standards.
- EU and international instruments are essential where providers, data or systems are outside Spain.
- The strongest evidence package includes: lawful authority, narrow scope, rapid preservation, forensic copy, hash, custody record, expert explanation and adversarial reproducibility.
- The main litigation risks are: unlawful access, excessive scope, broken chain of custody, absent hash, manipulated/private recordings and derivative taint.