

Valentine Guiriato

The digitalisation of European criminal cooperation instruments: towards a digital cross-border criminal procedure

Paris, 13 November 2026

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

Co-funded by the EU

Introduction

From mutual recognition to digitalised mutual recognition

LEGAL BASES

- **Art. 67 TFEU**
- **Art. 82(1) TFEU**
- **FD 2002/584 — EAW**
- **Directive 2014/41 — EIO**

"Judicial cooperation in criminal matters in the Union shall be based on the principle of mutual recognition of judgments and judicial decisions."

Art. 82(1) TFEU

YESTERDAY — FOR TWENTY YEARS

Rules enabling judicial decisions to circulate **legally**

TODAY

An infrastructure enabling decisions and evidence to circulate **digitally**

I. EU primary law

LEGAL BASES

Art. 82(1)(d) TFEU

Regulation 2023/2844

Digitalisation is not a stand-alone IT policy: it is a means of achieving the European area of criminal justice.

RECITAL 1 OF THE REGULATION — "DIGITAL BY DEFAULT"

Preserving the necessary safeguards, interoperability, security and mutual trust

Digital transmission: **from a practical arrangement left to the practice of the Member States to a legally organised mode of operation of cooperation**

II. The Regulation of 13 December 2023

The core instrument of digital judicial cooperation

LEGAL BASES

- **Regulation 2023/2844**
- **Art. 1 — subject matter**
- **Art. 3 — decentralised IT system**

ART. 1 — TO DIGITALISE IS TO ORGANISE

- the communication channel
- the identification of the actors
- the authenticity of exchanges
- the integrity of documents
- the receipt of documents
- remote participation

ART. 3 — DECENTRALISED SYSTEM

- No single European criminal case file
- Each State keeps its own systems
- Objective: interoperability

A network architecture, not a centralisation of case files

III. A technical infrastructure governed by EU law

LEGAL BASES

Regulation 2022/850 — e-CODEX

Art. 82(1) TFEU



RECONSTRUCTING THE DIGITAL TRAIL OF THE DOCUMENT

Who sent it? When? To which recipient? Received when? Content unchanged?

IV. The Directive of 13 December 2023 and the move of existing criminal law instruments into the digital environment

LEGAL BASES

Directive 2023/2843

Regulation 2023/2844

THE REGULATION

Creates the horizontal framework for digital cooperation

THE DIRECTIVE

Adapts the existing sector-specific instruments

Amendment of existing sector-specific instruments: financial penalties, transfer of sentenced persons, probation, supervision measures as an alternative to provisional detention, conflicts of jurisdiction

V. The legal value of the electronic document

LEGAL BASES

Regulation 2023/2844

Regulation 910/2014 of 23 July 2014

PAPER PROCEDURE

- The original
- The copy
- The handwritten signature
- Certification as a true copy
- The seal

DIGITAL ENVIRONMENT

- Authenticity
- Identification of the signatory
- Integrity
- **Traceability**

VI. French law

Article 801-1 and Articles D. 589 et seq. of the French Code of Criminal Procedure

LEGAL BASES

- **Art. 801-1 CCP**
- **Arts. D. 589 to D. 589-7 CCP**
- **Order of 6 September 2019**

D. 589	The digital file may itself be the procedural document
D. 589-1	The case file itself becomes digital
D. 589-3 to 5	Electronic signature, electronic seal
2019 Order	Archiving, conversion, re-materialisation, transmission by lawyers

VII. From 2029 onwards

LEGAL BASES

Ordinance 2025-1091 of 19 November 2025

ENTRY INTO FORCE

1 January 2029

L. 1611-1 All documents may be drawn up in digital format

L. 1611-2 Digital signature ensuring the document can no longer be altered

L. 1611-3 Fully digital case file, with no paper medium

L. 1611-3 sets aside certain provisions: original / copy · certification of copies as true copies · certain rules on placing items under seal

VIII. Electronic evidence

LEGAL BASES

Regulation 2023/1543 of 12 July 2023

Art. 82(1) TFEU

Art. 294 TFEU

Art. 1: European Production Order or European Preservation Order addressed to a service provider established or represented in another Member State

TRADITIONAL MODEL

Territory of the State → Authority of that State

REGULATION 2023/1543

The service provider, not the location of the server

XI. Data, production and preservation

LEGAL BASES

Regulation 2023/1543

FOUR CATEGORIES

Subscriber data	User identification	Traffic data	Content data

Safeguards vary with the category and the level of interference

TWO DISTINCT INSTRUMENTS

Production: obtaining the evidence

Preservation: preventing its deletion

Preserving data does not authorise the authority to access it

XII. Procedural safeguards

LEGAL BASES

- Charter of Fundamental Rights of the EU
- ECHR

Charter, Art. 7	Private life and communications
Charter, Art. 8	Protection of personal data
Charter, Art. 47	Effective remedy
Charter, Art. 48(2)	Rights of the defence
ECHR, Art. 6	Fair trial
ECHR, Art. 8	Private life and correspondence

Technology is never an exception to fundamental rights

XIII. Confidentiality and videoconferencing

Two practical checks for the lawyer

LEGAL BASES

- **Regulation 2023/2844**
- **EU Charter, Arts. 47 and 48**
- **ECHR, Art. 6**

XIV. LEGAL PROFESSIONAL PRIVILEGE

A technical review of the measure:

- time period and keywords
- accounts and devices
- data categories
- isolation of privileged communications

XV. VIDEOCONFERENCING

Can the person actually:

- participate, see and hear?
- receive interpretation?
- consult the documents?
- communicate **confidentially** with their lawyer?

Proportionality is measured by the volume, duration and scope of extraction

XIV. A six-step legality review

When faced with cross-border digital evidence

1. **The legal basis**
2. **Jurisdiction**
3. **The scope**
4. **Necessity and proportionality**
5. **Integrity of the evidence**
6. **Effective remedy**

The question that governs all the others: **who can challenge what, before which court, in which State and at what point?**

Conclusion

From a law of documents to a law of data

THREE TRADITIONAL CATEGORIES OF OUR CRIMINAL LAW DISPLACED

Territory

Regulation 2023/1543

The original

Future Art. L. 1611-3 CCP

The channel

Regulations 2023/2844 and 2022/850

From a culture of the case file to a culture of data and its traceability

Digitalisation can automate transmission. **It cannot automate the assessment of proportionality.**



Dimitris Lochias

Digitalisation of EU criminal law instruments in Cyprus

Paris, 13 November 2026

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

Co-funded by the EU

Would a criminal lawyer from 1980 recognise the process?

- The indictment still reaches the registrar on paper.
- A judge reviews it, and a court bailiff serves the accused in person.



How does the defence obtain disclosure?

Paper request

- Counsel deliver a written request to the District Prosecutor's Office by hand or by fax.

Online request

- Counsel can apply online and receive scanned copies of the case file.

In my experience, most lawyers still use the paper route.

Co-funded by the European Union | TRAVAR2

Digital evidence in a paper courtroom

- Criminal hearings are never conducted remotely.
- Counsel lodge documentary exhibits in hard copies.
- CCTV footage, telephone records and device data may reach the court on a USB drive.



A warrant at five in the morning

- A police officer locates the on-call judge.
- The officer presents the application in person.
- The judge signs a paper warrant.



Filing a criminal appeal from Limassol

- Counsel arrange delivery of the stamped appeal to the Court of Appeal in Nicosia.
- Directions hearings generally require counsel to attend in person.
- Skeleton arguments are filed on paper.



Co-funded by the European Union | TRAVAR2

Challenging a warrant through iJustice

Electronic filing

- Counsel can apply electronically to the Supreme Court for certiorari to quash a warrant.

At the hearing

- The court may still work from printed copies of the application and exhibits.

Co-funded by the European Union | TRAVAR2

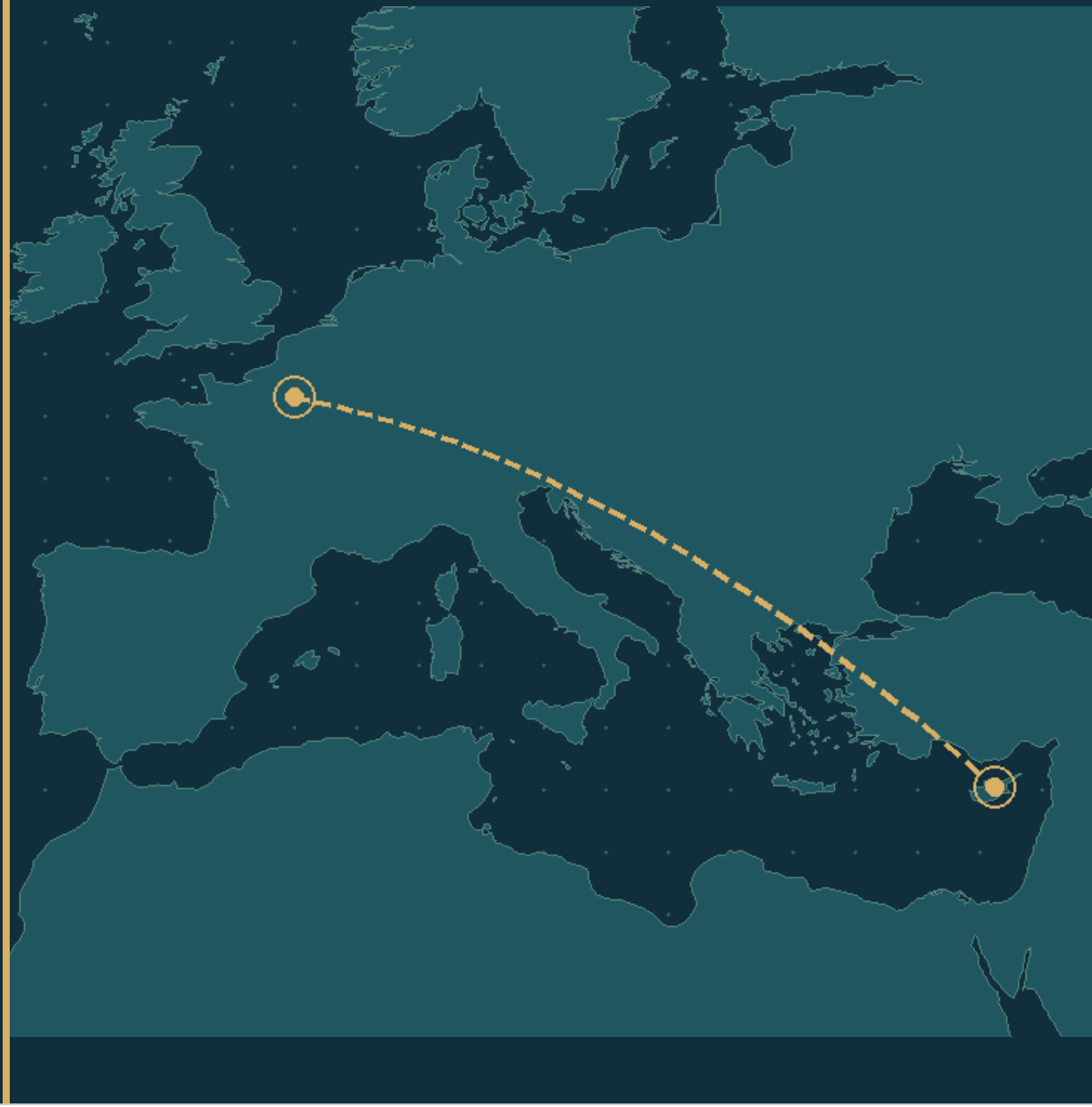
Criminal practice in the Sovereign Base Areas

- Counsel can email the registry and judges.
- Some issues are even dealt with by telephone.
- The parties and the court can share an electronic case bundle.
- Hearings can take place by Teams or Zoom.



EU judicial cooperation

Why cross-border communication matters



Why move cross-border exchanges online?

Speed and cost

- Faster exchanges reduce delay and administrative cost.

Privacy

- Secure channels help protect personal data and private life.

Continuity

- Authorities can keep cases moving when ordinary channels are disrupted.

Regulation (EU) 2023/2844, recital 4

When a Cypriot judge needs an urgent answer

35

days from arrest

Ordinary first-instance deadline when surrender is contested

- The District Judge can urgently request supplementary information in an EAW case.
- Waiting for a reply can mean another hearing and more time in custody.

Framework Decision 2002/584/JHA, Art. 15(2) · Cyprus EAW Procedural Regulation 17/2021, r. 3

Why both Member States need a digital channel

A request from Cyprus

- A Cypriot court can send a request instantly and still wait for a reply on paper.

A common channel

- National justice systems can exchange case information directly and securely.

Regulation (EU) 2023/2844, recitals 2 and 8

Co-funded by the European Union | TRAVAR2

Electronic evidence can disappear

- A provider may delete data before an ordinary cooperation request arrives.
- A preservation order can secure the data while the authority seeks production.
- Since 18 August 2026, EU orders can go directly to a provider’s designated establishment or legal representative.



Regulation (EU) 2023/1543, recital 8 and Arts. 6, 7 and 34

The most used instruments

Arrest warrant	• The European Arrest Warrant (EAW) provides for arrest and surrender.
Investigation order	• The European Investigation Order (EIO) is used to obtain evidence in another Member State.
Freezing and confiscation	• Orders concerning assets can be recognised and executed across borders.

Regulation (EU) 2023/2844, Annex II, points 1, 10 and 11

When do the common digital rules apply?

15 January 2026

- The Commission adopts the technical rules for the three instruments.

17 January 2026

- The legislative deadline for adopting those technical rules.

1 March 2028

- The common transmission rules apply to proceedings initiated from this date.

Regulation (EU) 2023/2844, Arts. 10(3)(a) and 26(3)–(4) · Implementing Regulation (EU) 2026/101

CYPRIOT CENTRAL AUTHORITIES

Who receives the request in Cyprus?

The Ministry of Justice and the specialised authorities



The Ministry of Justice and Public Order

The Ministry

- The Ministry assists with transmission and coordination for the principal mutual-recognition instruments discussed here.

Competent authorities

- The court decides on surrender. Direct authority-to-authority communication remains possible where the instrument permits it.

Law 133(I)/2004, s. 5; Law 181(I)/2017, s. 8(2)–(3)

Other instruments handled by the Ministry

Sentences	• Recognition of financial penalties and enforcement of custodial sentences.
Supervision	• Probation measures, alternative sanctions and pre-trial supervision measures.
Protection	• European Protection Orders.

Laws 179(I)/2007, 67(I)/2014, 69(I)/2014, 121(I)/2016 and 156(I)/2015

Two exceptions in Cyprus

MOKAS

- The Unit for Combating Money Laundering receives and transmits EU freezing and confiscation orders.

Chief of Police

- The Chief of Police is the central authority for exchanging criminal records through ECRIS.

Law 188(I)/2007, s. 43K(3) · Law 123(I)/2022, s. 4(1)

AN EAW IN PRACTICE

The European Arrest Warrant

From a French warrant to a Cypriot courtroom



How an EAW reaches Cyprus

SIS arrest alert

- The issuing authority can enter a SIS alert, including when the person's whereabouts are known.

Direct transmission

- The issuing authority can also send the EAW to the Ministry, directly or through its central authority.

These routes can operate together. Operational practice described by the authorities interviewed.

Who sees the alert and who follows up?

SIS / Arrest alert

- Cypriot officers have had access since 25 July 2023.
- The issuing state enters the alert and attaches a copy of the original EAW.

SIRENE / Follow-up

- National SIRENE bureaux exchange supplementary information about the alert.

Regulation (EU) 2018/1862, Arts. 7–8 and 26–27 · Council Decision (EU) 2023/870

A French warrant at Larnaca Airport

- A passenger check returns a hit on a French SIS arrest alert.
- The alert and attached EAW copy have the legal effect of an EAW. Cypriot officers can act immediately.
- Cyprus notifies France through SIRENE. The Ministry receives the update and liaises with France.

Regulation (EU) 2018/1862, Art. 31(1)



When France has a Cyprus address

Ministry of Justice

- The Ministry receives the scanned EAW by email, with a Greek or English translation.

District police

- The Ministry emails the warrant to police where the person lives or works.

District Judge

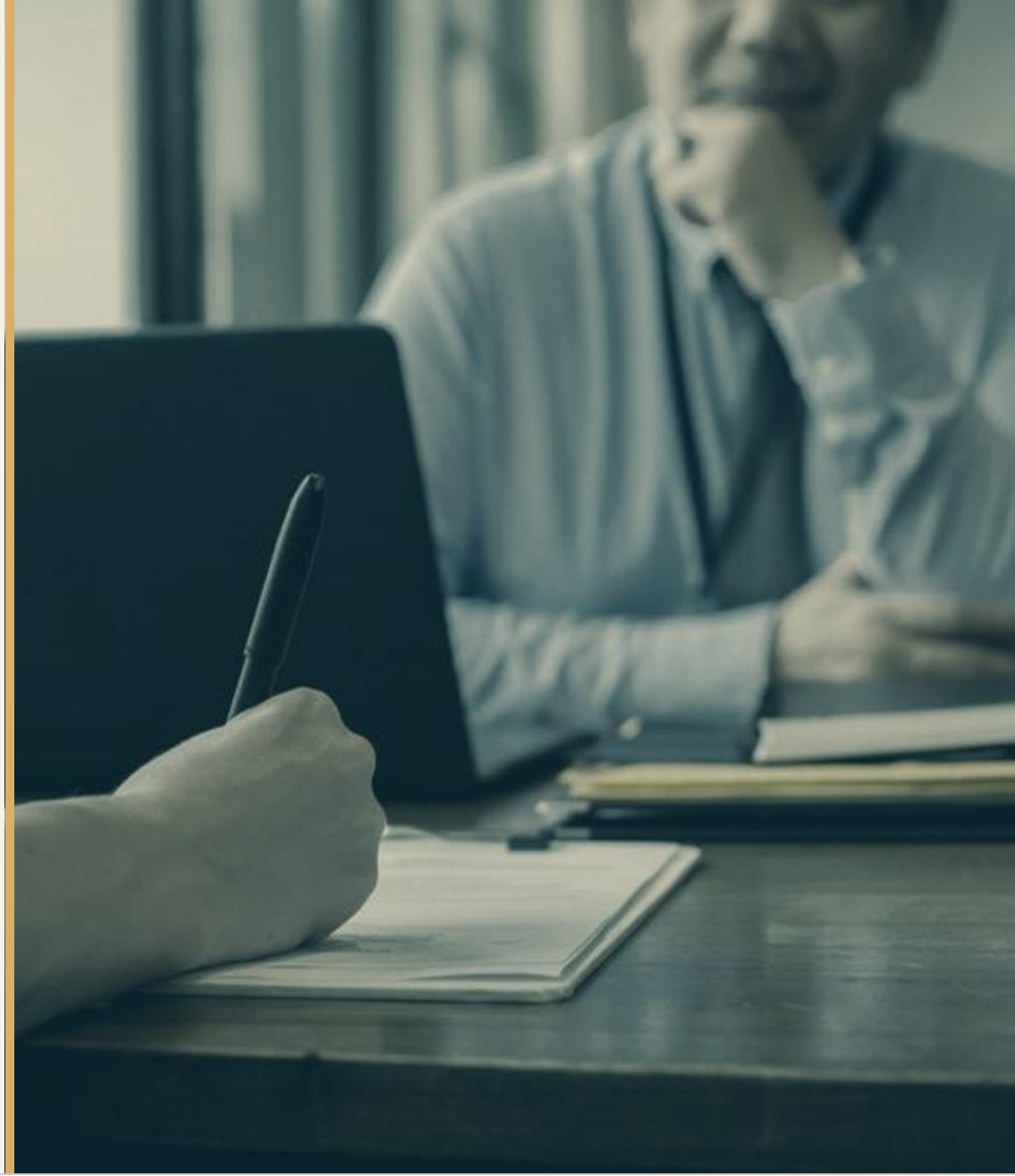
- After the arrest, the person is brought before the District Judge.

Transmission practice described by the Cypriot authorities interviewed

When the District Judge needs more information

- The Ministry emails the court’s request to the competent French authority.
- The reply returns by email and is printed for the hearing.
- Updates after hearings also pass through SIRENE.

Framework Decision 2002/584/JHA, Art. 15(2)



European Investigation Orders

From an emailed request to evidence gathered in Cyprus



How an EIO reaches the executing authority

The incoming email

- The Ministry receives the scanned EIO and supporting documents.

The requested measure

- The Ministry forwards the email to the authority responsible for that measure.

The police unit

- Most requests reach the specialist office for EIOs and judicial assistance.

The specialist police office in Cyprus

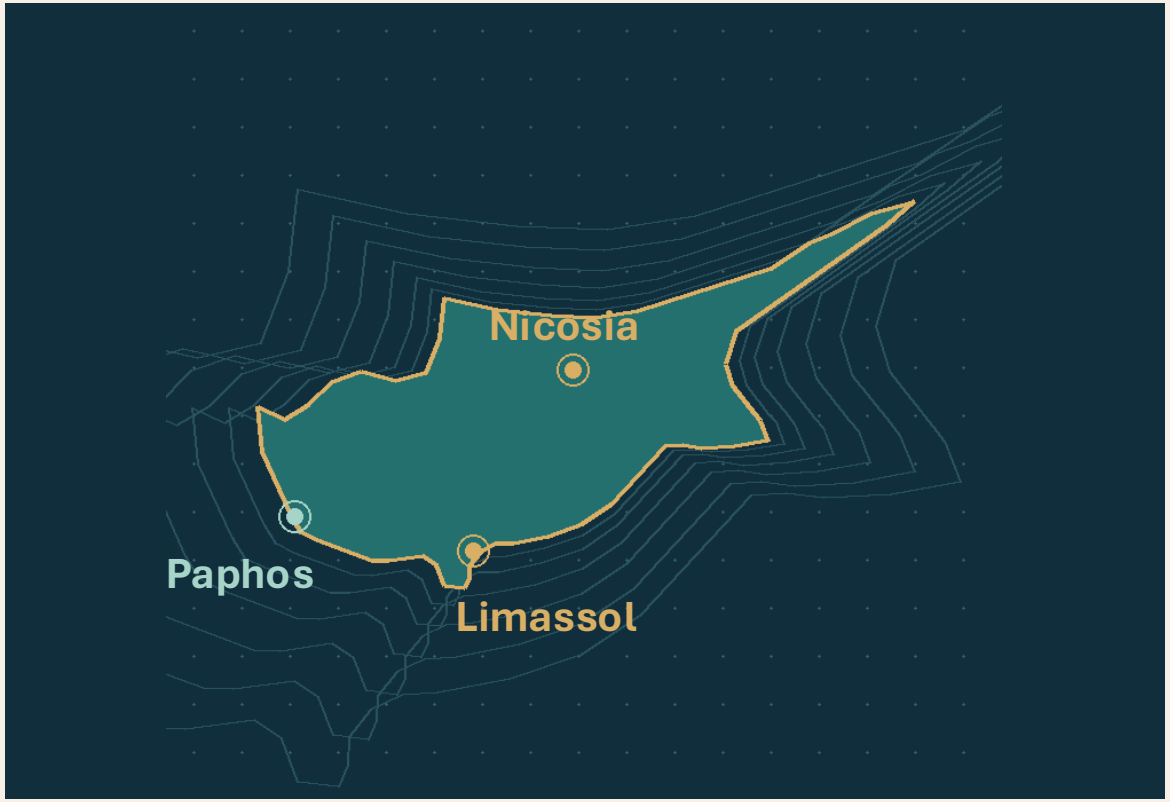
Office for Executing European Investigation Orders & Letters of Requests

Limassol office

- Covers Limassol and Paphos.

Nicosia office

- Covers the rest of the island.



What the 2024 evaluation found

Specialist officers	• The evaluators praised the dedicated police unit and its nationwide competence.
Banking information	• Police could use a central account database. Some banks still supplied paper records.
Physical evidence	• Bulky material could travel through diplomatic channels or secure post.

Council report 8637/24, pp. 14, 25, 40 and 50

e-EDES access and everyday practice

The 2024 position

- Authorities had received e-EDES training.
- Cyprus had yet to join the system.

The position reported to me

- Cypriot authorities now have access.
- EIOs are still routinely sent and received by email.

Council report 8637/24, pp. 25, 62 and 65; current practice reported by the speaker

The evaluators' recommendations

Regular training

- Provide joint EIO training, including CJEU case-law, for the authorities and practitioners involved.

Judicial training

- Provide urgent training for District Judges, with particular reference to their role as issuing authorities.

Secure exchanges

- Connect all competent national authorities to e-EDES as soon as possible.

Council report 8637/24, recommendations 3, 4 and 6, pp. 64–65

The legal framework for scrutiny

Issuing State

- Assesses necessity and proportionality.
- Hears challenges to the substantive reasons for issuing the EIO.

Executing State

- May consult the issuing authority.
- Retains safeguards governing execution and fundamental rights.

Directive 2014/41/EU, Arts. 6 and 9–14; Law 181(I)/2017, ss. 7 and 10–15

My experience of scrutiny in Cyprus

- Police pass the request to a judge through the warrant application.
- In the cases I encounter, I do not see a meaningful proportionality assessment at that stage.
- EIO-based applications can appear to receive more favourable treatment.



A German EIO for a house search in Limassol

- The Ministry receives the EIO and supporting documents by email.
- It emails the request to the specialised police unit.
- Police prepare an application to a District Judge for a search warrant.

Speaker's practical example of an incoming EIO



The request reaches a paper court process

Before the judge

- Police print the EIO and attach it to the paper application.

The search

- The judge issues a paper warrant, which police then execute.

Reporting back

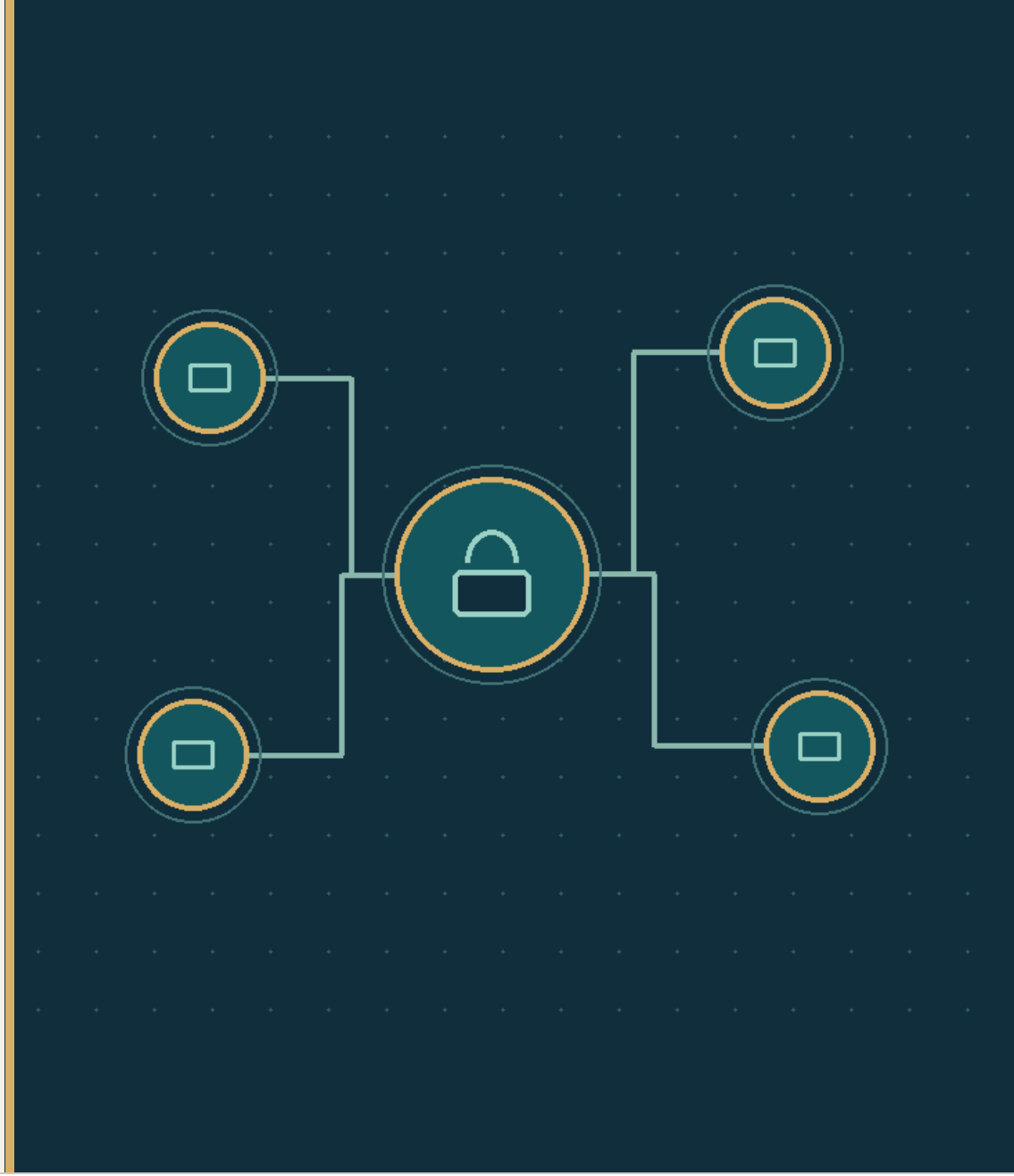
- The documents are scanned and returned to the Ministry for its execution report.

Speaker's account of the Cypriot execution procedure

Taking evidence by videoconference

- An EIO can arrange the examination of a witness or expert by video link.
- The framework also covers suspects and accused persons, subject to specific conditions.
- Digitalisation can concern the measure itself, as well as transmission of the request.

Directive 2014/41/EU, Art. 24; Law 181(I)/2017, s. 25



Freezing and confiscation orders

The route through MOKAS and the District Court of Nicosia



MOKAS receives and brings the request to court

Receipt by email

- MOKAS receives the certificate and supporting documents from the foreign authority.

Preparation on paper

- MOKAS prints the documents and prepares the court application.

Nicosia District Court

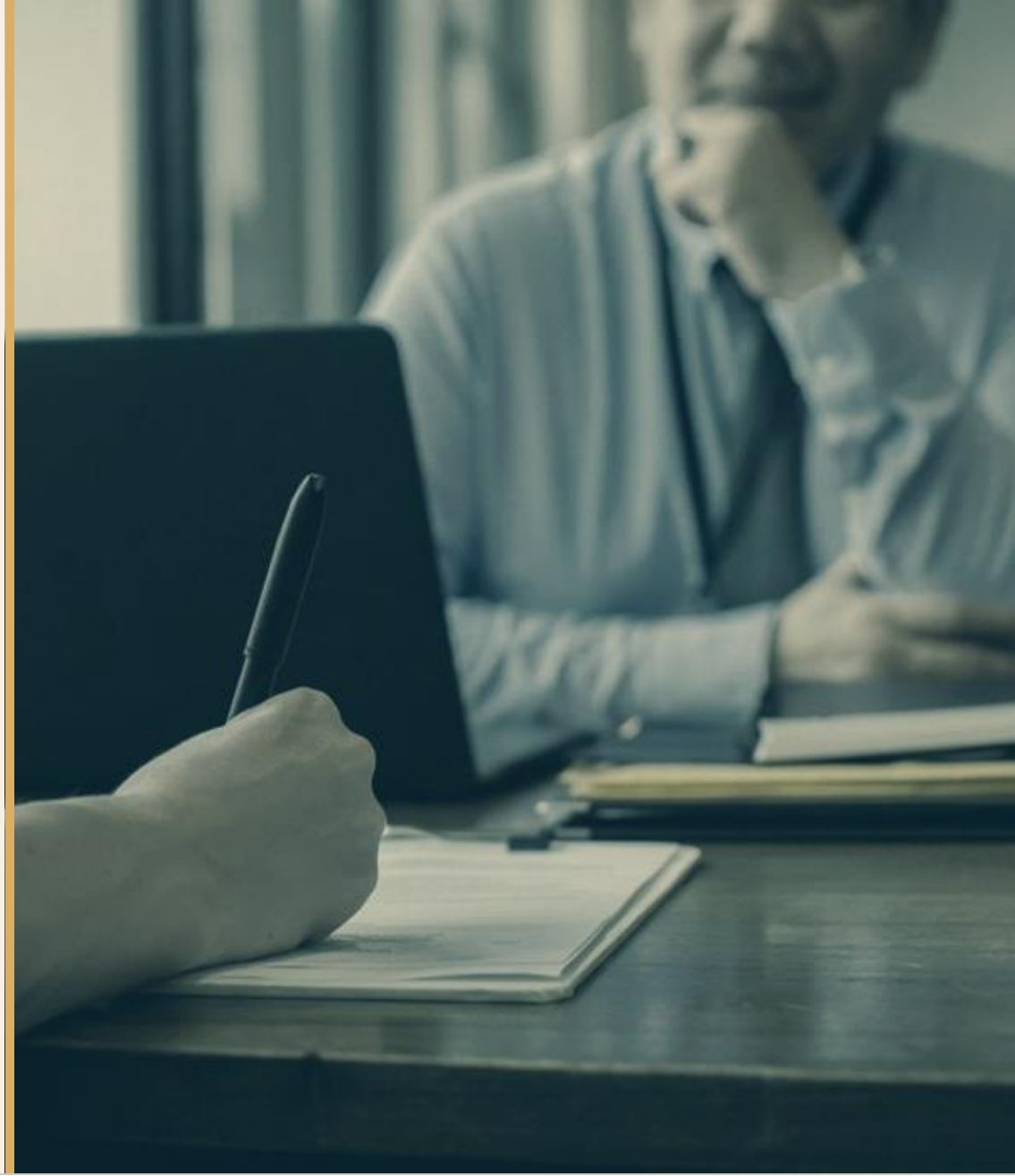
- The paper application goes before the President or a Senior District Judge of Nicosia District Court.

Regulation (EU) 2018/1805; Law 188(I)/2007, ss. 43IH and 43K.

After the court's decision

- MOKAS scans and transmits the decision to the appropriate authorities.
- Paper notification forms part of the practice described to me.
- The law also expressly permits electronic notification.

Law 188(I)/2007, s. 43KA(2)(γ); practice reported to the speaker



Where the digital process returns to paper

Cross-border exchange

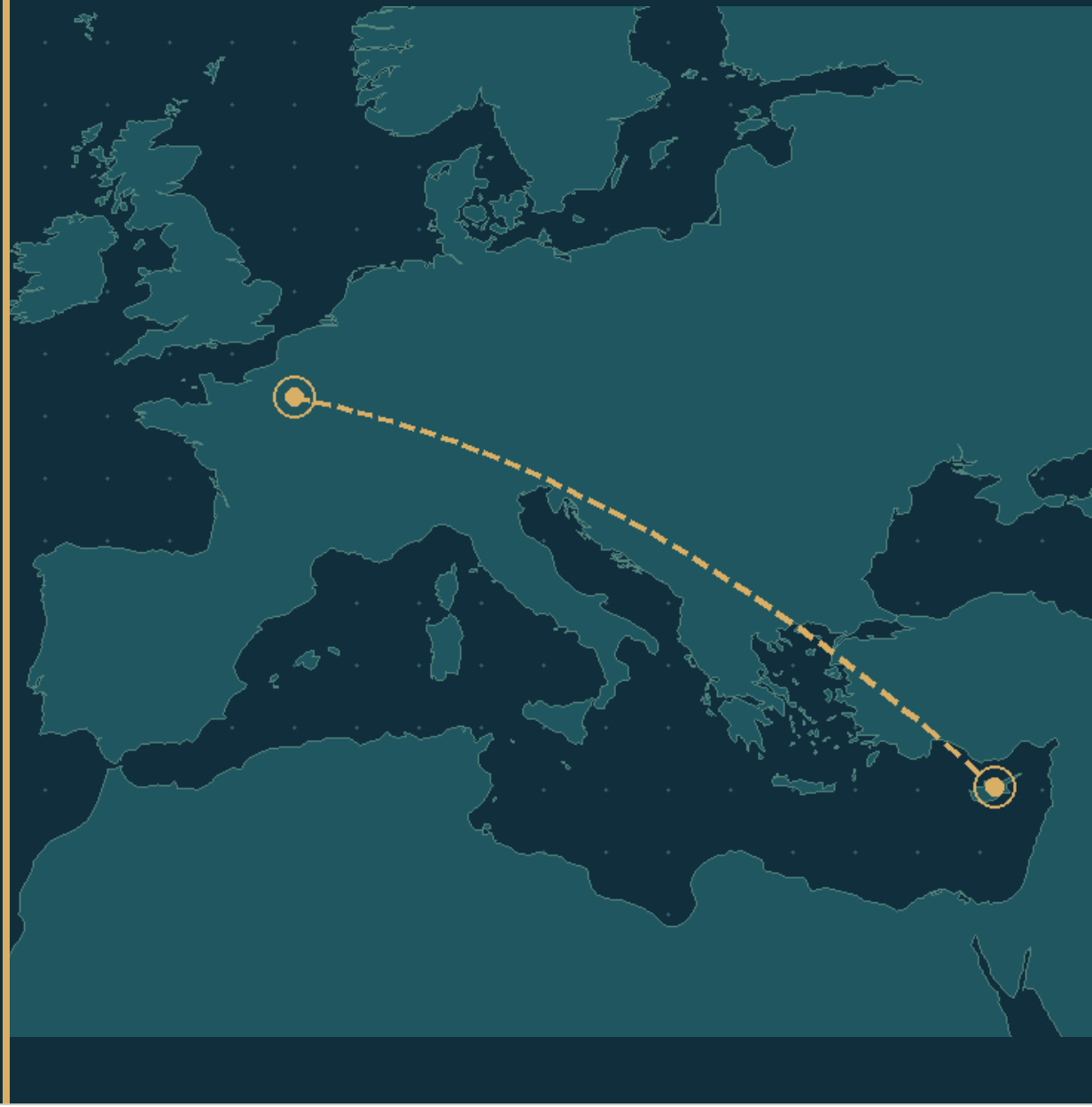
- The request arrives electronically and the result can be sent back electronically.

Domestic procedure

- In the practice described to me, applications, supporting material and notification still involve paper.

The European Public Prosecutor's Office

Electronic case management and national investigative steps



One EPPO with a decentralised structure

European Delegated Prosecutors

- Work at national level within a single EU prosecution office.

Cross-border assignments

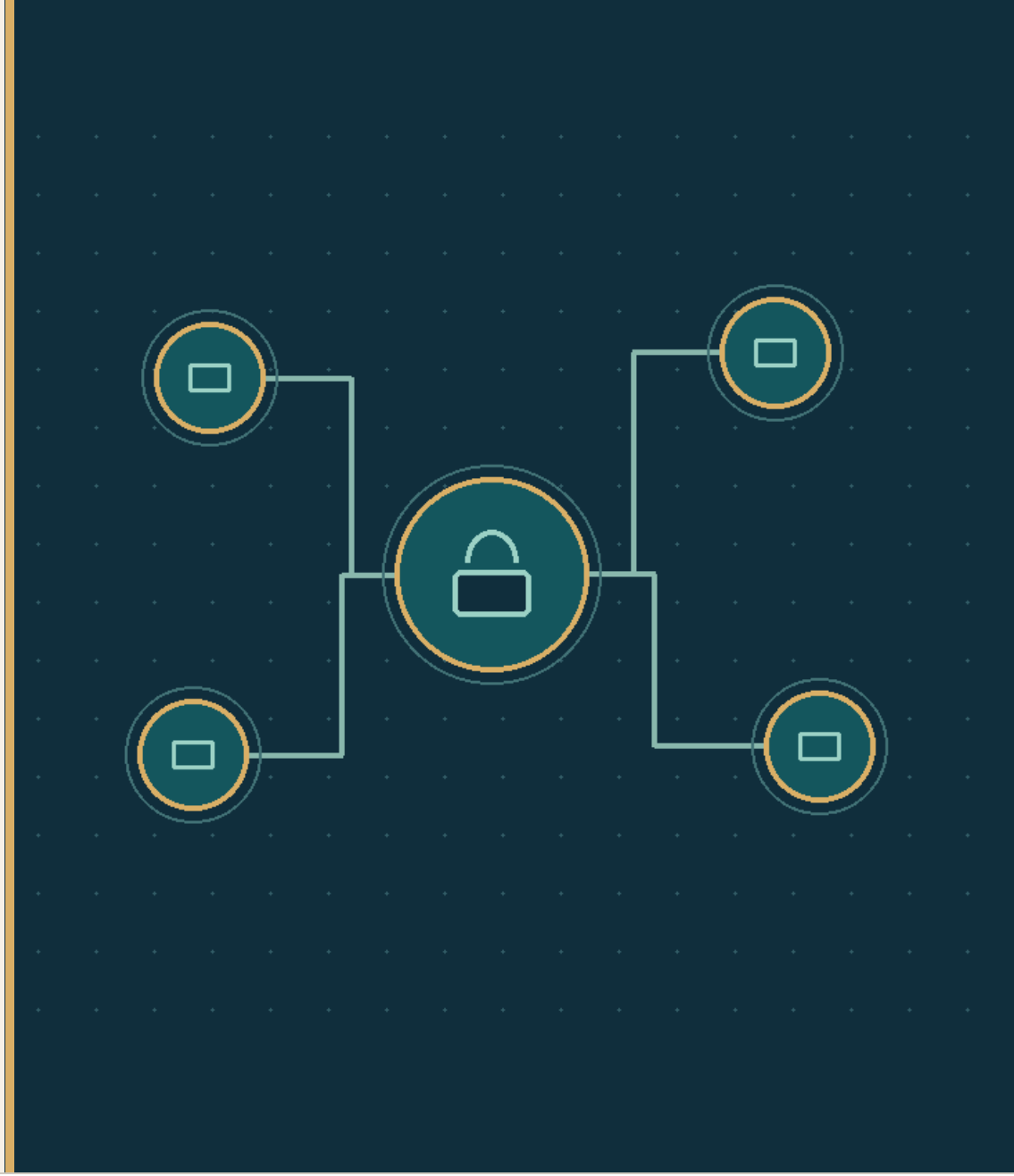
- The handling prosecutor assigns a measure to an assisting prosecutor.
- Execution requires the applicable national procedural steps.

Regulation (EU) 2017/1939, Arts. 8 and 31–32

The EPPO's own Case Management System

- The CMS supports investigations, internal workflows and secure access to case information.
- European Delegated Prosecutors in Cyprus carry out assigned investigative measures.
- Searches still require the procedural steps applicable in Cyprus.

Regulation (EU) 2017/1939, Arts. 31–32 and 44; EPPO Case Management System



A recent investigation involving Cyprus

€114m

estimated VAT losses

Investigation linked to Midas
EPPO announcement, 16 October 2026

- An EPPO investigation in Munich concerned suspected VAT fraud in smartphone sales.
- Searches and seizures took place in Cyprus.
- According to my information, the specialist police unit obtained and executed the search warrants.

EPPO, Investigation Midas, press release of 16 October 2026.

CONCLUDING THOUGHTS

Efficiency and judicial protection

Questions arising from practice in Cyprus



The next stage of digitalisation

What already works

- Authorities can exchange requests, information and results electronically.

What could improve

- Shared systems could improve continuity, security and file access, depending on permissions and implementation.

Efficient cooperation or effective scrutiny?



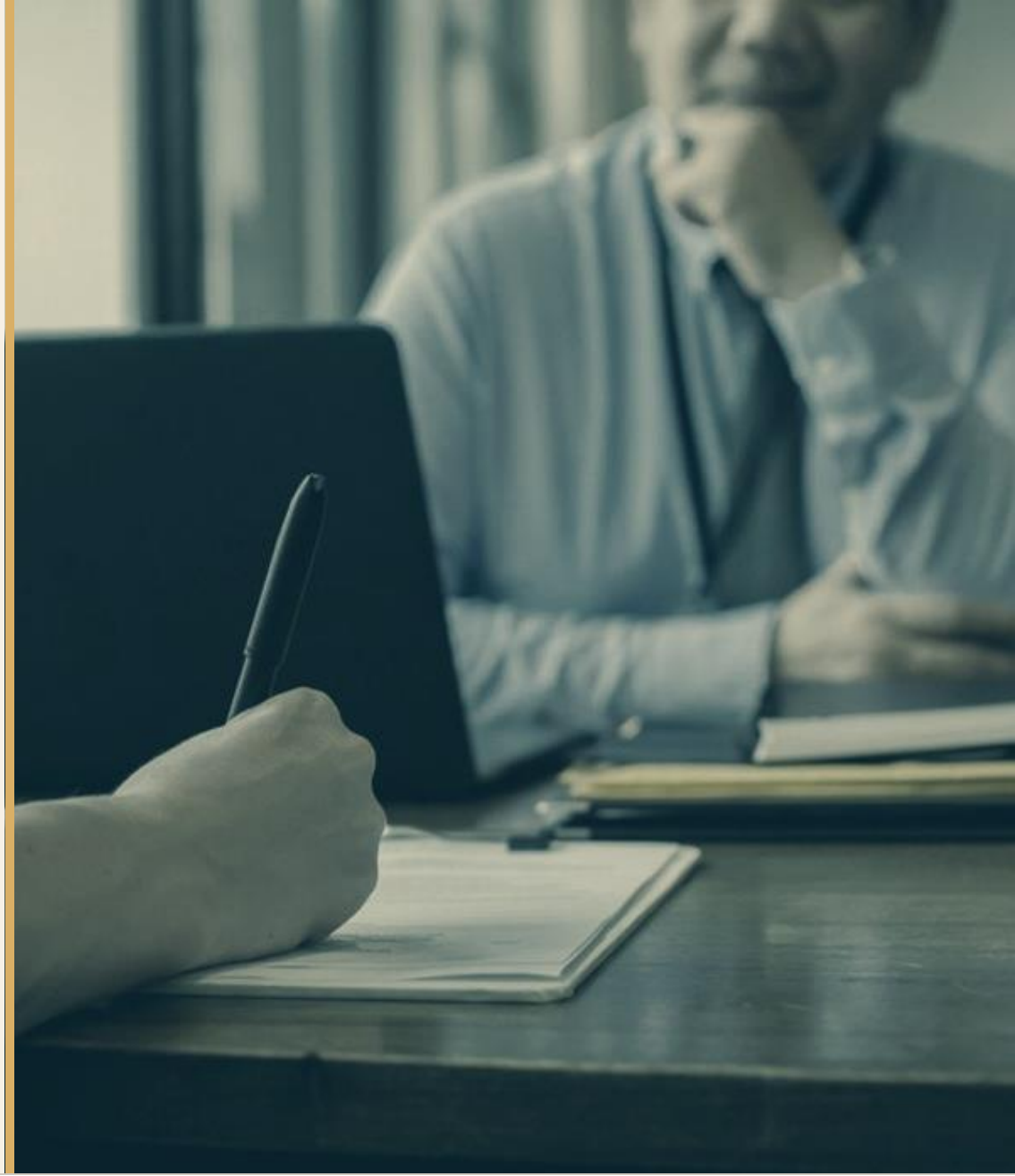
The evidential basis for a search warrant

- Police must explain the facts supporting a reasonable belief that evidence will be found at the premises.
- The judge must be able to assess that connection.
- A suspicion of fraud alone does not explain why evidence should be at a particular address.



A recent personal experience with an EIO

- The EIO sought a search of a client's home during a fraud investigation.
- In my assessment, it set out prosecutorial conclusions without the supporting facts.
- I challenged the resulting search warrant before the Supreme Court.



The court’s decision and my concern

The Supreme Court’s reasoning

- The EIO sufficiently described the client’s alleged role.
- The court referred to the foreign investigation.

My reading of the outcome

- The Court did not expressly adopt a lower legal threshold.
- My concern is the intensity of scrutiny applied in practice.

The speaker’s account of the judgment and its implications

Gavanozov II and effective remedies

- The issuing State must provide an effective remedy for the searches, seizures and video hearing covered by the case.
- An EIO cannot be issued where the necessary remedy against issuance is absent.
- Article 47 of the Charter requires effective judicial protection.

Gavanozov II, C-852/19, EU:C:2021:902, 11 November 2021, paras. 24–41 and operative part





Camille Renouard

The use of videoconferencing in criminal matters

Paris, 13 November 2026

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

Co-funded by the EU

Agenda

01 Historical Introduction

From exception to norm · 2001 - today

02 Legislative Framework

Art. 706-71 CCP · Procedural instability

03 EU & Constitutional Limits

ECHR · QPC 2026 decision

04 Advantages & Drawbacks

Overview

05 The CNB Position

Structured & constant criticism

06 The Cost-Driven Drift

Warning: systemic risk

07 Jurisprudence as Safeguard

CE 2020 · CC 2026

08 Conclusion

Key takeaways

09 Perspectives

What France needs · EU horizon

From Exception to Norm

2001 — First introduced as a strictly exceptional procedural tool - Law of 15 November 2001

2019 — Major reform: broader legislative authorisation - expanded to all stages: investigation, detention, trial, sentencing, enforcement

2020 — COVID-19 pandemic: near-total temporary generalisation; supreme courts immediately draw limits

2025 — Anti-narcotics law (loi narcotrafic) attempts to impose mandatory video-hearings for detained defendants in organised crime units

2026 — Constitutional Court strikes down the legislative provision - physical presence reaffirmed as a fundamental guarantee

From a derogatory tool to a structural feature of French criminal justice.

Article 706-71 CCP

Scope of Application

Covers all stages: investigation, pre-trial detention, trial (witnesses, experts, civil parties), appeal, enforcement of sentences.

Key Conditions

Requires: a judicial decision · technical guarantees (confidentiality, reliability) · consent of parties in some cases.

An Unstable Procedural Regime

Growing case law on nullities: mandatory prior notice to the defendant, sanctions for procedural irregularities, increasing litigation.

The Right to Refuse

Detained persons may oppose video-hearings in pre-trial detention matters — a key safeguard.

This right is limited where public order or escape risk is invoked.

QPC n° 2026-1192 — 10 April 2026

The Constitutional Court struck down the provision that denied detained persons any right to appear physically — finding it an excessive infringement of defence rights.

Abrogation postponed to 31 October 2027.

Physical presence is a fundamental guarantee.

An EU-Shaped Framework

EU Directive 2014/41

European Investigation Order

Enables cross-border video-hearings in criminal matters. Article 706-71 CCP expressly incorporates EU mechanisms: extradition, EIO, cross-border hearings.

ECHR - Article 6

Right to a Fair Trial

Case law requires that video-hearings do not undermine the right to be heard effectively. France must ensure equivalent procedural guarantees whether physical or remote.

Constitutional Protection

Conseil Constitutionnel

The Court has consistently held that video-hearings cannot disproportionately infringe defence rights - striking down provisions that limit the right to oppose or deny physical presence altogether.

European and constitutional courts serve as the ultimate check on the legislature's overreach.

Advantages & Drawbacks

Advantages

- Reduction of prisoner transfers - security & cost savings
- Faster scheduling of hearings
- Continuity of proceedings during crises

Drawbacks (the greater concern)

- Impaired communication between lawyer and client during proceedings
- Difficult choice for counsel: be at the court or beside the client?
- Loss of solemnity - the physical trial has an irreplaceable human dimension
- Technical biases: angle, framing and image quality distort the judge's perception
- Dehumanisation of justice - the accused becomes a face on a screen
- Undermines equality of arms and the oral adversarial process

The National Bar Council: A Structured & Constant Critique

The CNB does not oppose all use of video-hearings — but insists they remain a strictly limited exception, never a rule, and never a cost-cutting device.

1 No normalisation

The CNB opposes any automatic generalisation. Video-hearings must remain a strictly justified exception — not the default.

2 Defence of physical presence

Physical presence guarantees the solemnity of proceedings, the human assessment of the defendant, and the quality of oral argument.

3 Concrete risks to defence rights

Difficulty communicating with the client · Counsel forced to choose between court and client · Loss of effectiveness of pleadings · Breach of equality of arms.

4 Dehumanising effects

Technical biases (angle, framing, quality) alter the judge's perception. The accused becomes a face on a screen — isolated, diminished.

5 CNB's minimum requirements

Priority to physical presence · Video only when strictly necessary · Effective right to refuse · Confidential lawyer-client channel · Adequate technical conditions.

"Criminal justice cannot be reduced to a technical procedure. It rests on a human encounter between judge, lawyer and defendant." — CNB

The Cost-Driven Drift

Video-hearings are increasingly justified on budgetary and logistical grounds - not on the merits of individual cases.

Key Risks

- Systematic use without genuine justification in each case
- Erosion of the defendant's right to physical presence
- Gradual normalisation of a degraded form of justice for detained persons

CNB Reminder

- Video-hearings must remain the exception, never the rule
- Defendants must always retain a genuine and effective right to refuse
- Cost savings cannot override fundamental rights

The Constitutional Court has already sanctioned the legislator on this point — Decision n° 2026-1192 QPC.

The Judge as Guardian

When the legislature overreaches, courts push back.

Conseil d'Etat November 2020

Suspension of video-hearings in criminal trials

During the second COVID lockdown, the Conseil d'Etat suspended the ordinance extending video-hearings to the criminal trial phase - finding it a serious and manifestly unlawful breach of defence rights.

Before a cour d'assises, the severity of penalties and the role of intimate conviction of judges and jurors confer a specific place to oral debate. Physical presence during closing arguments and the defendant's last word are essential.

Conseil Constitutionnel April 2026

QPC n° 2026-1192 - Anti-narcotics law struck down

The provision would have made video-hearing mandatory for all detained persons in organised crime units - no possibility of appearing physically for the entire duration of pre-trial detention.

The Court held: the importance of the guarantee attached to physical appearance before the competent court renders such a blanket prohibition an excessive infringement of defence rights.

Both decisions confirm the same principle: videoconferencing is a tool in service of justice - not a substitute for it.

Key Takeaways

A Necessary but Limited Tool

- A legitimate option — not a substitute for physical presence
- Use must be individually justified, case by case

Fundamental Guarantees

- Right to oppose video-hearings in detention proceedings
- Confidential lawyer-client communication at all times
- Technical standards equivalent to a physical hearing

The Human Dimension

- Criminal justice rests on a human encounter: judge, lawyer, defendant
- No efficiency gain can justify its elimination

Justice is not a technical performance. It is a human encounter that the law must protect.

Perspectives

What France Needs

1

Mandatory advance notice

Defendants must be informed in writing before each hearing where a video-link is envisaged - with sufficient time to prepare.

2

Right to counsel at remote end

Defence counsel must have the option to be physically present at the location where their client testifies or appears.

3

Minimum technical standards

Clear procedural consequences for technical failures, including the possibility of nullity where audio or video quality impairs the effective exercise of defence rights

The EU Horizon

No unified EU standard yet

Member States apply ECHR Article 6 differently. There is no binding EU directive setting minimum technical or procedural standards for video-hearings in criminal proceedings.

Defining minimum safeguards rights

Physical appearance before the court should remain the default model. Common standards could include prior information of the accused, confidential lawyer-client communication, minimum quality technical requirements.

The role of defence lawyers

CCBE, national bars and legal practitioners across Europe are increasingly advocating for common safeguards to ensure that digital criminal proceedings fully respect defence rights

The future challenge lies not in establishing whether criminal hearings can be conducted remotely, but in ensuring that remote participation never diminishes the right to a fair trial or the rights of the defence.



Adrian Hărătău

National experience on digitalisation of EU criminal law instruments in Romania

Paris, 13 November 2026

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

Co-funded by the EU

The plan of the presentation

I	**The Romanian framework and practice**	*Law No 302/2004 · e-CODEX*
II	**The investigation order from the defence side**	*Articles 330–331 of Law No 302/2004*
	Legal remedies	*Issuing State and executing State*
	Access to electronic evidence	*The Code · EncroChat § 131*
III	**Hearing by videoconference**	*Three regimes, three texts*
IV	**Production and Preservation Orders**	*Regulation 2023/1543*
	Electronic transmission	*Regulation 2023/2844 · alternative means*
§	**Conclusions**	*What the law allows and what is applied*

PART I

Before the recent European regulations

The Romanian Framework

I

The legal basis for electronic transmission, one documented case, and the state of the infrastructure.

Requests are executed under Romanian criminal procedure

I

Requests addressed to the Romanian authorities in the fields governed by this law shall be carried out in accordance with the Romanian rules of criminal procedure, unless this law provides otherwise.

Article 7, Law No 302/2004 (unofficial translation)

WHAT THE LAW ALREADY PROVIDES

1. European arrest warrant, Art. 90(2): sent “by fax, e-mail or any secure means of communication that leaves a written record”.

2. Article 7: a rule that is often forgotten. Acts of execution in Romania are verified under Romanian rules.

A DOCUMENTED EXAMPLE

An investigation order from Bordeaux, executed in Romania

I

From the search to the Constitutional Court

11 Feb 2025 — Searches in Bacău and Satu Mare; devices and storage media seized. French case: bank cards cloned and used at petrol stations.

6 Oct 2026 — Constitutional Court: Art. 159(13) of the Code is constitutional only if “suspicion” means “reasonable suspicion”.

WHAT THE DEFENCE CHECKS

— The search was carried out under the Romanian Code of Criminal Procedure.

— The search warrant, the seizure of objects and the search report are verified under Romanian rules.

— Seizure of objects under Article 159(13): “suspicion” must mean “reasonable suspicion”.

The “electronic file” and e-CODEX: where Romania is today

THE “ELECTRONIC FILE” TODAY

— Two services: the courts' portal (public information) and consultation of documents (right of access needed).

— Law No 304/2022 keeps the file on paper; Article 15 provides for a National Electronic File.

— Access by CNP, the personal identification number: Romanian citizens or their lawyers.

— A foreign lawyer without a CNP is not excluded, but access must be organised in advance.

e-CODEX AT THE END OF 2025

— Source: the Ministry of Justice's activity report for 2025.

— 2025: conformity tests, needed to install and configure the infrastructure.

— Priority for the next period: making the system operational.

— The Ministry's connection point to the network was not working.

The procedure is verified on the documents in the file, not on press communications.

PART II

From the transmission of documents to the gathering of evidence

The European Investigation Order

II

A tool for the defence too · where to contest it · how to get access to the electronic evidence.

The investigation order is also available to the defence

> *… the European Investigation Order shall be issued … on their own initiative or at the request of the parties or of the main procedural subjects …*

Article 330(1), Law No 302/2004 (unofficial translation, excerpt)

WHAT THE TEXT MEANS

1. "At the request of the parties or of the main procedural subjects": so also at the request of the suspect.
2. The defence can ask for evidence located in another Member State.
3. It does not have to wait for the prosecutor to take the initiative.

AN EXAMPLE

Twenty messages from a three-month conversation

II

PRECISE AND REASONED

✓ The defence asks for the rest of the conversation.

✓ The period is defined.

✓ The reason is given: the context could change the meaning of the selected messages.

✓ The authority can evaluate it, and cannot easily refuse it without explanation.

GENERAL REQUEST

✗ “All the client's data held by the foreign authorities.”

✗ No link with the accusation is shown.

✗ Necessity and proportionality are not met.

✗ It will be refused.

The same conditions also work against our client

a

Necessary and proportionate

Assessed in each case by the issuing authority

In relation to the purpose of the criminal proceedings, taking into account the rights of the suspect or accused person.

b

Possible in a national case

The same conditions

The measure could be ordered under the same conditions in a similar national case.

Was it necessary? Would the same measure be permitted in an ordinary national case?

“A prosecutor signed it, so it is null” is an incomplete argument

HP · Case C-724/19

16 December 2021

— The order was for obtaining traffic and location data.

— In a national case, only a judge could order the measure.

— Decision: the prosecutor could not issue that order.

— Recognition by the executing State does not repair the lack of competence.

EncroChat · Case C-670/22

30 April 2024

— The French authorities already held the data.

— The order was for their transmission.

— Decision: a prosecutor may issue it if competent to order transmission in a comparable national situation.

Obtaining data, or transmitting data already obtained: the answer to “who can sign?” is different.

II

Where do we contest the order?

1 EXECUTION

In the executing State

— Contested under the rules of that State.

— In Romania: the legal remedies of the Code, same conditions, same time limits (Art. 338(1)).

2 ISSUING

In the issuing State

— The reasons of substance may be contested only before the issuing authority (Art. 338(2)).

— Without a colleague there, the argument never arrives at the competent authority.

3 SUSPENSION

Not automatic

— Contesting does not suspend the measure or the transfer (Art. 338(3)).

— Transfer may be suspended (Art. 337(2)); it must be if it would cause “serious and irreversible damage”.

The person who asks for suspension must describe the damage. Invoking confidentiality is not enough.

II

Two reference points and one open question

C-852/19

Gavanozov II · 11 November 2021

No legal remedy in the issuing State against orders for searches, seizures and the hearing of a witness by videoconference: the directive and Article 47 of the Charter do not permit such an order to be issued.

Art. 351

Notification of interception · Law No 302/2004 (Article 31 of the directive)

A State intercepting a person on Romanian territory, without Romanian technical assistance, must notify Romania. The Prosecutor's Office attached to the High Court replies within 96 hours. Ask to see the notification and the reply.

C-625/25

Prudniez · not yet decided · question from the French Cour de cassation

Must the executing State give a legal remedy to a person against whom the evidence is used in the issuing State? Does equivalence require it? Opinion of the Advocate General: 19 November 2026.

Article 338(1) gives the legal remedies of the Code "under the same conditions", but does not say who may use them when the person is judged in another State.

Evidence rarely arrives in the form in which it was collected

II

WHAT THE FILE RECEIVES

— A PDF with fragments of conversation.

— A table of names and telephone numbers.

— A note by the investigators explaining where the data come from.

WHAT THE DEFENCE MAY NOT HAVE

— The conversation from which the messages were extracted.

— Whether the translation corresponds to the original.

— The data that attribute the account to a particular person.

— The explanation of the selection: why these messages and not the others.

Article 94(2) of the Code: study the documents, note data, obtain photocopies. The request must show exactly what is absent.

Refusal, integrity, prior control

Art. 95

Complaint against a refusal to allow consultation

The superior prosecutor decides and communicates, with reasons, within 48 hours. Say what access was refused and what defence cannot be prepared.

Art. 168

Integrity of the material

A computer search must use means “capable of ensuring the integrity of the information”. Ask for the source of the data, the operations carried out, the copies, the conversions.

Hash

What a hash value shows

A hash is a digital fingerprint of a file. It shows whether two files are identical. It does not show who wrote the message, or whether the data were obtained legally.

C-548/21

Landeck · 4 October 2024

Access to data on a telephone: prior control by a court or an independent authority, except in justified cases of urgency.

II

When the material cannot be checked but decides the case

> *… not in a position to comment effectively … likely to have a preponderant influence on the findings of fact.*

CJEU, M.N. (EncroChat), C-670/22, 30 April 2024, paragraph 131 (excerpt)

TWO CONDITIONS, THEN ONE MORE STEP

1. Why the client cannot effectively contest the evidence: which verifications are impossible, and for what reason.
2. How much the accusation depends on that material.
3. Exclusion must be physical (Art. 102(3) of the Code; Constitutional Court Decision No 22/2018), in the electronic file too.

A reference to the judgment without these two analyses is a quotation, not an argument.

PART III

From the evidence to the person

Hearing by Videoconference

III

Each procedure has its own rule on consent and on the presence of the lawyer.

III

Which procedure are we in?

1 ROMANIAN TRIAL

Article 364(1) of the Code

— Accused deprived of liberty, at the place of detention.

— With consent, lawyer present.

— Art. 106: detained persons, exceptional cases only.

— Art. 597(2), court for the execution of sentences: consent no longer required.

2 INVESTIGATION ORDER

Article 345, Law No 302/2004

— Witnesses and experts; also suspects and accused persons.

— Refusal possible: no consent, or contrary to fundamental principles of Romanian law.

— Bissilli, C-325/24.

3 REG. 2023/2844

Article 6, since 1 May 2025

— Six instruments. The EIO is not on the list.

— A lawyer's advice before consent.

— Confidential lawyer–client communication.

Article 364(1) does not permit an accused person who is free to participate at a distance.

III

A recent judgment answers an old question

THE CONTEXT

Article 345 of Law No 302/2004: hearing by videoconference at the request of another State.

Two specific grounds for refusal: the suspect or accused person does not consent, or the measure is contrary to the fundamental principles of Romanian law.

Bissilli: a person detained in Belgium was to be heard in a trial in Italy.

THE COURT DECIDED

1. An EIO may be issued to hear the accused person during the trial as well.

2. Condition: the purpose is to obtain evidence, and nothing more than is necessary for that.

3. No refusal only because the measure is not possible in a similar national case; another ground in the directive remains possible.

The order cannot be the basis for participation at a distance in the entire trial.

Consent after legal advice, and a confidential channel

III

Scope

Six instruments, not the EIO

European arrest warrant · transfer of the enforcement of sentences · probation · supervision measures · European protection order · freezing or confiscation.

Art. 6(2)

Consent

First, the possibility to ask for the advice of a lawyer (Directive 2013/48/EU). Consent is voluntary and unequivocal; the requesting authority verifies it before the hearing starts.

Exception

Serious threats to public security or public health

The absence of a room or of an escort is not such a threat.

Art. 6(5)

Confidentiality

Communication between the person and the lawyer is confidential before and during the hearing, in accordance with national law.

A box marked on a form does not prove confidentiality

III

ROMANIA'S NOTIFICATION ON e-JUSTICE

— The courts use a platform that integrates Zoom, Teams and other applications.

— On confidentiality, one sentence: communication with the lawyer is possible, in conditions of confidentiality.

— It does not say how.

THREE POINTS TO HAVE RECORDED

1. **Where the lawyer is located.**
2. **How a pause for a confidential consultation is requested.**
3. **Through which channel the consultation takes place.**

During the hearing: say what could not be heard or seen; ask for it to be recorded and corrected and, if necessary, for an interruption.

PART IV

Regulation 2023/1543, applicable since 18 August 2026

Orders Addressed to Providers

IV

European Production Orders and European Preservation Orders · electronic transmission and alternative means.

IV

From a prosecutor in Lyon to an account used in Bucharest

Lyon

The prosecutor: issuing authority

For the content of the messages, a judge is necessary.

certificate: subscriber data of the account →

← *reply within 10 days · 8 hours in emergencies*

The provider

Its European representative, in another Member State

The "enforcing State" is where this representative is established, not the client's State. Its notification depends on the category of data.

information, in principle from the issuing authority; it may be delayed ↓

Bucharest

The client, and the Romanian authorities

Who in Romania knows about this order? Perhaps nobody.

Articles 8, 10 and 13, Regulation 2023/1543

IV

Four questions for the defence

ARTICLE 4

Who signed, and for what data?

Subscriber and user-identification data: a prosecutor too. Other traffic data and content: a judge. Look at the data actually requested.

ARTICLE 5

Why these data, why this period?

Necessity, proportionality, a similar national order possible. Traffic and content: a maximum penalty of at least three years, or listed offences. The reasons are not in the certificate.

ARTICLES 8 AND 13

Who was informed?

Traffic and content: the enforcing authority is notified. The person is informed by the issuing authority; a delay needs reasons recorded in the file.

ARTICLES 5(9), 10(5), 12(1)(a)

Is professional secrecy involved?

A lawyer's account, or a client's correspondence with a lawyer: the regulation intervenes at three moments.

The regulation intervenes at three moments

Art. 5(9)

Issuing the order

Data stored on an infrastructure provided to professionals bound by professional secrecy (a law firm's e-mail service): a traffic or content order only if the professional resides in the issuing State, if contacting them could damage the investigation, or if the secrecy has been lifted. Otherwise: the EIO.

Art. 10(5)

Execution by the provider

The provider informs the issuing and enforcing authorities if the data could be protected. It decides “based solely on the information contained in the EPOC” (the certificate).

Art. 12(1)(a)

Control by the enforcing State

Where it has been notified (traffic and content data), the enforcing authority may refuse execution because the data are protected by immunities or privileges.

A letter that tells the provider in advance which accounts contain lawyer–client communications creates no obligation, but leaves a written trace.

IV

Not only a risk: preservation as a tool for the defence

PRESERVATION ORDER

The provider must not delete the data. Nobody gets access to content.

ONE EXTENSION

Thirty more days.



Day 0 **Day 60** **Day 90**

ARTICLE 1(2)

An order may also be requested by a suspect or an accused person, or by a lawyer acting for that person.

If the data can help the client and may disappear, the defence asks for preservation immediately, not only at trial.

What is Romania doing? The position on 8 November 2026

IV

Two laws, at different stages

- **8 Jun 2026** — Senate adopts the draft law implementing the regulation (PL-x 467/2026).
- **18 Aug 2026** — The regulation applies. The directive's deadline for providers to designate an establishment or representative.
- **6 Oct 2026** — Favourable report of the Legal Committee, Chamber of Deputies. Final vote not yet held.
- **21 Oct 2026** — Senate adopts the law on designated establishments (Directive 2023/1544). Sent for promulgation.

ARTICLE 18 · THE REMEDY

— Before a court of the issuing State.

— Legality, necessity and proportionality of the order.

— A German order is contested in Germany, with a German colleague.

Providers already active have six more months to designate a representative: for a time, an order to a Romanian provider may have nobody designated to receive it.

IV

Three days to submit the challenge

FRIDAY	SATURDAY	SUNDAY	MONDAY	TUESDAY
informed not counted	**1**	**2**	**3**	**last day** to submit the challenge

THE CHALLENGE

Submitted to the issuing authority within three days of receiving the information; the first day and the last day are not counted. It does not suspend execution.

THE DECISION

Within five days. This is a limit for the court, not a guaranteed period for writing the reasons.

THE REASONS

Until the date fixed for the decision on the challenge, Article 425¹(3) of the Code: submit in time, give the reasons later.

IV

Two regulations, two calendars

The dates

- **1 May 2025** — Regulation 2023/2844 applies. The videoconferencing rules in Article 6 already apply.
- **28 Jul 2025** — System specifications for orders to providers adopted (Regulation 2025/1550).
- **16 Jan 2026** — Implementing Regulation 2026/101 published: arrest warrant, investigation order, Regulation 2018/1805.
- **18 Aug 2026** — Regulation 2023/1543 applies; the obligation to use the system is already in force.
- **1 Mar 2028** — Obligatory communication through the decentralised IT system, for procedures started from that date.

FOR THE DEFENCE

— The European electronic access point (Article 4) covers civil and commercial procedures only.

— A lawyer's access to the criminal case file is still governed by national procedural law.

— No public source that I found shows whether the Romanian authorities are really connected.

IV

What happens when the system cannot be used?

THE RULE · ARTICLE 19(5)–(6), REG. 2023/1543

— Transmission “by the most appropriate alternative means”.

— Requirements of speed, security and authenticity.

— The transmission is recorded in the system without delay.

— Evidence over 25 megabytes goes by alternative means (Regulation 2025/1550, annex, point 3.2).

FOUR QUESTIONS FOR THE DEFENCE

1. **What prevented the use of the system?**
2. **Which channel was used?**
3. **How is reception proved?**
4. **Where is the transmission recorded?**

A file is not illegal because it came through another channel, and not inadmissible only because it is electronic (Article 8, Reg. 2023/2844).

What the law allows and what is actually applied

In force

Legal bases

For electronic transmission and for videoconferencing.

Applicable

Regulation 2023/1543

Directly applicable to orders addressed to providers, since 18 August 2026.

Pending

One law and one draft law

One law waiting for promulgation; one draft law in the Chamber of Deputies.

Not yet

The system and the practice

The e-CODEX connection of the Ministry of Justice was not working at the end of 2025. Practice under Regulation 2023/1543 is not yet publicly documented.

CLOSING

Speed says nothing about legality.

Nor about the defence's ability to check the evidence. That is where we will see whether digitalisation serves the defence too, and not only the authorities.

1

In each case

Legality and verifiability are examined case by case.

2

On the documents

What was received, when, from whom, with which annexes.

3

In time

Transformed into reasoned requests before it is too late.

Thank you.

Adrian Hărătău · Lawyer · Trainer at INPPA · adrian@haratau.ro



Clotilde Lepetit

Fundamental Rights and Professional Ethics of the Lawyer in the Face of the Digitalisation of Criminal Procedure

Paris, 13 November 2026

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

Co-funded by the EU

Same fundamental rights, new technological environment

Digitalisation changes how procedure works, not the level of protection

European Convention on Human Rights	EU Charter of Fundamental Rights
• Art. 6: fair trial • Art. 8: private life and correspondence	• Arts 7 and 8: private life, communications, personal data • Arts 47 and 48: effective remedy, fair trial, presumption of innocence, rights of defence

One phone: a hand-held object, years of private life

Communications	Photos	Locations	Contacts
Finances	Health data	Lawyer–client exchanges	

The challenge: making existing rights effective in a radically different technological environment.



01

Acquiring digital evidence

Fundamental rights as a limit on investigative powers

Retention: no general data hoarding for future use

Even before any investigation, Arts 7 and 8 of the Charter apply to the very existence of the data

CJEU · GRAND CHAMBER

C-140/20

Commissioner of An Garda Síochána and others

5 April 2022

QUESTION

Irish murder trial: traffic and location data were admitted as evidence. May a State impose general retention of communications data to fight serious crime?

HOLDING

EU law precludes general and indiscriminate retention of traffic and location data for the purpose of combating serious crime.

DEFENCE ANGLE

Ask not only how the evidence was obtained, but why the data still existed and under which legal framework it was retained.

The possible usefulness of data to a future investigation does not justify its general retention.

Access to data: proportionality and independent control

Retention and access are two distinct interferences, each requiring its own justification

CJEU · GRAND CHAMBER

C-746/18

H.K. v Prokuratuur

2 March 2021

CONTEXT

Estonian criminal proceedings: conviction based on electronic communications data. Under what conditions may authorities access traffic and location data?

HOLDING 1: SERIOUSNESS

Metadata can be a serious interference (Arts 7–8 Charter). Where it allows precise conclusions on private life, access is limited to serious crime or serious threats to public security.

HOLDING 2: WHO DECIDES

Prior review must be carried out by a court or an independent administrative body. The Estonian public prosecutor lacked the necessary independence.

Two lines of control for the defence: the scope of the access, and the independence of the authority that authorised it.

Seizing a device is not exploiting all of its data

Proportionality must extend from physical seizure to the extraction and use of the data

FRENCH COURT OF CASSATION

Crim. 5 March 2024

Appeal No. 23-80.229

HOLDING

Validates the filing in the case file of data extracted from a phone and selected by keywords directly related to the facts under investigation.

WHY IT MATTERS

Computer processing becomes legally relevant: the keyword defines the perimeter of data that may enter the proceedings.

NEW QUESTIONS FOR THE DEFENCE

- Which keywords were used?
- Which period was covered?
- Which accounts were queried?
- Which file categories were included?
- Was the whole device searched?
- Is irrelevant data still retained?
- Can the defence discuss the search method?

Seizure meets lawyer–client confidentiality

Protection must be organised at the filtering stage, before protected content is read

Saber v Norway

ECtHR · 17 December 2020

Smartphone seized and copied; it held exchanges between the applicant and his lawyers. Violation of Art. 8: insufficient safeguards to protect and filter privileged data.

Wieser and Bicos Beteiligungen v Austria

ECtHR · 16 October 2007

Search and copy of data on a law firm's computer system. Violation of Art. 8: the safeguards applied to paper documents were not properly reproduced for electronic data.

A guarantee cannot vanish because information changes medium. Digital volume and sensitivity may call for more safeguards: a true procedural architecture of confidentiality, applied before investigators read protected content.



02

The digital criminal trial

The defence must be able to understand, exploit and challenge the evidence

From formal access to effective access to data

Sigurður Einarsson and Others v Iceland: four stages that the Court clearly distinguishes

Data initially collected → **Information flagged as potentially relevant** → **Items placed in the investigation file** → **Items actually produced at trial**

ECTHR · 4 JUNE 2019

Banking-crisis prosecutions. Massive data volumes were searched by keywords with the Clearwell e-discovery tool; applicants alleged insufficient access to the data and no real part in the digital filtering (Art. 6 §§ 1 and 3(b)).

HOLDING

No violation on the facts. But Art. 6 requires the defence to have, in practice, the time and facilities needed to prepare its case; equality of arms does not require identical technology.

Raw hard drives for the defence versus indexing, cross-searching and chronology tools for the prosecution: equality of arms takes on a new dimension.

Yüksel Yalçınkaya v Türkiye: challenging e-evidence

The Grand Chamber's central judgment on determinative electronic evidence

ECTHR · GRAND CHAMBER

No. 15669/20

Yüksel Yalçınkaya v Türkiye

26 September 2023

FACTS

Conviction for membership of an armed terrorist organisation, largely based on use of the encrypted messaging app ByLock. Violations of Art. 6 § 1 and Art. 7.

PRINCIPLE 1

The electronic nature of evidence does not justify a lower standard of protection; technical complexity cannot be held against the defence.

PRINCIPLE 2

Where the defence cannot directly examine raw data or test its integrity and reliability, national courts must apply particularly rigorous scrutiny.

The less direct technical control the defence has, the more demanding judicial control must be, especially when electronic evidence is decisive.

The adversarial principle must reach the process

Digital evidence: the defence must be able to question how the evidence was produced

How was this conversation found?	In which mass of data?	With which keywords?
Which software ran the search?	Which data was excluded?	Was the data transformed?
Does source data still exist?	Can the defence reproduce the search?	Do technical logs record each operation?

From the result back to the process that produced it: the adversarial principle must cover not only the evidence but also its chain of transformation.

Iceland: selecting relevant data within a mass. Yalçınkaya: integrity and reliability of the underlying data.

Digital evidence cannot become automatic guilt

Yüksel Yalçınkaya v Türkiye, Art. 7: from technical fact to criminal qualification

ART. 7 ECHR

National courts attached decisive weight to ByLock use. The Court found that this led, in practice, to largely automatic criminal liability, without sufficient individualisation of the constituent elements of the offence.

A piece of data may prove a technical fact, but a gap always remains between technical data and criminal qualification.

LEGAL REASONING MUST FILL THE GAP

Intent	Knowledge
Concrete conduct	Context
Alternative explanations	Constituent elements

Digital evidence may help establish a fact. It must never automate guilt, a point that gains weight with automated tools and artificial intelligence.

Irregularly obtained evidence: no automatic exclusion

European law lays down no general rule of automatic exclusion

CJEU

C-310/16

Dzivev and Others

17 January 2019

CONTEXT

Telephone interceptions, some of them authorised by a court that was not competent to authorise them.

PRINCIPLE

A collection irregularity should not be turned into an automatic, undifferentiated response.

FIVE DISTINCT QUESTIONS FOR THE LAWYER

1. Was the measure used to obtain the data lawful?
2. Is the data itself still technically reliable?
3. Can it be admitted under applicable national rules?
4. Could the defence effectively challenge it?
5. Does its use affect the overall fairness of the trial?

Videoconference and effective participation

Marcello Viola v Italy: the unavoidable starting point; the topic was covered in depth this morning

ECTHR

Marcello Viola v Italy

5 October 2006

CONTEXT

Applicant attended hearings by videoconference in organised-crime proceedings.

HOLDING

Not in itself incompatible with the Convention, but it must pursue a legitimate aim and its practical arrangements must respect fair-trial and defence rights.

WHAT THE COURT LOOKS FOR

Following the proceedings effectively	Being heard in satisfactory conditions
Communicating effectively with counsel	Communicating confidentially with counsel

Fundamental rights across the whole data lifecycle

The capacity to collect must never become, by itself, the justification for collecting

Retention	Access	Seizure	Filtering	Trial evidence	Presence
Commissioner of An Garda Síochána and others	H.K. v Prokuratuur	Cass. crim. 2024	Saber; Wieser and Bicos	Sigurður Einarsson; Yalçınkaya; Dzivev	Marcello Viola

THE LAWYER'S ETHICAL REQUIREMENT

- Never accept a computer output as incontestable because the technology behind it looks complex.
- Be competent enough to ask the right legal questions of the investigator, the expert, the engineer and the judge.
- Formal access is not an effective defence; a person on a screen is not effective participation; theoretical protection is not real confidentiality.



Laurent Caruso

The integrity of evidence and the rise of artificial intelligence: from digital evidence to AI-mediated evidence

Paris, 13 November 2026

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

Co-funded by the EU



01

AI redefines what counts as evidence

I. Synthetic evidence, deepfakes and provenance

AI can create, modify, reconstruct and interpret information

SOURCES

Council of Europe — Discussion paper on deepfakes and criminal law (February 2026)

Council of Europe — work on AI and criminal law: deepfakes as a priority

A. SYNTHETIC EVIDENCE

The danger lies in **hybrid evidence**: five words inserted in a genuine recording, one face replaced in CCTV footage, one message generated within an authentic exchange.

B. THE "LIAR'S DIVIDEND"

AI **makes false evidence more credible**, while **making genuine evidence less inherently credible**: an inconvenient recording may simply be called a deepfake.

C. PROVENANCE

Original file, device, date, metadata, exports, edits, earlier versions. **Back to classical methods:** chain of custody, corroboration, forensic analysis, contemporaneous records, witness evidence.

The more convincing synthetic evidence becomes, the less appearance alone can establish authenticity.



02

Evidence transformed by AI

II. Enhancement, transcription, summaries

When AI is used on genuine evidence, the boundary becomes much less clear

SOURCES

CNB — 2024 practical guide on generative AI: evaluate, improve and verify the generated result

A. ENHANCEMENT OR GENERATION?

Information present in the source, or information **inferred by the model** because it is statistically likely? e.g. an “enhanced” blurred licence plate.

B. TRANSCRIPTION & TRANSLATION

Locating a passage is not proving the **precise words spoken**. Liability may depend on the remaining 5 %: slang, irony, a coded expression, a negation.

C. AI SUMMARIES

AI does not merely organise information but **frames our understanding of the case**. What did it omit? Did it distinguish an allegation from an established fact?

Rule 1: **Never present generated information as though captured by the original sensor.**

The greater the evidential significance of the output, the greater the need to return to the source.



03

When AI draws the conclusion

III. Evidence versus algorithmic inference

"The algorithm identified him" is not an evidential explanation

The camera recording
= evidence

The software "match"
= an inference derived from it

TWO QUESTIONS — NEVER MERGED

1. **Is the underlying evidence authentic?**
2. **Is the inference drawn from it reliable?**

WHAT THE LAWYER NEEDS TO KNOW

- What was the system designed to do?
- What data were supplied to it?
- Was it validated for this type of use?
- What error and false positive rates are known?
- Were the circumstances comparable with testing?
- Was there human review?

Can the conclusion be independently tested? Technological complexity cannot become a substitute for evidential reliability.



04

European law: a framework, not yet a law of AI evidence

IV. A framework under construction

Several legal developments point in the same direction

LEGAL FRAMEWORK

- **Regulation (EU) 2024/1689 — AI Act**
- **Council of Europe Framework Convention on AI**
- **European Committee on Crime Problems**

AI Act: risk-based approach; human-centred and trustworthy AI; high level of protection for fundamental rights. Some law-enforcement and justice uses are particularly sensitive.

Framework Convention: lifecycle and risk-based approach; human rights and the rule of law at the heart of AI governance.

European Committee on Crime Problems: working on AI and criminal law, including digital evidence and deepfakes.

FOUR CONCEPTS CLEARLY EMERGING

Traceability	Risk assessment	Human oversight	Accountability

No comprehensive European law of AI evidence yet — but these concepts will matter increasingly.



05

The criminal lawyer’s five questions

V. Five questions

When AI has produced, modified or interpreted an evidential item

1	**What is human evidence and what is machine output?**	Separate the original data from its transcription
2	**Can we return to the original?**	Never let the AI output replace the source
3	**Can the operation be reconstructed?**	System, version, date, task, inputs, edits, validation: preserve an audit trail
4	**What is the risk of error in this particular use?**	General performance ≠ forensic reliability in the case
5	**Can another person challenge the conclusion?**	Forensic integrity meets procedural fairness



06

When lawyers use AI

VI. The CNB's practical framework

Built progressively between 2024 and 2026

PROFESSIONAL FRAMEWORK

- **CNB — Generative AI guide (2024)**
- **CNB — Choosing legal AI tools (2025)**
- **CNB — Ethics and AI (March 2026)**
- **French Bar — international work**

2024	Functioning, potential uses and risks of generative AI; evaluation and verification of generated output
2025	Criteria: functionality, data sovereignty, confidentiality, security, possible reuse of client data by underlying models
March 2026	Professional secrecy, personal data, competence, diligence, prudence and independence
International	False case law, erroneous legal analysis, artificially created evidence, fundamental-rights risks; continued lawyer responsibility

AI can delegate a task. It cannot delegate professional responsibility.



07

Find, organise, test - not decide

VII. A practical distinction

For criminal lawyers

Find | **Organise** | **Test** | **× Decide**

Be much more cautious when the tool moves from assisting analysis to making the evidential judgment itself.

CNB publications 2024–2026: AI should be used, lawyers should become competent in its use, generated outputs need to be understood and verified, and the choice of tools must itself be informed.

Final rule: always preserve the route back to the evidence.

The more fundamental danger arises when we can no longer reconstruct why the machine reached the conclusion on which the criminal process relies. **That will become one of the central questions of evidential integrity in the age of AI.**