Emilie Quinton - Lawyer, *Secrétaire de la Conférence,* Paris Bar

Overview of Criminal Law Instruments and their Digitalisation

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

Co-funded by the EU

Why This Matters: Justice Without Borders

The EU is an **Area of Freedom, Security and Justice** (Art. 3 TEU; Title V TFEU). Two objectives drive its action:

- Ensuring **effective access to justice**;
- Facilitating **judicial cooperation in criminal matters** between Member States.
- Two engines have carried this: **mutual recognition** (built on mutual trust) and **direct cooperation** between national authorities.

The shift

Digital transformation is the next step - moving cross-border criminal justice **from paper to platform**.

The Instruments: a Map of EU Cooperation

- **European Arrest Warrant** - FD 2002/584/JHA (surrender of requested persons).
- **European Investigation Order** - Directive 2014/41/EU (cross-border evidence-gathering).
- **Freezing & confiscation** - Reg. (EU) 2018/1805; plus transfer of prisoners (2008/909), European Protection Order (2011/99), probation (2008/947), supervision (2009/829), confiscation (2006/783), conflicts of jurisdiction (2009/948).
- **Criminal records & electronic evidence** - ECRIS; and the e-Evidence package (slide 9).

The common thread

One State's judicial decision is recognised and executed in another - on **mutual trust**, with narrow refusal grounds.

From Paper to Platform: the EU Digital Strategy

- **e-Justice action plans** (2009-2013, 2014-2018) and the **European e-Justice Portal** - a single gateway to cross-border justice.
- **Early building blocks** - online forms, ECRIS (criminal-records exchange), and the promotion of videoconferencing.
- **Guiding principles** - digital by default, interoperability, security, avoiding social exclusion, preserving mutual trust.

The goal

Modernise cross-border civil and criminal procedures **without weakening rights or access to justice**.

e-CODEX: the Technical Backbone

- **Regulation (EU) 2022/850** - the legal basis for e-CODEX; governance entrusted to eu-LISA (amending Reg. 2018/1726).
- **A decentralised, interoperable communication system** - no central EU database.
- Fast, secure and reliable exchange of electronic data and documents between national systems.
- **Respects judicial independence** and each State's existing back-end systems.

In one line

e-CODEX is the secure “rails” on which digital judicial cooperation runs.

The Keystone: Digitalisation Regulation 2023/2844

- **Regulation (EU) 2023/2844** - the core framework for digitalising judicial cooperation; applicable since 1 May 2025.
- **A decentralised IT system based on e-CODEX**, with a single European electronic access point on the e-Justice Portal.
- Introduces **electronic communication, digital document exchange and videoconferencing tools**.
- **Directive (EU) 2023/2843** - companion text aligning existing instruments; requires national transposition.

The principle

“Digital by default” in cross-border cooperation - directly applicable (Regulation) and transposed (Directive).

The Operational Tool: the e-EDES Portal

- **e-EDES** (e-Evidence Digital Exchange System) - built by the European Commission; complies with e-CODEX.
- **Default secure channel** for transmitting requests, documents and digital evidence between competent authorities.
- **Pilot mode for European Investigation Orders** today; expanding ahead of the e-Evidence Regulation.
- **Exceptions** - physical / technical limits, where originals are required, or force majeure.

Why it matters

This is where cross-border criminal cooperation **actually becomes digital, day to day**.

The Roll-out Calendar 2026-2029

- **17 January 2026** - European Arrest Warrant (2002/584), European Investigation Order (2014/41), Freezing & Confiscation (2018/1805).
- **17 January 2027** - Transfer of prisoners (2008/909), European Protection Order (2011/99).
- **17 January 2028** - Confiscation orders (2006/783), Conflicts of jurisdiction (2009/948).
- **17 January 2029** - Probation measures (2008/947), Supervision measures (2009/829).

Take-away

Digital channels become mandatory instrument by instrument - **diary the dates that touch your practice**.

The Next Frontier: e-Evidence

- **Regulation (EU) 2023/1543** - European Production & Preservation Orders for e-evidence in criminal proceedings; applies from 18 Aug 2026.
- **Directive (EU) 2023/1544** - designated establishments / legal representatives of service providers; transposition by 18 Feb 2026.
- **Direct cross-border requests** - authorities in one State ask providers in another directly, with limited involvement of the host State.
- Exchanged through e-EDES / e-CODEX.

Stakes for the defence

Faster access to private data across borders - and new questions of **legality, proportionality and remedies**.

Remote Hearings under Regulation 2023/2844

- Videoconferencing must verify identity, ensure visual / audio / oral communication, and enable **effective participation**.
- **A mere telephone call** is not sufficient for an oral hearing.
- **Consent** of the suspect / accused / convicted (and affected persons under Reg. 2018/1805) is the general rule.
- **Derogation** only for genuine, present or foreseeable threats to public security or health, and strictly necessary.

The line

Efficiency is welcome - but **directness, immediacy and physical presence** stay central to criminal adjudication.

The Other Side: Rights and Safeguards

- **Anchored in the Charter and the ECHR** - Arts 6, 7, 8, 47, 48 (liberty, privacy, data protection, effective remedy, defence).
- **The procedural-rights "roadmap" still applies** - interpretation (2010/64), information (2012/13), access to a lawyer (2013/48), presumption of innocence & presence (2016/343), children (2016/800), legal aid (2016/1919).
- **Confidential lawyer-client communication** and an **effective remedy** (Art. 47) must survive digitalisation.

The key idea

Digitalisation creates **no new rights - but new ways to infringe them**. Rights are the starting point, not an afterthought.

What It Means for the Defence

1. **Know the plumbing** - e-CODEX, e-EDES, the e-Justice Portal: understand how evidence now moves.
2. **Diary the deadlines** - each instrument goes digital on its own date (2026-2029).
3. **Police the safeguards** - consent, confidentiality, effective participation, identity, technical quality.
4. **Treat competence as ethics** - digital literacy is now part of professional diligence.
5. **Build the remedy** - challenge unlawful or unsafe digital practice under Art. 47 and the procedural directives.

Conclusion: Digital by Default, Human by Design

- **A coherent EU architecture** - instruments (EAW, EIO, e-evidence…) + infrastructure (e-CODEX, e-EDES) + framework (Reg. 2023/2844).
- **The promise** - faster, interoperable, more accessible cross-border justice.
- **The condition** - it must stay human-centric, transparent, fair, accountable and rights-respecting.

“Not everything technologically possible is also socially desirable, ethically acceptable or legally justified.” - Stefano Rodotà

Helin Köse - Lawyer, Former Secretary of the Conference, Paris Bar

Use of videoconferencing in criminal matters

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

Co-funded by the EU

Appearance through a screen

Audi alteram partem: hear the other side. In criminal matters, videoconferencing is not a remote exchange. It is a **mode of appearance**.

Two forces pull against each other

- **Efficiency** : security, speed, court management, fewer prison transfers.
- **The core of the trial** : presence of the accused, confidential bond with counsel, effective defence.

How far can audiovisual appearance serve efficient justice without weakening the presence of the accused and the effectiveness of the defence?

Roadmap

France → the European standard (ECtHR & EU) → a comparative glance (Turkey) → a toolkit for the defence.

Why criminal matters demand heightened scrutiny

- Not every use is equal: a remote expert is not a detained accused arguing for liberty.
- **Immediacy is constitutive of the criminal trial** : speech, silence, attitude, eye contact, contradiction. The court judges a person, not only a file.
- **The screen creates an appearance of unity** while two places remain: the place of judgment and the place of detention.
- Even when the technology works, it can weaken the bond with counsel : an “invisible wall”.

Decisive criterion

Not administrative convenience but **procedural necessity**.

France — legislative expansion (art. 706-71 CPP)

- **2001** - Art. 706-71 introduced (Law of 15 Nov. 2001); limited at first to certain investigative acts.
- **2019 → 2025** - progressive extension to all stages, “in the interests of the proper administration of justice” (Laws of 23 Mar. 2019; 13 June 2025).
- **Aug. 2024 Circular** - Ministry of Justice (DACG) guidance on use in criminal matters.
- **Judicial pragmatism** - fewer extractions, fewer transfer risks, easier scheduling.

The limit

“Proper administration of justice” cannot become an **automatic** ground; managerial logic must not overtake the logic of appearance.

France - constitutional resistance

- Defence rights are anchored in **Article 16 of the 1789 Declaration**.
- **Cons. const., 20 Sept. 2019 (2019-802 QPC)** - no videoconferencing without consent in certain pre-trial detention hearings; a detainee could otherwise go a year with no physical appearance.
- **Cons. const., 10 Apr. 2026 (2026-1192 QPC)** - the narcotrafic law (13 June 2025) left a gap: a criminal accused detained over six months, not personally heard for at least six months, could not object. Held unconstitutional; transitional right to refuse.

The shift

Physical presence is no longer a procedural comfort : it becomes a **constitutional argument for the defence**.

The European standard — a common framework

– **ECtHR, Marcello Viola v. Italy (2006):** video participation is not, in itself, contrary to Article 6.

Admissibility is conditional, four cumulative requirements:

1. an accessible **legal basis**
2. a **legitimate aim** (security, witness protection, reasonable time)
3. **individualised necessity**
4. **practical safeguards** - image/sound quality, confidential communication with counsel

– **ECtHR, Sakhnovskiy v. Russia (GC, 2010)** & **Kucera v. Austria (9 Dec. 2025)** : effective, confidential contact with counsel is decisive; lawful arrangements must work in practice.

The EU layer — shared rules across our jurisdictions

- **Directive (EU) 2016/343** : presumption of innocence and the **right to be present at trial** (Art. 8); binds every EU Member State.
- **Regulation (EU) 2023/2844** (“digitalisation of judicial cooperation”) : applicable since **1 May 2025**.
  - governs videoconferencing in **cross-border** criminal cooperation
  - the suspect or accused must, in principle, **consent** to remote participation

Take-away

Across France, Romania, Ireland, Spain, Cyprus, Greece, Poland and Bulgaria, the same **ECHR + EU floor** applies: consent, necessity, and concrete safeguards.

A Comparative glance : Turkey and SEGBIS

- **SEGBIS** (Ses ve Görüntülü Bilişim Sistemi) - audiovisual system inside the UYAP environment; 2011 Regulation, in all courts and prisons since 2013; basis Art. 196 §4 CMK.
- **A different starting point** - France debates the expansion of an option; Türkiye debates the control of a system already installed and routine.
- **A Council of Europe State** - bound by Art. 6 ECHR, with individual application to the Constitutional Court since 2012.
- **Turkish Const. Court, Şehrivan Çoban (2020)** - a terrorism case: after transfer to a distant prison, the accused was refused in-person attendance and heard via SEGBIS. Violation: the court must give concrete, individualised reasons; abstract security or distance is not enough.
- **Under scrutiny** - heavily used in post-2016 mass trials; criticised for eroding immediacy (face-to-face) and equality of arms.

Convergence

Same rule as Strasbourg and Paris: audiovisual appearance **must not neutralise the defence**.

A toolkit for the defence

1. **Identify the procedural moment** : the graver the stakes, the higher the scrutiny.
2. **Object, on the record** : where the law allows refusal, make it clear and reasoned (Art. 706-71-1 CPP; reinforced by the 10 Apr. 2026 decision).
3. **Demand reasons and alternatives** : why no physical appearance? A delayed transfer or short adjournment may suffice.
4. **Protect confidentiality** : secure a confidential channel with counsel; decide where counsel stands (court vs. place of detention).
5. **Record every technical failure** : frozen image, inaudible sound, no contact with counsel: preserve it in the record of the hearing.

Conclusion : a threshold of acceptability

- The issue is **not** modernisation versus tradition, nor accepting versus rejecting technology.
- It is whether **digital justice remains compatible with an effective defence**.
- Three converging signals : French constitutional case law, the ECtHR and EU law point the same way: **presence is the rule, remote appearance the justified exception**.

For the defence

Videoconferencing is a **litigation issue in its own right**.

Martina Biondo Vincenti, lawyer at the Paris and Milan bar

Considerations of fundamental rights and lawyer's ethics regarding digitalisation

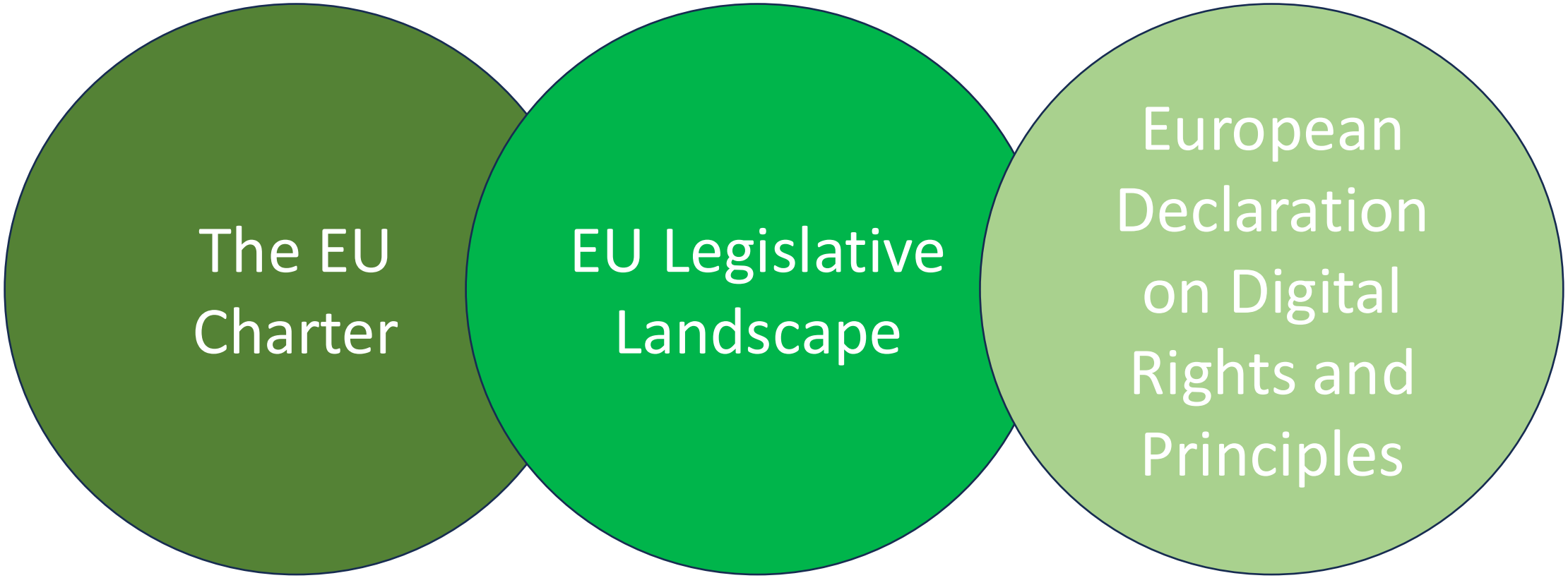
Training of Lawyers in various areas of EU law 2 **#TRAVAR2**

Co-funded by the EU

ROADMAP

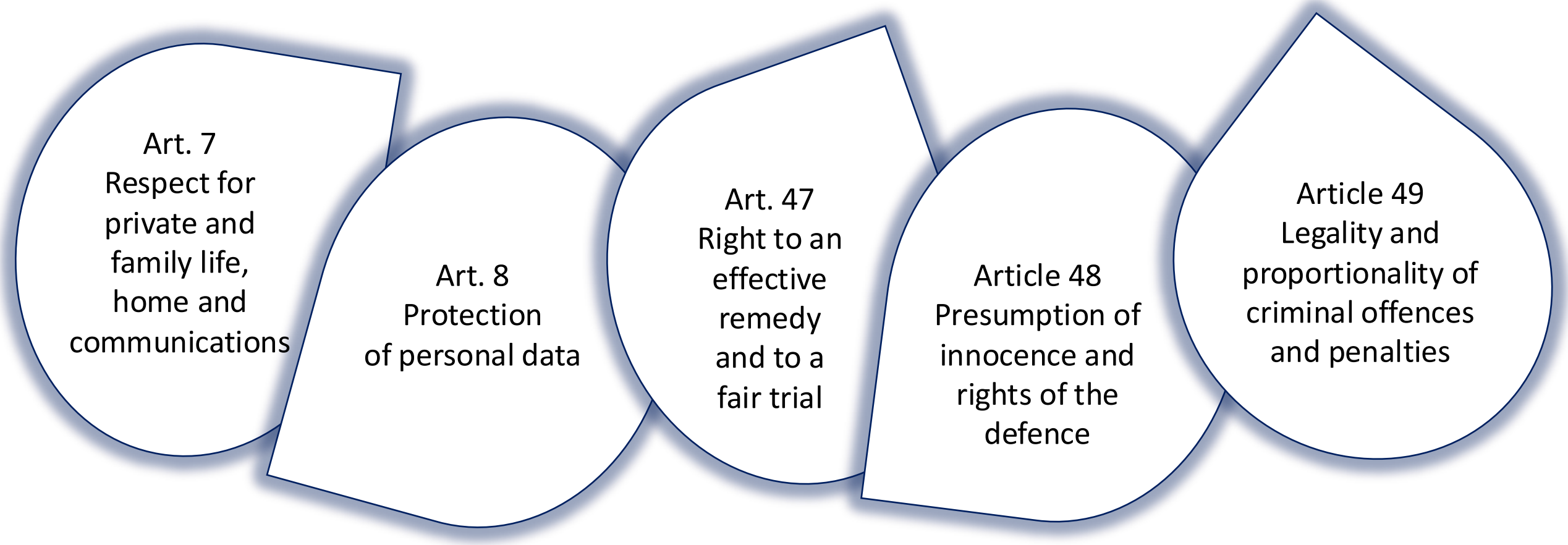
Part I	The EU Framework: Rights and Principles
Part II	Digitalisation in Criminal Proceedings: Safeguards and Tensions
Part III	Lawyers' Ethics in the Digital Era
Conclusion	Closing Remarks and Questions

I. THE EU FRAMEWORK: RIGHTS AND PRINCIPLES



I.A. The EU Charter

"*Our EU Magna Carta*" – M. O'Flaherty, FRA, 2019



I.B. The EU Legislative Landscape

REG. 2023/2844

The reg. on the digitalisation of judicial cooperation

- ✓ Digital by default principle
- ✓ Electronic communication between authorities
- ✓ Digital exchange of documents
- ✓ Videoconferencing
- ✓ Electronic signatures and seals

N.B. It directly applies

Directive 2023/2843

The Digitalisation Directive

It aligns existing instruments of judicial cooperation in criminal matters — mutual recognition instruments, evidence directives, framework decisions — with the new digital framework.

N.B. It requires transposition

Other specific regulations

- ❑ GDPR (REG. 2016/679)
- ❑ e-CODEX (REG. 2022/850)
- ❑ The e-Evidence Regulation (REG. 2023/1543)
- ❑ The Council of Europe Framework Convention on AI (2024)

I.C. The European Declaration on Digital Rights and Principles (2022)

Binding

Political vision
Digital rights

- Human-centric digital transition
- Solidarity and inclusion
- Connectivity
- Digital education
- Fair and just working conditions
- Data protection and privacy
- Non-discrimination and gender equality
- Consumer protection
- Sustainability

II. DIGITALISATION IN CRIMINAL PROCEEDINGS: SAFEGUARDS AND TENSIONS

PRIORITIES

- ❑ Harmonised digital development
- ❑ Equal access to technological infrastructure
- ❑ Digitalisation of judicial cooperation
- ❑ Effective use interoperability between national systems
- ❑ Facilitation of cross-border judicial proceedings through digital tools and technologies
- ❑ Safeguarding EU values, rule of law and fundamental rights

Videoconferencing (REG. 2023/2844)

DOUBLE CONDITION

1. Member state request of a hearing of a suspect, accused, convicted or affected person present in another Member State

2. Circumstances justify the use of technology

N.B. A mere telephone call is explicitly excluded as insufficient for oral hearings.

TECHNICAL REQUIREMETS

The technology must:

- ✓ Allow verification of the identity of participants
- ✓ Enable visual, audio and oral communication (two-way and simultaneous)
- ✓ Enable effective participation during the hearing
- ✓ Comply with personal data protection standards
- ✓ Ensure confidentiality of communications and data security

Videoconferencing (REG. 2023/2844)

GENERAL FUNDAMENTAL RIGHTS

- ❑ Right to interpretation
- ❑ Right of access to a lawyer
- ❑ Right to information and case file access
- ❑ Right to be present at trial
- ❑ Special safeguards for children

Videoconferencing (REG. 2023/2844)

SPECIFIC RIGHTS

Right to say no

Consent of the person concerned (suspect, accused, convicted person, or affected person)

- Given voluntarily and unequivocally
- Prior to the start of the hearing
- Preceded by full information about rights and the procedure
- Preceded by the possibility of seeking legal advice
- Recorded if the national law allows it

Exception

i) Where participation in a hearing in person poses a serious, genuine and foreseeable threat to public security or public health and

i) the derogation is strictly necessary.

N.B. The person must have the possibility of seeking a review.

Videoconferencing (REG. 2023/2844)

SPECIFIC RIGHTS

- ❑ Confidentiality of Lawyer-Client Communication
- ❑ Access to infrastructures
- ❑ Effective remedy

The case of Mr. Dupont

ISSUES

X Late answer from the judge - Report of the hearing

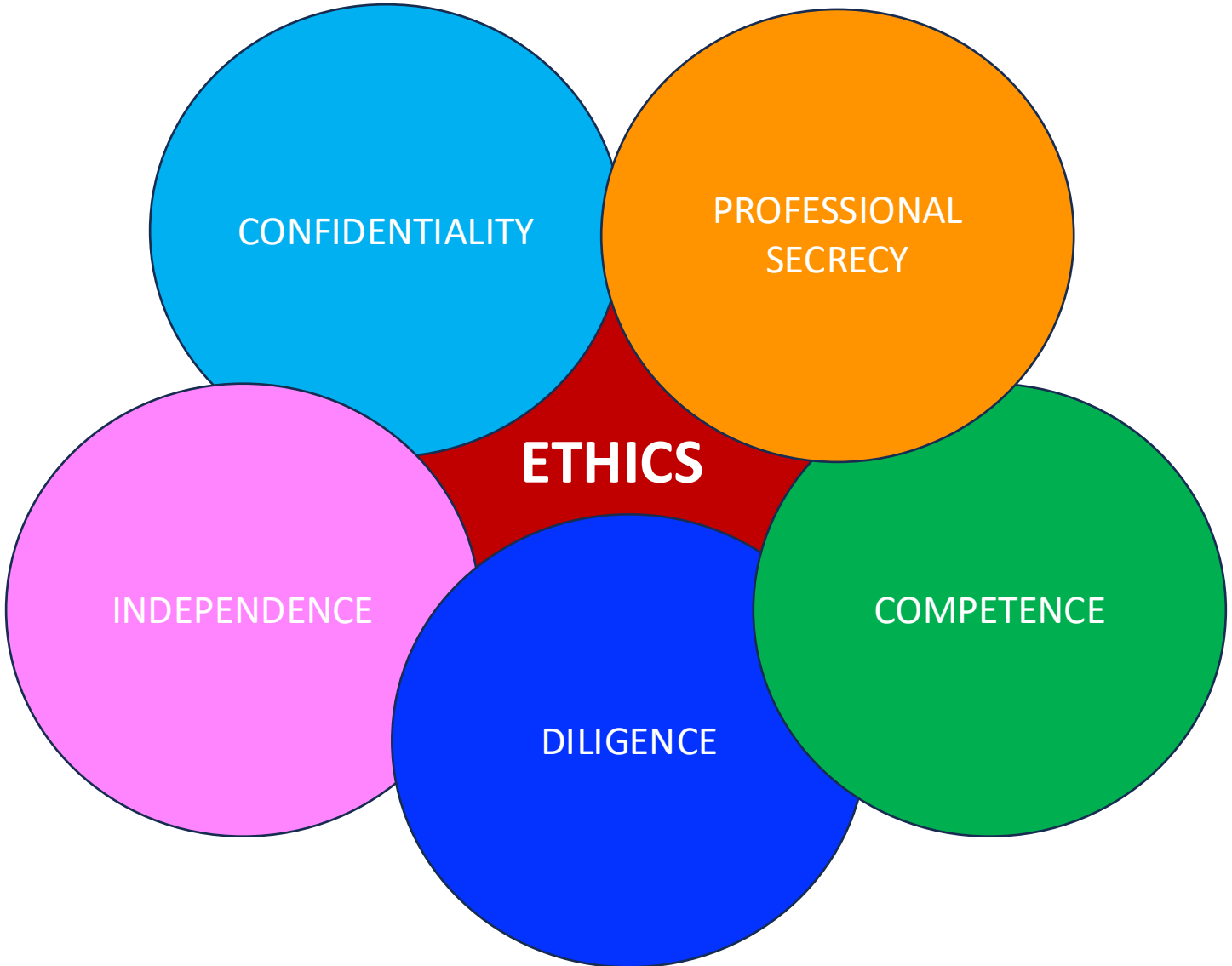
X Defence forced to self-administer the procedure

X Court officials unfamiliar with protocol

X Consulate unable to assist

X Infrastructure quality not guaranteed until D-day

PART III — LAWYERS' ETHICS IN THE DIGITAL ERA



Specific issues

Specific issues

Case studies

FRANCE

Court of Appel of Paris
24 Jan. 2026
Pôle 5-ch. 11, RG n° 21/10238

Lawyer vs Google

GERMANY

Judicial data must be hosted exclusively on national territory

Digital sovereignty

Any solution?

- Dedicated bar-certified digital infrastructure: secure e-mail, document storage, file sharing
- Compulsory training on digital tools and procedural obligations
- Economic assistance mechanisms for small firms and solo practitioners
- Codification of digital ethics in national Bar rules and the CCBE Code of Conduct

CONCLUSION

DIGITAL JUSTICE PRINCIPLES

- ❑ **Human-centric**: technology serves the person, not the institution
- ❑ **Transparency**: the workings of digital systems must be open to scrutiny
- ❑ **Fair**: equality of arms must be preserved in every digital environment
- ❑ **Accountable**: there must be effective remedies when digital processes go wrong
- ❑ **Respectful of fundamental rights**

Ashley Le Cauchois — Counsel, Simmons & Simmons Paris

EU e-evidence procedures: A practical perspective under French law

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

Co-funded by the EU

Opening and roadmap

Scope — criminal proceedings only: electronic evidence obtained from service providers.

1 **Current routes — and what e-evidence adds** Where the new channel fits among existing tools.

2 **The mechanism** Providers, the two orders, addressees, data categories and issuing authorities.

3 **The EU package and the French state of play** Regulation, Directive, and France next steps.

4 **Safeguards and remedies** The lawyer's role and professional secrecy — where the controls sit.

5 **Three practical cases** From provider triage to the corporate internal investigation.

THREAD Thread running throughout: when the order goes directly to a provider, where is the filter — and who operates it?

A practical entry point

E-evidence is usually presented through cybercrime, terrorism or online-platform cases. In practice it also reaches ordinary criminal and white-collar crime proceedings.

The relevant evidence often sits in a user account, an application, cloud storage, messaging or a provider's infrastructure managed by a third party — not in the device itself.

A manufacturer is not automatically covered. What matters is the associated digital service — account, app, cloud, synchronisation, messaging or hosting — through which data is stored or processed.

Before e-evidence, authorities could already seek that data: a French réquisition where the holder was in France; MLA, an EIO, or an uncertain direct request to a foreign provider otherwise.

E-evidence does not create the need, nor invent direct provider requests. It formalises a direct EU channel — with standard forms, deadlines, confidentiality obligations, enforcement and sanctions.

THE REAL QUESTION Does it also change the safeguard architecture — for the authority, the provider, professional secrecy and defence rights?

Who can receive an e-evidence order?

The Regulation does not apply to every company holding data. It targets "service providers" offering services in the Union (art. 3). What matters is the function, not the brand name.

Electronic communications services

Telecom and internet access providers; email, messaging, VoIP and similar services.

Domain name & IP numbering services

Domain registries, registrars, DNS services and IP-related services.

Certain information society services

Cloud and hosting, online marketplaces, platforms and applications where users can communicate, or where storing / processing data is a defining component of the service.

Important limits

- Financial services are excluded — a bank or payment institution is not targeted as such under the Regulation.
- A manufacturer of digital device is not automatically in scope merely because a connected devices exists.
- The condition is whether the relevant digital service stores, processes or enables access to the data sought.

Many e-evidence issues will look like cybercrime but not only: they may arise in ordinary criminal or white-collar crime cases where the evidence simply sits in a cloud account, a platform or a provider environment.

The two orders — and the addressee

Once the relevant provider is identified, the Regulation creates two instruments — and then settles who receives the order.

Order	Purpose	Deadline / duration
EPOC — European Production Order	The provider produces the requested data to the issuing authority.	10 days; 8 hours in an emergency.
EPOC-PR — European Preservation Order	The provider preserves the data so it is not deleted or altered.	60 days; extendable by 30 days; bridges to production.

To whom is it sent?

- **Recipient —** The provider's designated establishment / legal representative (created by the Directive).
- **Rule — art. 5(6) —** The order is addressed to the provider acting as controller — the actor determining the purposes and means of the processing.
- **Exception — art. 5(6) —** It may be addressed directly to the processor where the controller cannot be identified despite reasonable efforts, or where contacting it might be detrimental to the investigation.
- **Information — art. 5(7) —** The processor normally informs the controller, unless the issuing authority asks that this be delayed for as long as necessary and proportionate.

Four data categories — and why the issuing authority matters
Special focus on EPOC

The category determines who may issue the order, what offence threshold applies, and whether another Member State is notified .
This issue is particularly crucial in relation to EPOCs, since EPOC-PRs may be issued either by a judge or by a prosecutor and are not subject to any notification requirement.

Category	What it means	Who can issue / validate	Notification
Subscriber	Who is behind the account — identity, contact, billing.	Any offence; prosecutor possible under national law.	No
Identification	Data requested solely to identify a user — e.g. IP + timestamp.	Any offence; prosecutor possible under national law.	No
Traffic	The envelope — who, when, from where, how long, which device.	Judicial issuance or validation required; seriousness threshold.	Rule / exception
Content	The substance — message body, document, image, file.	Judicial issuance or validation required; seriousness threshold.	Rule / exception

Key French point — pending adaptation

- For EPOC targeting traffic and content data, a prosecutor should not be able to issue alone: issuance or validation by a judge, a court or an investigating judge is required.
- The French adaptation text will have to decide who prepares, who issues and who validates — and under which domestic procedure.
- In a preliminary investigation, one plausible model would be validation by the JLD — presented as a possible architecture, not current law, until a text is confirmed.

Current routes — and what e-Evidence adds

E-evidence is best understood among the tools that already exist. Each route keeps a function; none disappears.

Route	How it works today	Limits	Role after e-evidence
Domestic production request	A national authority orders an entity within reach to produce data (FR: réquisition).	Works where the holder or contact is domestically reachable.	Still used for domestic evidence and national cases.
MLA	State-to-State cooperation, usually through central authorities.	Global and treaty-based, but often slow.	Still needed outside the EU and for broader State cooperation.
European Investigation Order	Judicial authority to judicial authority within the EU.	Broader than e-evidence, but still authority-to-authority.	Still used for investigative acts and evidence beyond stored provider data.
Direct provider request	A request is sent directly to a provider abroad.	May depend on provider policy, voluntary cooperation and local-law assessment.	E-evidence formalises this direct route for covered stored data.

- *Scale: in 2019, France reportedly issued only 55 MLA requests for electronic data — the formal channel did not carry the full practical demand (illustrative figure).*

WHAT E-EVIDENCE ADDS A formal EU channel from the issuing authority to the provider for one object — stored electronic data. Art. 32: the channel is non-exclusive (an added route, not a replacement).

The package and state of play — June 2026

Two EU instruments, doing different jobs. Direct applicability of the Regulation does not settle every domestic procedural question.

Instrument / point	Function	Timing / status
Regulation (EU) 2023/1543	The operational instrument — creates the EPOC and the EPOC-PR; directly applicable.	Applies from 18 Aug. 2026.
Directive (EU) 2023/1544	The provider-side infrastructure — designated establishments / legal representatives.	Transposition due 18 Feb. 2026.
Commission infringement package	Failure to communicate complete transposition measures.	22 Member States targeted; France included. As of today: no further development on the French side / to be monitored closely
French mechanics	Issuing, validation, execution, refusal, remedies, sanctions, urgent cases.	Still to be clarified at preparation stage.

France — focus on a few points to clarify (but not least)

- Who may issue an order?
- Who validates traffic / content orders — possibly the JLD in preliminary investigations, but not confirmed?
- Who acts as executing / central authority in France?
- What procedure for objections, refusals, sanctions and remedies?
- What practical channel for transmission, translation and urgent cases?

The French point of comparison

A few French criminal law procedure reference points to keep in the background when reading the Regulation.

Evidence is free proof, but collection is not. Under art. 427 CPP, offences may be proved by any means, on the judge's inner conviction — yet legality, fairness, proportionality and adversarial debate still govern how data is collected.

The réquisition is the familiar tool. An order to produce information or data. An EPOC is also about production of data, though it is an autonomous EU instrument, not a French réquisition with a European label.

Access is graded. Subscriber/identity, connection (traffic) data and content are not treated alike. Since Cons. const. 2021 (n° 2021-952 QPC), connection data carries specific thresholds and conditions.

Some material is protected even against production. Attorney-client correspondence, journalists' sources and medical secrecy do not become ordinary data merely because a third party holds them.

REFLEXES TO KEEP Who can ask · which data category · how intrusive the measure is · whether protected material is at stake · when the defence can challenge it.

Safeguards and remedies — where are the controls?

The Regulation does not rely on one single filter. The safeguards exist, but they are distributed across several actors and s everal moments.

Issuing / validation authority
For EPOC targeting traffic and content data, the order must be issued or validated by a judge, a court or an investigating judge — a prosecutor cannot issue alone.

Necessity and proportionality
The order must be targeted and justified, and available in a comparable domestic case — no higher power than the internal one.

Notification to the executing State (only for an EPOC)
None for subscriber / identification data; the rule for traffic / content, subject to a connection-and-residence exception. Where notified, refusal grounds may be raised.

Refusal grounds
Under national laws: immunities and privileges, press freedom, and absence of double criminality.
Under European principles: manifest breach of fundamental rights and ne bis in idem..

Provider-side checks
Requests for clarification, problems apparent from the certificate, impossibility or conflict with a third-party law provided by the Regulation.

Information & effective remedies
Information of the person concerned, subject to confidentiality where necessary, and the right to an effective remedy (art. 18) before a court in the issuing State.

PRACTICAL POINT Some controls operate before production, some during execution, some only afterwards — that timing is where the defence issue begins.

e-Evidence & The lawyer's role

Many of these points will also depend on how the transposition is organized at national level.

Legality of the order
Competence of the authority; judicial issuance or validation for traffic / content; sufficient reasons; necessity and proportionality.

Scope
Data category, accounts, custodians, dates, keywords or technical identifiers — a broad mailbox request is not a targeted subscriber request.

Notification
Was the executing State notified, or was the art. 8 exception relied on? Notification is one route through which refusal grounds operate before production.

Professional secrecy / privilege
Is protected material included or at risk? Arts. 5(9)–(10) (privileged professionals), 10–11 (provider flags), 12 (refusal where notified), 18 (remedies).

Remedies
Can the order, the production, the preservation or the use of the evidence be challenged — and the effective ability to comment be preserved?

Defence use
The defence cannot itself issue an EPOC, but under national law it may request investigative measures or production of electronic evidence in its favour.

FOCUS POINT Protected material in a corporate cloud tenant — shared mailboxes, collaboration platforms, investigation workspaces — is not always labelled as privileged: the provider may not know, and the defence may discover it only later.

Case A — the provider's triage problem

CASE A

Scenario A cloud or messaging provider receives an EPOC for content data concerning a business customer. It has 10 days — 8 hours in an emergency — and sees the certificate, not the criminal file.

The certificate shows the issuing authority, the data category, the time range and a basic description — not the underlying case.

The provider is placed in the position of first operational filter — but it acts with limited information, limited time, and structural incentives toward compliance rather than substantive review.

Three distinct responses, not to be confused: produce; request clarification if the certificate is incomplete or manifestly incorrect; flag a privilege issue apparent on the face of the order; or invoke the third-country conflict mechanism (art. 17).

What the provider is not expected to do: conduct a full legal audit of the customer's data or reconstruct French professional-secrecy rules from limited information.

INCENTIVES & LESSON Good-faith compliance is protected (art. 15(2)); failure to comply may trigger sanctions of up to 2% of global annual turnover (art. 15(1)). Where the provider is the only filter before production, preparation is the only realistic safeguard. It cannot happen inside an 8-hour window.

Case B — silent preservation and later disclosure

CASE B

Scenario After 18 August 2026, an authority issues an EPOC-PR to preserve a company director's cloud mailbox in a corruption investigation. The provider preserves the data and keeps the order confidential — the company may not know.

The preserved data should not disappear — but contextual material outside the preservation scope may keep moving: logs, local exports, business-system data, or material under routine retention policies. **The issue is the gap between what is preserved and what continues to move: contextual data outside the preservation scope may be deleted under routine retention, making it harder for the defence to reconstruct and challenge the evidence when it later discovers the sequence.**

A production order follows later; the defence then discovers the earlier preservation. The question is no longer only admissibility — it is whether the evidential sequence can be reconstructed.

Defence requests become concrete: the EPOC-PR, the EPOC, the dates, the scope, the preservation logs, the production history and the chain of custody.

PREVENTIVE LESSON For companies: retention policies must be documented, consistent and genuinely routine — a deletion policy is far easier to explain when it is not invented after the problem appears.

Case C — journalist, lawyer & notification

Useful if the discussion turns to notification, press freedom or lawyer secrecy.

An investigative journalist from another Member State now lives in France, assisted by a French lawyer. Her country of origin opens proceedings and seeks content data from a provider whose designated recipient is in Ireland.

Art. 8(2): if the offence was committed in the issuing State and the target resides there, the executing State is not notified. If the journalist now resides in France, the exception may not be met — residence becomes a concrete defence point.

Substance: press freedom, protection of sources and lawyer secrecy are recognised — but operational only if the authority identifies the issue, the provider flags it, the executing State is notified, or the defence later obtains enough to challenge.

USE ONLY IF ASKED Mutual trust does not eliminate practical friction: some cases will test whether the framework is strong enough where press freedom or professional secrecy is genuinely at stake.

IN CLOSING

Closing

A direct, faster channel for stored electronic evidence — added to the toolkit, not replacing MLA, the EIO or national procedural safeguards.

The key shift is where the first filter sits: in many cases the order reaches the provider directly, the executing State is not always notified, and the controller may be bypassed.

The Regulation applies from 18 August 2026 — but the French issuing, validation and enforcement circuit is still not settled and should be monitored closely.

Watch points: issuing / validating authority, notification, the controller / processor route, professional secrecy in cloud environments, remedies, and the first litigation.

The effectiveness of e-evidence will likely be limited by the ongoing technological evolution of criminal actors, who will continue to develop sophisticated methods of concealing their data through VPNs and anonymisation relay networks, such as Tor.

ONE FINAL QUESTION **Where is the filter — and can the defence test it effectively once the evidence has entered the file?**

Tony Collier, Irish Solicitor

Dangers of Digitalisation in Criminal Law

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

Co-funded by the EU

Benefits of digitalisation in criminal justice

- Faster access to electronic evidence
- Better EU cross-border cooperation
- Quicker and more efficient procedures
- Stronger preservation of digital records
- Better traceability, oversight, and enforcement
- More flexible hearings through remote participation

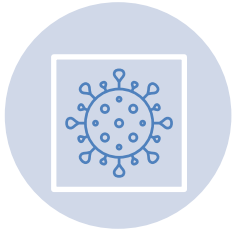
Irish Legislative Development

- Criminal Justice (International Cooperation on Electronic Evidence and Other Matters) Bill 2026
- Transposes Directive (EU) 2023/1544 of the European Parliament
- Aims to enable gathering of electronic evidence in criminal proceedings
- Gives further effect to European Production Orders and Preservation Orders
- Creates an Irish framework for handling digital evidence and service provider compliance

Risks in Digitalisation to fair procedures

- Criminal proceedings engage liberty and access to justice
- Efficiency must not undermine fairness
- Article 6 ECHR expressly protects legal assistance in criminal cases as supposed civil cases
- The future question is not whether technology will be used, but how

Remote Hearings



COVID-19 accelerated remote hearings

Crisis responses should not become default practice without assessment

Digital tools should serve fairness, not become an end in themselves

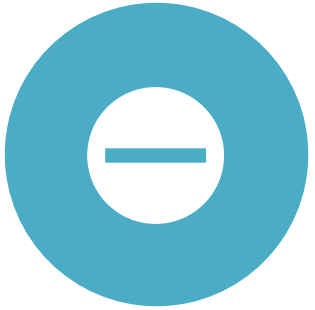
Cost and speed can create pressure for permanent adoption

The Presumption of Presence

A FUNDAMENTAL TENET OF JURY TRIAL

JUDGE, COUNSEL, DEFENDANT, WITNESSES, AND PUBLIC ARE ORDINARILY PRESENT

IRISH LAW ALLOWS LIMITED DEROGATIONS IN DEFINED CIRCUMSTANCES



PRESENCE REMAINS THE DEFAULT, NOT AN INCONVENIENCE TO BE BYPASSED

Irish and International Legal Framework

Criminal Evidence Act 1992: live television link for witnesses other than the accused

Section 21 Criminal Justice Act 1984: witnesses ordinarily appear in person unless leave is given

Directive 2016/343: right to be present at trial

Rome Statute Articles 63, and 64(7): presence of accused, and a public hearing

What Is Lost When Presence Is Reduced?

- Human dynamics of trial are altered in ways not yet fully understood
- Fairness is both substantive and perceptual
- Digital hearings weaken non-verbal communication
- Public confidence in the rule of law may be affected

When Departure from Presence May Be Justified

Encroachment on the presumption of presence must have a purpose

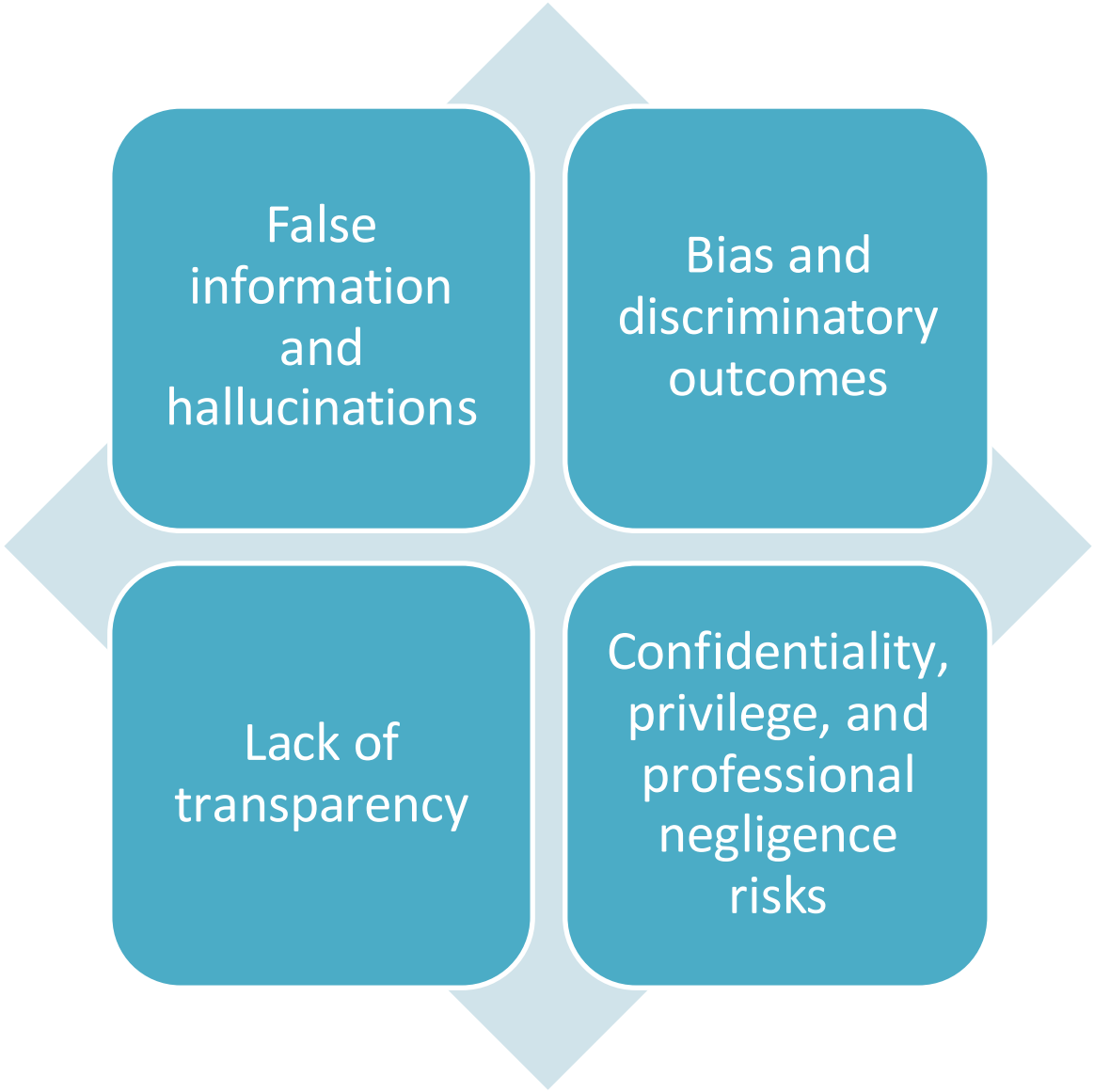
Particular relevance for vulnerable victims and witnesses

Pre-recorded evidence may improve the experience of justice in those cases

Any departure must still protect the accused's fair trial rights

Artificial Intelligence

Main AI Dangers



Von Geitz v. Kelly & Robertson [2026] IECA 29.

- Allen J. was critical of the submission of incorrect citations and non-existent cases during the course of the appeal. He stated:

- *"The plaintiff's written submissions are littered with propositions of law in quotation marks which are unsupported by authority, the non-existent cases were hallucinations generated by AI, it was nevertheless the responsibility of the plaintiff – as it is of every litigant – to check whatever may have been thrown up by whatever tool he used to ensure in the short term that his opponents were not sent on a wild goose chase and ultimately that the Court was not presented with rubbish*."

Lack of transparency

Some AI tools are effectively opaque. It may be unclear:

- what data was used
- how the model weighs different factors
- why it produced a particular result
- how often it is wrong
- whether it performs differently across demographic groups

Professional negligence and ethical exposure

- filing incorrect submissions
- missing disclosure issues
- giving bad advice
- breaching duties of competence, supervision, or confidentiality
- misleading the court, even unintentionally

Reduced legal skill and overdependence

If practitioners rely too much on AI for first drafts, case theories, research, and evidence review, they may gradually lose core skills:

- close reading
- fact analysis
- legal judgment
- cross-checking
- drafting precision
- strategic thinking

Evidential concerns

- Burden of proof in criminal cases is high
- Has the potential to introduce doubt into what before would be considered real evidence
- Provenance and chain of custody issues more pronounced

Manipulated Evidence

- Deepfakes and fabricated evidence
- Contamination of evidence review
- AI makes digital artifacts easier to counterfeit and harder to assess
- The problem is persuasive false evidence, not only total fabrication
- Voice, video, messages, screenshots, and timelines may all be manipulated

Safeguards

- Red-flag training for judges and practitioners
- Using specific legally tailored AI platforms
- AI evidence experts
- Clear oversight mechanisms

Lower risk uses, if carefully supervised

Some uses are comparatively safer if there are strong human review and secure handling of data, such as:

- organizing large disclosure sets
- flagging duplicate material
- creating chronologies from checked source documents
- suggesting redactions for human approval
- formatting draft documents
- searching within transcripts

Conclusion

- Digital tools must strengthen, not weaken, criminal justice
- Efficiency is legitimate only when compatible with fairness
- Presence, challenge rights, authenticity, and confidentiality remain central
- The question is controlled modernization, not convenience-driven change

Cristina Casellas Vazquez, Spanish Lawyer

Electronic evidence in Spanish criminal proceedings

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

Co-funded by the EU

Training of Lawyers on various areas of European Union Law 2

Co-funded by the European Union

#TRAVAR2

MANGO FOUNDER MYSTERY

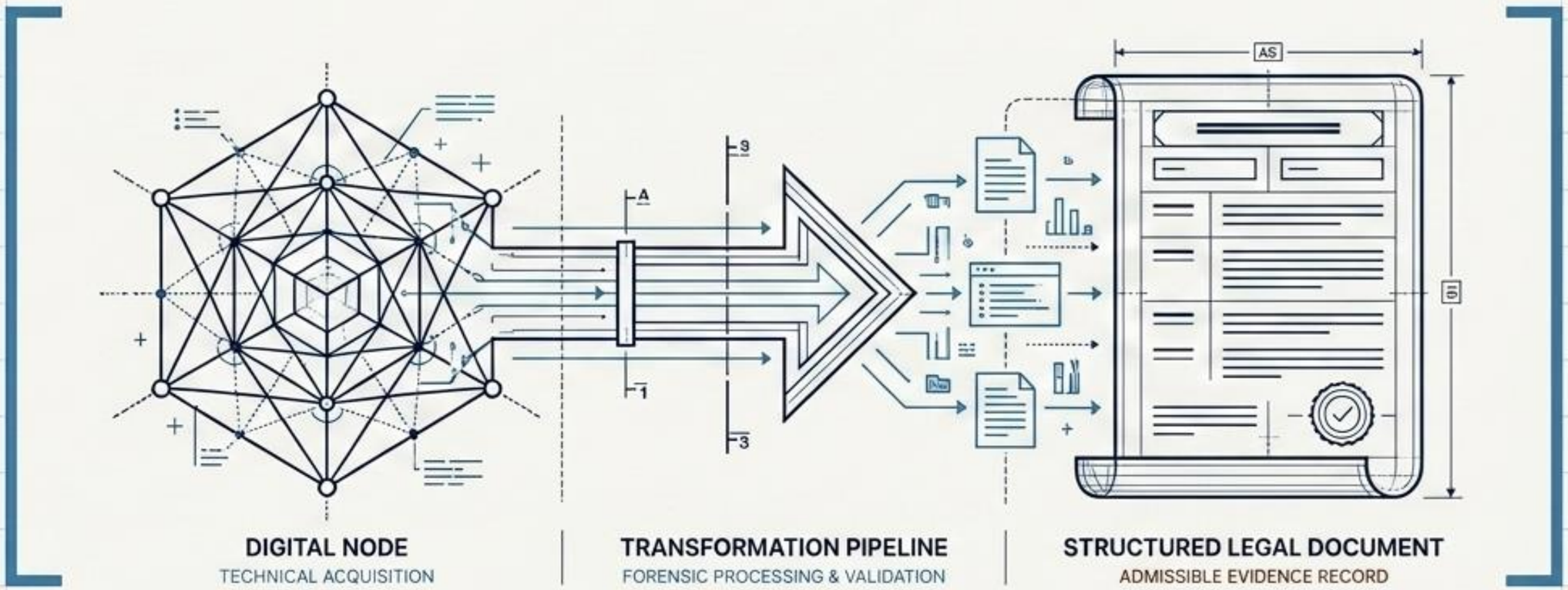
- NO WITNESSES
- PHONE EVIDENCE
- MESSAGES ABOUT INHERITANCE TENSIONS

Training of Lawyers on various areas of European Union Law 2

Co-funded by the European Union

#TRAVAR2

THE EDITORIAL LEGAL SCHEMATIC



Electronic evidence in Spanish criminal proceedings

Strategic guide and diagnostic framework for acquisition, preservation, and litigation (LECrim, EU, and Budapest Convention).

SLIDE ID: L-2024-DIGITAL-EVIDENCE-SCHEMATIC-01 | DATE: OCTOBER 28, 2024

The Two Pillars of Electronic Evidence

Training of Lawyers on various areas of European Union Law 2

Co-funded by the European Union

#TRAVAR2

Lawfulness (Legality)

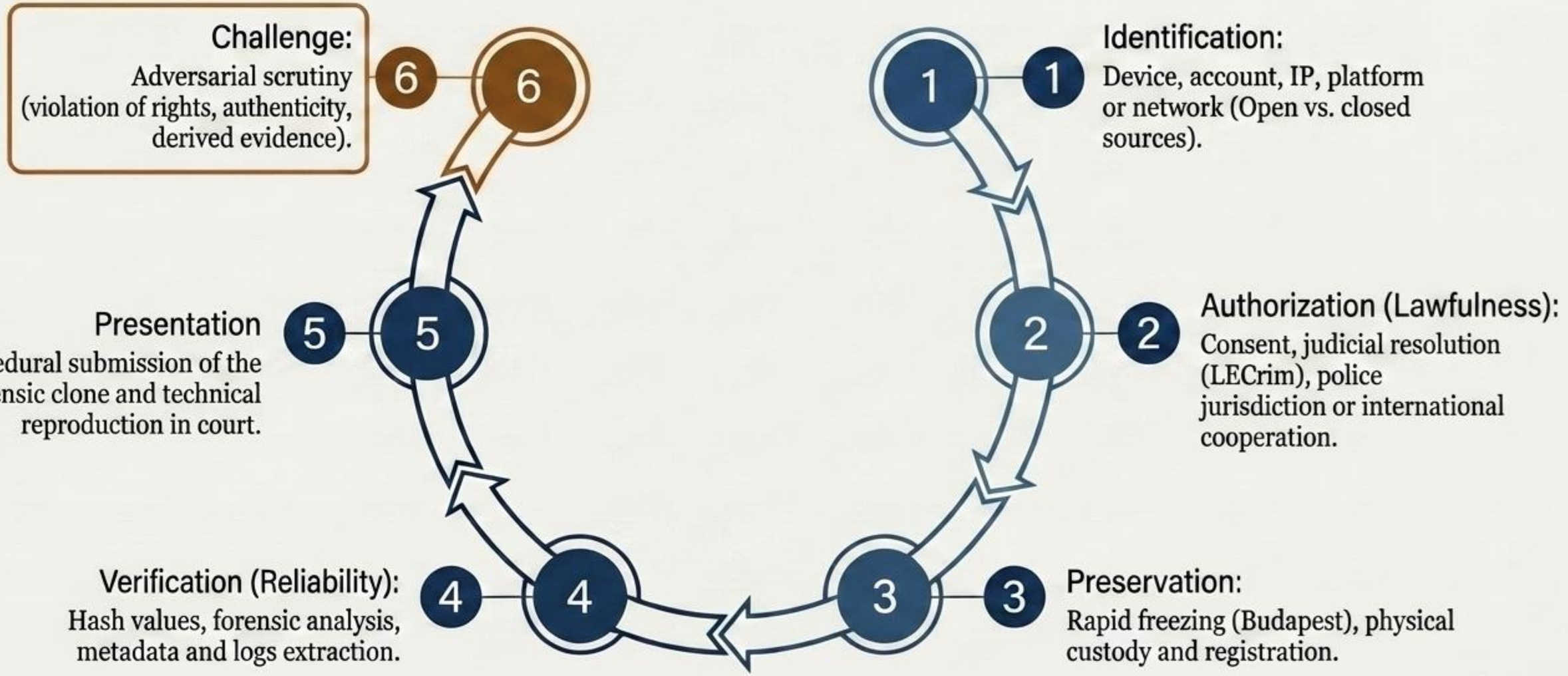
- **Concept:** Evidence has been obtained without violating fundamental rights (privacy, secrecy of communications, data protection).
- **Framework:** Art. 11.1 LOPJ. Control of proportionality and necessity.
- **Litigation Risk:** Null and void and exclusion from the process (Exclusionary Rule).

Reliability (Technical)

- **Concept:** It is possible to demonstrate the identity, integrity, authenticity and continuity of custody of the data (eIDAS Regulation 910/2014).
- **Framework:** Forensic chain of custody and Hash values.
- **Litigation Risk:** Loss of evidentiary value due to manipulation or breach of custody.

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

The Lifecycle of Digital Evidence



Training of Lawyers on various areas of European Union Law 2

Co-funded by the European Union

#TRAVAR2

QUICK HEADS UP

IP ADDRESS: Numeric label assigned to every device connected.

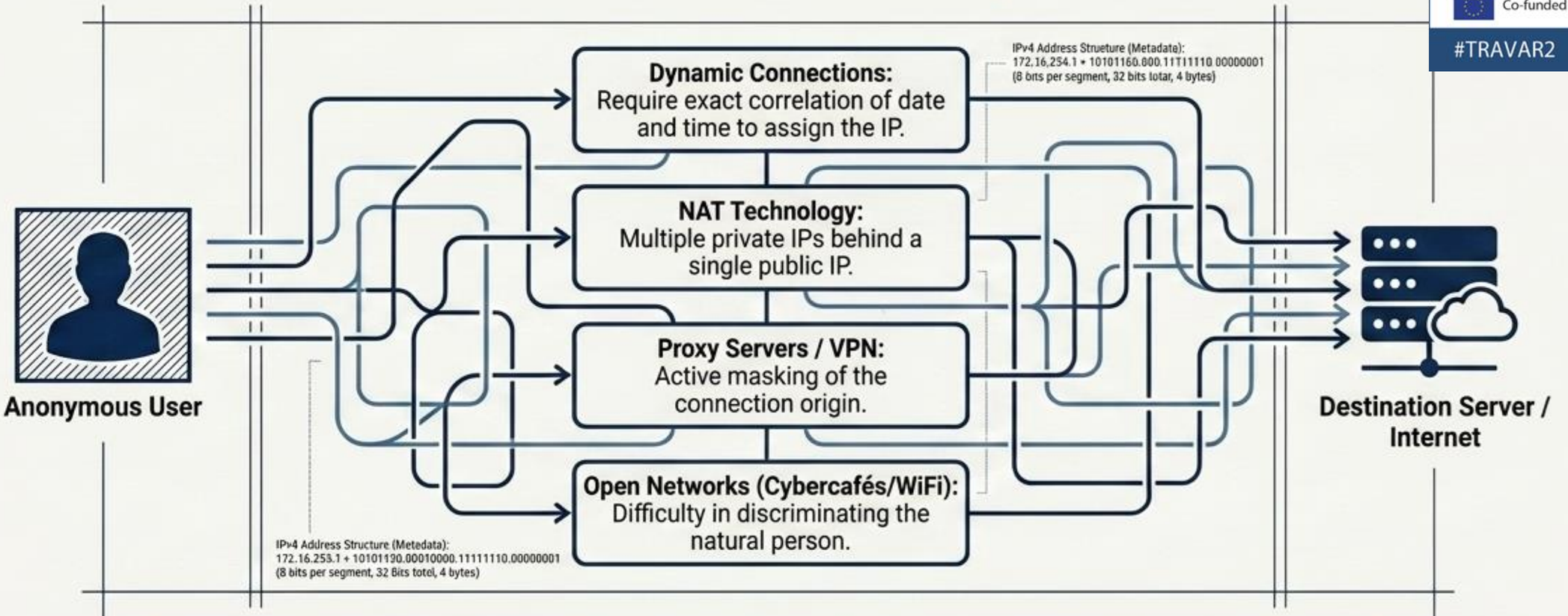
PUBLIC IP: This is public and can be shared by several individuals.

Private IP: Unique numeral label whithin a local network.

VPN: Virtual Private Network masks IP and encrypt network traffick

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

Technical Frontier I: The IP Address Labyrinth



The Legal Key (Art. 588 ter k LECrim)

Without Authorization

The Police can obtain the IP used to commit the crime through lawful tracking or access. (Considered personal data, Art. 18.4 CE).

With Authorization

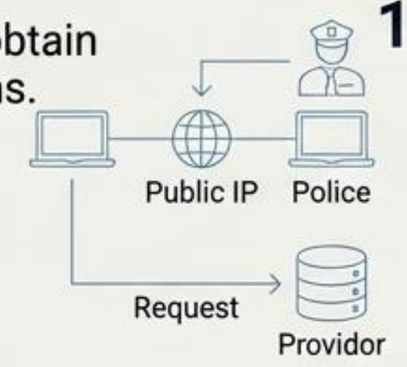
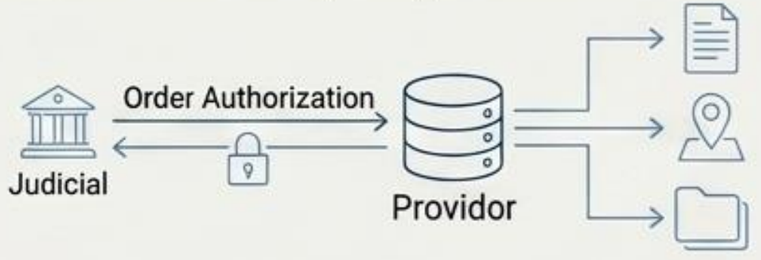
Judicial intervention is required to compel operators to surrender retained traffic data **(Law 25/2007)** to identify the civil holder of the IP.

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

The National Acquisition Matrix (LECrim)

Regulatory framework for access to communications data (Art. 588 ter J-M).

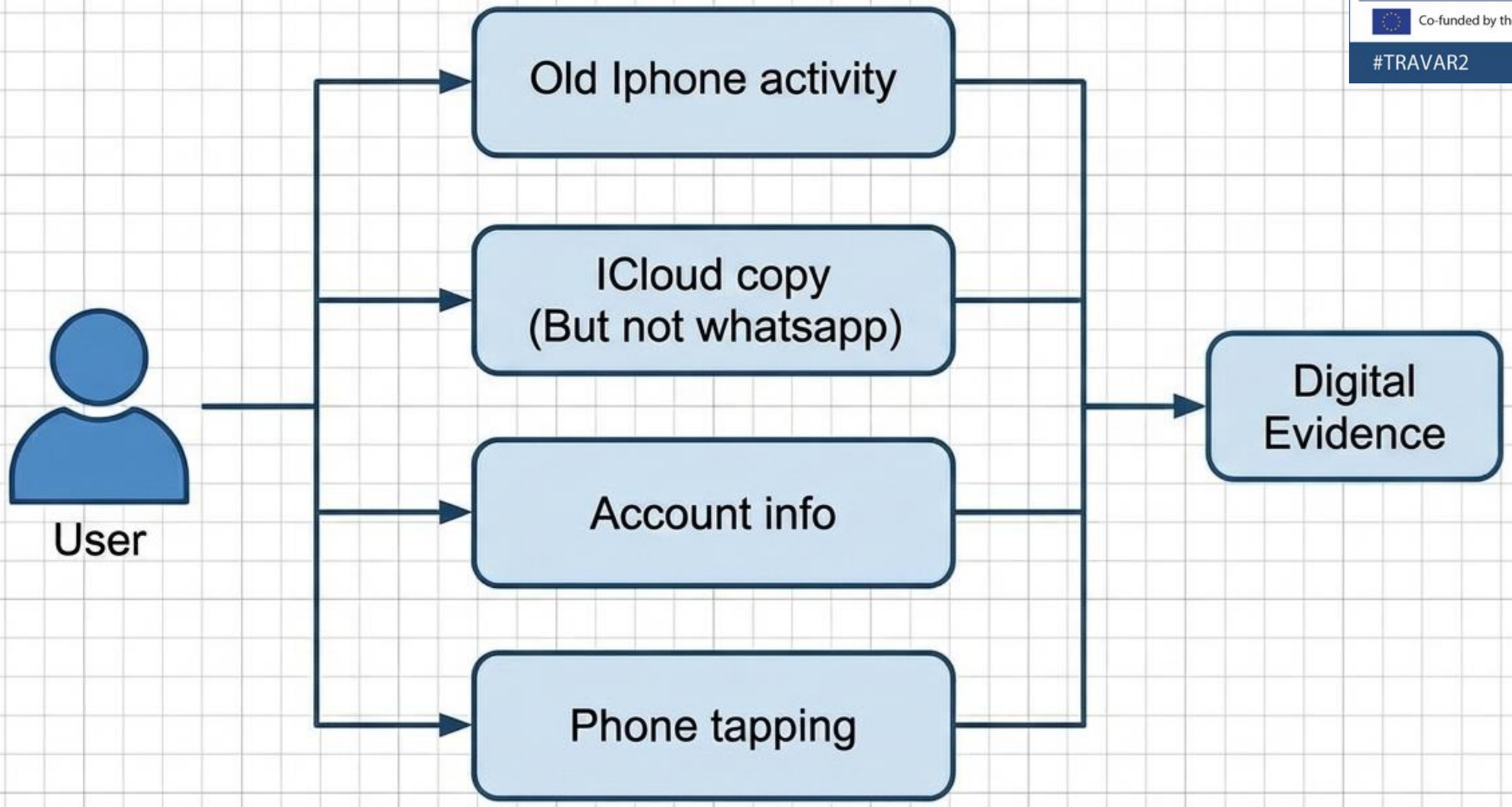
Level of Intrusion

Required Authority	Low Intrusion	High Intrusion
Direct — Police/Prosecutor Access	**1** **Art. 588 ter K:** The Police can obtain the public IP by their own means. **Art. 588 ter M:** Direct request (Prosecutor/Police) to the provider to identify communication line holders. 	**2** ⚠ **[Prohibited]** **Direct access without judicial authorization is totally prohibited for traffic and content data.**
Judicial Authorization Required	**3** **Art. 588 ter K (Second part):** Judicial Order required to request providers to link an IP to the holder (retained data). 	**4** **Art. 588 ter J:** Mandatory judicial authorization to access traffic, location, and content data of communications retained by the provider. 

Training of Lawyers on various areas of European Union Law 2

Co-funded by the European Union

#TRAVAR2



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

ANOTHER QUICK HEADS UP

BLOCKCHAIN: is a digital archive, decentralized (stores data across a network of computers), where data entries (transactions) are grouped in blocks. Every block has the hash of the previous block, creating a link (thus a chain).

HASH FUNCTION: algorithm that turns any data into a string of letters and numbers (HASH). Its Unique and cannot be reverse engineered.

WALLET: stores, sends and receives digital assets (as bitcoin). Has a Public Key (like IBAN) and a Private Key (password or digital signature)

Technical Frontier II: The Blockchain and Web3 Ecosystem

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

Decentralized Logic

- **Cryptographic Trust:** Distributed, immutable, and auditable registers (Proof of Stake/Authority).
- **Tokenization (MiCAR):** Real-world assets (RWA) and stablecoins as evidence of financial operations.
- **Audit Tools:** Use of network explorers (Etherscan, LACNET) as a source of digital proof.

Legal Tensions and eIDAS 2.0

- **The clash with GDPR:** The technical immutability of blockchain makes the right to be forgotten and rectification impossible. Solution: Off-chain storage of personal data.
- **The European Digital Identity Wallet (EUDI Wallet):** Central point of sovereign identity and transaction signature (eIDAS2 Regulation), connecting cryptographic anonymity with legal identity.

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

The Role of Technical Intermediaries (DSA)

Platforms, social networks, and cloud services act as de facto custodians of digital evidence.

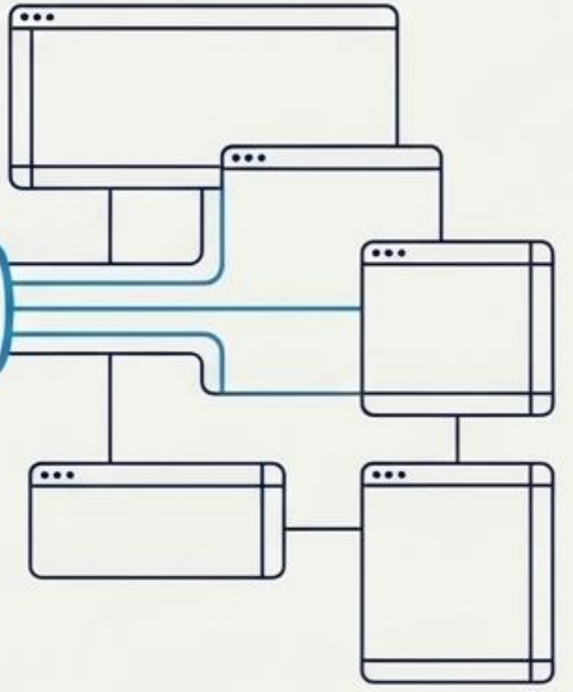
Sovereign Authorities
(Police/Judicial)

Art. 10 (Information Orders):
Obligation to provide specific information about individual users under national orders. The order must be necessary and proportionate.

The DSA Conduit (Directly applicable in Spain)

Art. 18 (Suspicion Notification):
Proactive duty of platforms to alert authorities if they suspect a serious crime (threats to life/safety).

Technical Intermediaries
(Cloud, Social Networks, Marketplaces)



⚠ **Volatility Risk:** In open sources, immediate capture is critical before the provider or the user deletes the content.

Cross-Border Cooperation in the EU

Training of Lawyers on various areas of European Union Law 2

Co-funded by the European Union

#TRAVAR2

Current System: European Investigation Order (EIO)

Mechanism: From Judicial Authority to Judicial Authority (Directive 2014/41/EU).

Execution: Request analyzed by the receiving country to assess conflict of rights and proportionality.

Speed: Theoretical legal deadline of 30 to 90 days (high friction).

The New Paradigm: E-Evidence (From August 2026)

Mechanism: Direct orders to the Legal Representative of the service provider (without going through the provider's state).

Tools (EU Regulation 2023/1543): EPOC (European Production Order) and EPOC-PR (European Preservation Order).

Speed: Preservation without delay. Delivery in 10 days, or only 96 hours in urgent cases.

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

Global Reach: The Budapest Convention

The first international treaty focused on cybercrime and electronic evidence.

Core Architecture

- **Expedited Preservation (Arts. 29/30):** Immediate preservation of data (generally 60 days) to prevent destruction while rogatory commissions are issued.
- **24/7 Network (Art. 35):** Permanent point of contact to ensure immediate assistance and technical advice.

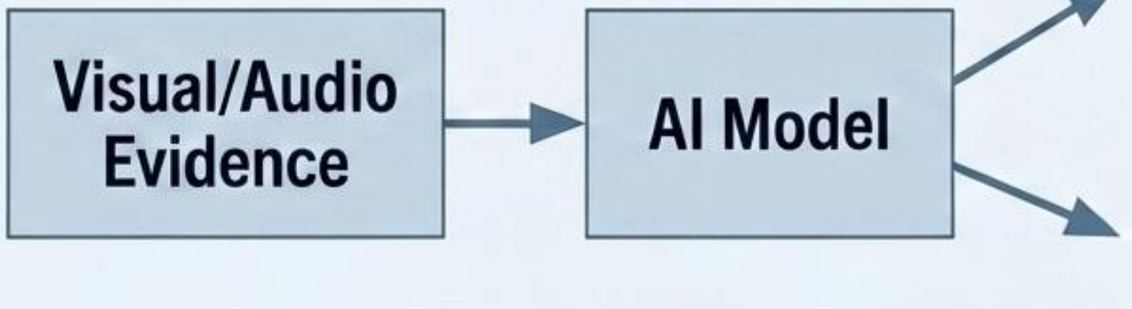
The Second Protocol Revolution (2022)

- **Direct Cooperation:** Permits direct access to providers in another State for domain and subscriber registry data.
- **Emergency Cases:** Accelerated delivery of stored data and direct transmission between judicial authorities.
- **Tools:** Video conferences and intercontinental Joint Investigation Teams.

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

Technical Frontier III: AI and Deepfakes

The direct threat to the pillar of Reliability.



Vector 1: Alteration of Evidence

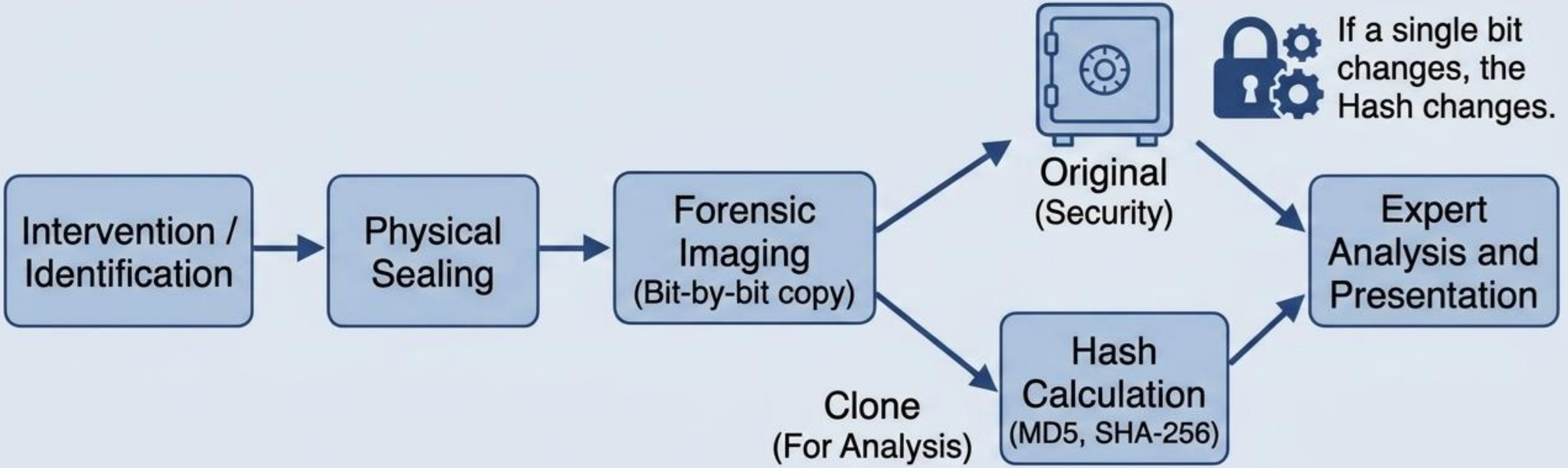
- **Mechanism:** Ultrafalsification of audio or video to simulate facts, confessions, or presences.
- **Procedural Effect:** Systematic challenge for manipulation. Requires expert computer forensic analysis (metadata, pixel noise, physical inconsistencies).

Vector 2: Generation of Evidence

- **Mechanism:** AI used by police to enhance evidence (blurry images) or create simulations of events.
- **Procedural Effect:** Risk of bias and black box effect. Requires algorithmic transparency and significant human oversight.

Defense Mechanism: Any audiovisual evidence not corroborated by solid chains of custody or verified metadata is vulnerable to the doctrine of generative falsehood.

Forensic Chain of Custody



Litigation Rule

A generic allegation of manipulation is not sufficient to invalidate the evidence; the challenger must identify exactly when, how, and where the continuity of custody was broken.

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

Diagnostic Matrix: Probationary Exclusion Doctrines

Exclusion Rule (Art. 11.1 LOPJ)	Falciani Doctrine (STS 116/2017)	Poisoned Fruit	Recordings between Individuals
Concept: Proof obtained by directly or indirectly violating fundamental rights.	**Concept:** Proof obtained illicitly by a private third party (non-state).	**Concept:** Proof derived lawfully but from an originally void source.	**Test:** Good faith and spontaneity vs. deception and prefabricated provocation.
	Balancing Test: The purpose (to evade the law?), intensity of the violation and general prevention are	**Test:** Is there a natural causal and legal connection with the illicit origin?	
Effect: Radical nullity and exclusion; the court cannot base the conviction on it.	**Effect:** There is no automatic nullity; it can be admitted depending on the context.	**Effect:** Exclusion, unless attenuation, inevitable discovery or independent source is proven.	**Effect:** Admitted if part of the natural interaction; excluded if it violates the integrity of the process (or uses torture/extreme coercion).

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

Litigation Strategy Panel

Contribution Checklist (Before relying on the evidence)

- ❑ Map the exact legal route used for acquisition.
- ❑ Identify every person/entity in the chain of custody.
- ❑ Verify the existence of the original, the clone, and the Hash record.
- ❑ Isolate potentially contaminated evidence from other independent evidence.
- ❑ Prepare justification for necessity and proportionality (Art. 18.4 CE).

Challenge Checklist (Before attacking the evidence)

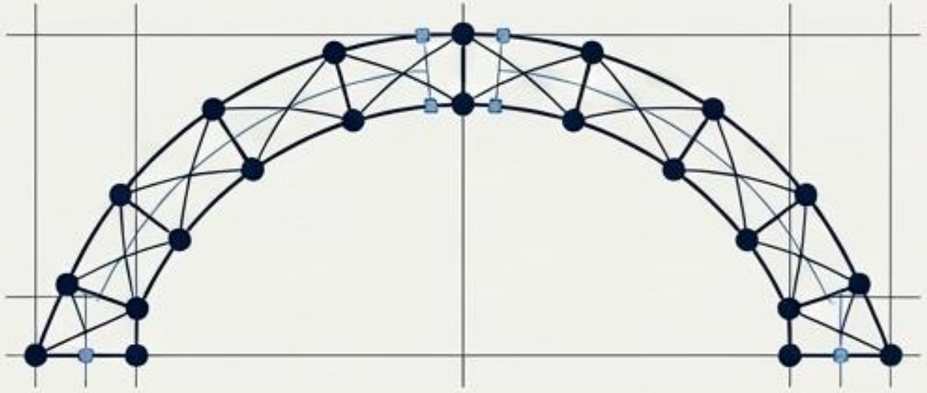
- ❑ Precisely identify which fundamental right or procedural rule has been infringed.
- ❑ Articulate the causal link between the infringement and the evidence presented.
- ❑ Specify the exact technical defect (where the custody or hash is broken).
- ❑ Identify derived evidence affected by the same defect (Poisoned Fruit).

Training of Lawyers on various areas of European Union Law 2

Co-funded by the European Union

#TRAVAR2

Synthesis: The New Role of the Jurist



Central Insight: Digital evidence is not simply a technical object; it is the battlefield where fundamental rights are defined.

Double Nature:

Spanish and European law no longer rely solely on human testimony, but on the combination of procedural authorization (Legality) and verifiable cryptography (Reliability).

Liquid Jurisdiction:

From the OEI to E-Evidence (2026), national borders are disappearing technically and legally.

Final Conclusion:

Probationary excellence requires thinking like an investigator, analyzing like a forensic scientist, and litigating like an architect of law.