George Dominic Pop

# An overview  of main EU criminal law instruments in the context of digital judicial cooperation

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

Co-funded by the EU

- **COUNCIL FRAMEWORK DECISION of 13 June 2002 on joint investigation teams (2002/465/JHA)**

- **REGULATION (EU) 2018/1805 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 14 November 2018** on the mutual recognition of freezing orders and confiscation orders

- **DIRECTIVE 2014/41/EU OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 3 April 2014** regarding the European Investigation Order in criminal matters

- **DIRECTIVE (EU) 2023/1544 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 12 July 2023** laying down harmonised rules on the designation of designated establishments and the appointment of legal representatives for the purpose of gathering electronic evidence in criminal proceedings

- **COUNCIL FRAMEWORK DECISION 2009/829/JHA of 23 October 2009** on the application, between Member States of the European Union, of the principle of mutual recognition to decisions on supervision measures as an alternative to provisional detention

- **COUNCIL FRAMEWORK DECISION 2008/947/JHA of 27 November 2008** on the application of the principle of mutual recognition to judgments and probation decisions with a view to the supervision of probation measures and alternative sanctions

- **COUNCIL FRAMEWORK DECISION of 13 June 2002** on the European arrest warrant and the surrender procedures between Member States (2002/584/JHA)

- **COUNCIL FRAMEWORK DECISION 2003/577/JHA of 22 July 2003** on the execution in the European Union of orders freezing property or evidence

- **DIRECTIVE (EU) 2023/2843 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 13 December 2023 amending Directives 2011/99/EU and 2014/41/EU of the European Parliament and of the Council, Council Directive 2003/8/EC and Council Framework Decisions 2002/584/JHA, 2003/577/JHA, 2005/214/JHA, 2006/783/JHA, 2008/909/JHA, 2008/947/JHA, 2009/829/JHA and 2009/948/JHA, as regards digitalisation of judicial cooperation**

Adrian Hărătău

# Fundamental rights and lawyers' ethics in the digitalisation of EU criminal proceedings

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

Co-funded by the EU

# Imagine this: 08:13, Tuesday morning.

**Your client** — a mid-sized Romanian SaaS founder — calls in panic.

A European Production Order
***(EPOC)*** has been served on his cloud provider in Ireland.

**The order requires:**

- all e-mails of the last 18 months,
- including a folder labelled
***"Counsel — privileged"***.

Deadline for compliance:
**10 days.** In emergency: **8 hours.**

## Three urgent questions:

**1** **What law applies?**
*Romanian? Irish? EU?*

**2** **What rights can you invoke?**
*Privacy · Defence · LPP*

**3** **What is your ethical duty?**
*Confidentiality · independence*

# Where we are going

## I The Digital Turn

EU criminal-justice architecture · the new instruments

## II Fundamental Rights

Charter map · privacy · fair trial · effective remedies

## III Lawyers' Ethics

Independence · confidentiality · LPP · AI · cyber-hygiene

## IV Practical Toolkit

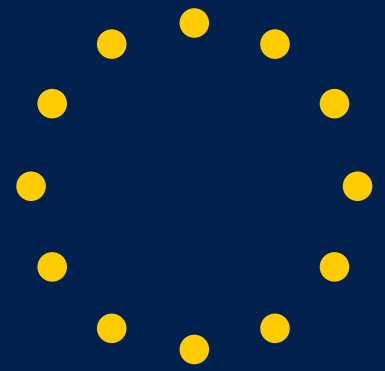
Checklists · red flags · scripts

## Q Discussion

Open questions · cases · take-aways

PART I

*From paper files to packets*



# The Digital Turn

How EU criminal cooperation has been re-engineered for the cloud era — and why every defence lawyer needs to know the four new building blocks.

# More than half of criminal investigations are now cross-border.

**>50%**

of EU criminal investigations involve cross-border electronic evidence

**10 mo**

average time of classic MLA procedures → weeks lost

**120d → 10d**
**10d → 8h**

EIO · EPOC · EPOC in emergency

*Source: European Commission · DG Justice (e-Evidence factsheet, 2023) · Regulation (EU) 2023/1543*

*"Speed used to be the prosecution's problem. It is now the defence's problem too."*

# Four pillars holding up digital EU criminal justice

**1** **Regulation (EU) 2023/1543**

***EPOC & EPOC-PR***

European Production / Preservation Orders for e-evidence. Applicable from 17 Aug 2026.

**2** **Directive (EU) 2023/1544**

***Designated establishments & legal representatives***

Service providers must have an EU contact point. Transposition deadline: 18 Feb 2026.

**3** **Directive 2014/41/EU**

***European Investigation Order (EIO)***

The traditional cross-border investigative tool — now complemented, not replaced.

**4** **e-CODEX + Decentralised IT System**

***Secure communication channel***

Common digital infrastructure for authorities ↔ service providers.

*Take-away: all four pillars are simultaneously in force — every defence file may need to navigate all of them.*

# From a prosecutor's desk to a server in Dublin in 10 days

**Day 0** — 1 — Issuing authority (judge, prosecutor) creates an EPOC

**Day 0** — 2 — Notify the executing state (for traffic / content)

**Day 0** — 3 — Service provider receives the EPOC via e-CODEX

**Day 10** — 4 — Provider transmits data (or refuses on 4 grounds)

**Notify** — 5 — Authority informs the data subject — deferral possible

⚡ **EMERGENCY (Art. 10 Reg. 1543):** Subscriber data and IP must be produced in **8 hours**. Other data — when there is an imminent threat to life, physical integrity or critical infrastructure.

# Where we stand in May 2026

## Romanian timeline

- **12 Jul 2023** — Adoption of Reg. 1543 + Dir. 1544 by EP/Council
- **18 Feb 2026** — Transposition deadline for Dir. 1544
- **4 May 2026** — RO Government adopts draft law (Min. Economy + ANCOM)
- **18 Aug 2026** — Compliance deadline for existing service providers
- **17 Aug 2026** — Regulation 2023/1543 becomes directly applicable

## KEY ACTORS IN RO

**ANCOM** · designated Central Authority

**MJ** · EPOC project (Reg. 1543)

**MEDAT + ANCOM** · EPOC implementation

**DIICOT / DNA / Parchete** · issuing authorities

**Judecători de drepturi & libertăți** · validation

**UNBR / INPPA** · professional standards

**Romanian sanctions: 10,000 RON – up to 2% of worldwide annual turnover** · judicial fines under Reg. 1543 · 3-year limitation period.

# The lawyer's role: from reactive to anticipatory

| *Yesterday · Analog mind-set* | *Tomorrow · Digital mind-set* |
| --- | --- |
| · Paper files, physical evidence | · **Data, metadata, cloud, encryption** |
| · Defence engages after charges are formalised | · **Defence must intervene BEFORE data is produced** |
| · National forum, national rules | · **Multi-state forum: issuing, executing, hosting state** |
| · Months to react to MLA / EIO | · **Days — sometimes hours — to react** |
| · Privilege protected by the physical envelope | · **Privilege depends on grounds for refusal & client awareness** |

PART II

*The Charter is the new criminal procedure code*

# Fundamental Rights at Stake

Privacy, data protection, defence rights, effective remedies — mapped onto the digital workflow.

# Five Charter articles every digital-criminal lawyer must memorise

| | |
|---|---|
| **Art. 6** | **Liberty & security**<br>Detention based on digital evidence — admissibility threshold |
| **Art. 7** | **Private & family life**<br>Communications, devices, location — the digital extension of home |
| **Art. 8** | **Protection of personal data**<br>Lawful basis, purpose limitation, retention limits, independent oversight |
| **Art. 47** | **Effective remedy & fair trial**<br>Right to challenge, equality of arms, full review by a court |
| **Art. 48** | **Presumption of innocence & defence**<br>Access to file, time and facilities, lawyer's presence, LPP |

*+ Art. 6 ECHR · Art. 8 ECHR · Art. 13 ECHR · Strasbourg case-law remains the floor — Luxembourg builds upward.*

# From Digital Rights Ireland to La Quadrature du Net II

## C-746/18 · H.K. v. Prokuratuur

*2 March 2021*

**Holding:**

Access to traffic / location data only for serious crime; the prosecutor — directing the investigation — cannot authorise that access. The authority must be neutral.

**Take-away for the defence:**

- Independent prior review
- Serious-crime threshold
- Proportionality + necessity

## C-470/21 · La Quadrature du Net II

*30 April 2024*

**Holding:**

Generalised IP-address retention is permissible — but only with safeguards: technical separation, encryption, prior independent review for matching identity.

**Take-away for the defence:**

- IP retention green-lit (limited)
- Mandatory safeguards
- Defence-rights respect

# C-670/22, M.N. · CJEU, 30 April 2024 — a new admissibility test

## FACTS

French police infiltrated **EncroChat**, an encrypted-phone network used by organised crime. Live communications were intercepted and shared with other Member States via EIO.

German defendant M.N. contested the use of this data in Germany — arguing the EIO had been issued without proper notification and that the defence could not effectively challenge the evidence.

## THE COURT HELD

**1.**

An EIO does not require the same offence threshold as the underlying interception in the issuing state.

**2.**

BUT: the issuing state must NOTIFY the executing state when the intercepted person is on its territory.

**3.**

AND: national courts must EXCLUDE evidence the defendant cannot effectively comment on — if it has significant impact on the findings of fact.

# Art. 18 Reg. 1543 · where, when, how to challenge

## WHERE

In the issuing state

before a court

having full review power

Safeguards in the executing state

are without prejudice

## WHEN

Same deadlines as for

comparable domestic measures

Defence rights apply at

evaluation of evidence

in criminal proceedings

## HOW

Challenge legality

Challenge necessity

Challenge proportionality

+ rights under GDPR

+ rights under LED (2016/680)

⚠ **The biggest practical risk: the data subject is informed AFTER the data has been transferred.** ***Anticipation > reaction.***

# Art. 12 Reg. 1543 · the executing state's veto — your client's shield

**(a)** **Immunities & privileges**

Including legal professional privilege & press freedom rules of the executing state.

YOUR MAIN GROUND

**(b)** **Manifest violation of a Charter right**

Exceptional cases · concrete & objective evidence · Art. 6 TEU + Charter.

**(c)** **Ne bis in idem**

Same offence already finally adjudicated in another Member State.

**(d)** **Double criminality**

Outside the Annex IV catalogue · 3-year minimum sentence threshold in the issuing state.

*Recital 47: "the lawyer's professional secrecy … the journalist's sources …" — explicitly named protected categories.*

# Art. 13 Reg. 1543 · the most under-discussed safeguard

**THE RULE**

The issuing authority MUST inform the data subject without undue delay — including information about available legal remedies.

**THE EXCEPTIONS**

Defer · restrict · withhold — under conditions of Art. 13(3) Dir. 2016/680: ongoing investigation, public security, protection of others, judicial proceedings, third-state interest.

**FIVE QUESTIONS THE LAWYER MUST ASK THE PROSECUTOR**

1. When did the EPOC/EPOC-PR issue?
2. Who issued it? Validation by judge/court?
3. What categories of data? Subscriber / traffic / content?
4. Has the executing state been notified? When?
5. **Has my client been informed? If deferred, on what ground?**

PART III

*Ethics is the firewall when the law is in flux*

# Lawyers' Ethics

Independence · confidentiality · LPP · AI · cybersecurity — the duties that cannot be outsourced.

# Five ethical pillars — re-read for the digital age

## 1 Independence

From state, from the client, from the platform.
No cloud lock-in that compromises judgment.

## 2 Confidentiality

Absolute · perpetual · extends to all communications, metadata, files.
CCBE Model Code, Art. 2.3.

## 3 Loyalty to client

Avoid conflict — including conflicts arising from shared software vendors or AI tools.

## 4 Integrity

Truth to the tribunal · authenticity of evidence · no fabricated AI sources.

## 5 Competence

Continuing legal AND technological education.
Cyber-literacy is now part of the practice.

*Sources: CCBE Charter of Core Principles · CCBE Model Code 2021 · Statutul profesiei de avocat (RO) · Codul deontologic UNBR.*

# Why LPP is the lawyer's single most powerful procedural shield

**LPP today covers:** the content of communications, the metadata, the identity of the client, the existence of the relationship, the platforms used. *(CCBE, 2024)*

| WHO | WHAT | WHERE | DURATION |
|---|---|---|---|
| Lawyer admitted to a Bar in the EU · acting in legal capacity. | Information given or obtained in the context of legal advice or defence. | On any device, in any storage, in any jurisdiction — privilege travels with the data. | Indefinite — survives the end of the mandate, the death of the client. |

**Recital 47 + Art. 12(1)(a) Reg. 1543:** your client's data, held by a service provider, can be refused on LPP grounds — but only if you flag it in time.

# What the European Bars say — and what we must implement

## BARS / INPPA MUST

- Publish guidance on EPOC handling
- Maintain emergency contact lists 24/7
- Train lawyers on Reg. 1543 and Dir. 1544
- Engage with ANCOM as Central Authority
- Define LPP-flagging protocols for service providers
- Audit own cloud and communication infrastructure

## INDIVIDUAL LAWYERS MUST

- **Encrypt at rest and in transit (end-to-end)**
- **Vet cloud providers (location, sub-processors)**
- **Maintain segregation: client data ≠ AI training**
- **Pre-emptive LPP notification to providers**
- **Continuing training: cyber, AI, digital forensics**
- **Insurance: cyber and professional liability**

*Sources: CCBE 2024 Recommendations on e-Evidence Regulation · CCBE 2016 Surveillance Recommendations · CCBE 2019 CLOUD Act Assessment.*

# ChatGPT, Claude, Copilot · the new ethical frontier

## OPPORTUNITIES

- ✓ Drafting standard pleadings & motions
- ✓ Summarising long case-files
- ✓ Multilingual translation (verified)
- ✓ Legal research first pass
- ✓ Predicting procedural timelines

## RISKS

- ✗ **Confidentiality breach via consumer LLMs**
- ✗ **Hallucinated citations (fictional case-law)**
- ✗ **Bias and discrimination amplified**
- ✗ **Cross-border data flows triggering US/CN access**
- ✗ **AI Act high-risk classification for justice tools**

*Reference: EU AI Act (Reg. 2024/1689) · Annex III(8) — administration of justice = HIGH RISK · FBE Guidelines 2.0 (Sep 2024).*

# Remote hearings & confidential client communication

### Effective participation

The accused must be able to hear, follow, and react to the proceedings — Sakhnovskiy v Russia.

### Counsel access

Confidential, secure, real-time channel with the lawyer — separate from the public stream.

### Reasoned decision

Domestic court must justify why a video link is used — Marcello Viola v Italy.

### Technical reliability

Court adjourns if quality fails — Bivolaru v Romania (2017) for remote hearings.

*Reference: ECHR Guide on Art. 6 (criminal limb) · CEPEJ Videoconferencing Guidelines (2021) · Reg. 2023/2844 on digitalisation of judicial cooperation.*

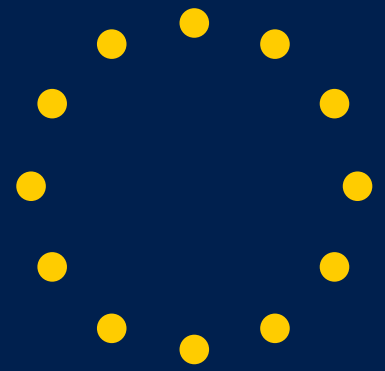
# The lawyer as the first line of digital defence

| | | |
|---|---|---|
| 1 | **Strong authentication** | MFA on all devices and platforms — including phone and shared calendars |
| 2 | **Encryption at rest & transit** | Full-disk encryption · S/MIME or PGP · encrypted messengers (Signal, Threema) |
| 3 | **Data segregation** | Client files separate from personal cloud · no auto-sync to consumer storage |
| 4 | **Incident response plan** | Documented procedure · notification to the Bar within 72h · GDPR breach analysis |
| 5 | **Vendor due diligence** | Written DPA · sub-processor list · location of servers · audit rights |

***Failing these duties is no longer just bad practice — it can amount to professional misconduct under Art. 39 of the Romanian Lawyers' Statute.***

PART IV

*Theory becomes muscle memory*



# Practical Toolkit

Checklists, red flags, and exact phrases you can use in your next file — starting tomorrow.

# For the digital criminal defence lawyer (print it · pin it)

1. Did I receive a notification under Art. 13 Reg. 1543? When?
2. Who is the issuing authority? Was the order validated by a judge?
3. What category of data — subscriber, traffic, content?
4. Was the executing state notified for traffic or content data?
5. Has my client been informed? If deferred, on what specific ground?
6. Is any of the requested data potentially privileged (LPP)?
7. Did I flag LPP to the service provider in writing — pre-emptively?
8. Have I prepared an Art. 18 challenge — in the issuing state?
9. What is my GDPR / LED parallel strategy (access, rectification, erasure)?
10. Is my own infrastructure compliant — would my files survive an EPOC?

5 RED FLAGS

# When to challenge an EPOC / EPOC-PR — triggers for Art. 18 action

| | | |
|---|---|---|
| 1 | **Prosecutor-only validation of content data**<br>Reg. 1543 art. 4(2) requires judicial validation. Prokuratuur reinforces it. | *C-746/18* |
| 2 | **No notification of the executing state for traffic/content**<br>Mandatory under art. 8 Reg. 1543. EncroChat: notification is the linchpin. | *C-670/22* |
| 3 | **Privileged data not flagged or screened**<br>Art. 12(1)(a) + recital 47 → grounds for refusal not exhausted. | *Reg. 1543 art. 12* |
| 4 | **Disproportionate scope ("all e-mails for 5 years")**<br>La Quadrature: proportionality requires targeted, time-limited measures. | *C-470/21* |
| 5 | **Defendant cannot effectively comment on the evidence**<br>EncroChat test: exclusion required when impact on findings of fact is significant. | *C-670/22, para 130* |

CLOSING

# The lawyer is the human firewall.

*When the data crosses borders in seconds, only ethics, training and vigilance protect the client.*

**1 Anticipate**

Audit your client's cloud. Audit your own.

**2 Invoke**

Charter rights + Reg. 1543 grounds of refusal + CJEU case-law.

**3 Document**

Every step, every notification, every refusal — written.

***Q & A · 4 minutes · Thank you.***

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

Daniela Zaharia Manescu

# Videoconferencing and remote hearings in criminal proceedings

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

Co-funded by the EU

- Introduction: Advantages and Risks
- Relevant European Framework
- Procedural Safeguards and Fundamental Rights
- National Regulation (Romania)
- Hearing Minors via Videoconference – RNA National Report 2025
- The Experience of Minors and Professionals
- Practical Recommendations
- Best Practices for Lawyers
- Conclusions

# Advantages

- **Procedural efficiency and cost reduction;**
- **Protection of detainees and vulnerable persons;**
- **Acceleration of cross-border judicial cooperation;**

# Risks

- **Possible impairments of the right to a fair trial;**
- **Technical and confidentiality issues;**
- **Difficulties in assessing credibility and emotional state;**
- **Possible negative impact on minors; (RNA Report)**

# General European Framework

- **Regulation (EU) 2023/2844 – the central act of the digitalization of justice;**
- **Directive 2014/41/EU (European Investigation Order) – Art. 24;**
- **EU Charter of Fundamental Rights – Art. 47 and Art. 48;**
- **2000 Convention on Mutual Assistance in Criminal Matters;**

**Minimum guarantees: confidentiality, interpretation, consent, effective participation;**

# Regulation (EU) 2023/2844 – Art. 6

- **Regulates hearings by videoconference in judicial cooperation in criminal matters;**
- **Applies specifically to: EAW (European Arrest Warrant), EIO (European Investigation Order), recognition of judgments;**
- **Provision of information regarding the procedure for conducting a hearing via videoconference or other distance communication technology and regarding one's procedural rights (e.g., right to a lawyer and interpreter);**
- **Ensuring confidential communication with the lawyer;**
- **Voluntary and unequivocal consent;**

**Exception: Without prejudice to the principle of a fair trial and the right to a remedy under domestic procedural law, the competent authority may decide not to request consent if participation in an in-person hearing represents a serious threat to public security or public health, which is proven to be real and present or foreseeable.**

- Minimum technical quality + remedies for incidents;
- Access to infrastructure;
- Increased attention to persons with disabilities;
- Hearings of minors – informing the holder of parental responsibility;
- The best interests of the child;
- Respect for fundamental rights (Art. 47-48 of the Charter);
- Stored in a secure manner and not broadcast publicly;
- The possibility of resorting to an effective remedy in case of violation of the guarantees provided for in Art. 6;

# Directive 2014/41/EU – Art. 24
# European Investigation Order (EIO)

- **Possibility of hearing witnesses via videoconference, if the person is on the territory of another Member State and their physical presence is not appropriate;**
- **Possibility of hearing suspects or accused persons via videoconference is permitted, but may be refused by the executing state if it would be contrary to the fundamental principles of its law;**
- **Refusal of execution – only in exceptional cases;**
- **Obligation to comply with Art. 6 ECHR standards and the EU Charter;**
- **Ensuring interpretation and legal assistance;**
- **Presence of the authority for identity verification;**
- **The hearing is conducted directly by the judicial authority from the state that issued the order (e.g., a Romanian judge), according to its national law;**
- **The right to invoke the privilege against self-incrimination (right to remain silent);**
- **The executing state may refuse the videoconference if: The person whose hearing is requested does not consent in limited cases, or there are no technical means available for a secure and high-quality transmission.**

# Romanian Regulation

**Criminal Procedure Code:**

- **Art. 106 para. (2) – A person in detention can be heard at the place of detention via videoconference, in exceptional cases and if the judicial body considers that this does not prejudice the proper conduct of the trial or the rights and interests of the parties.**
- **Art. 364 – the defendant can participate in the trial of the case via videoconference (may request the trial of the case in absentia).**
- **Art. 597 – participation of a convicted person who is in detention or interned in an educational center via videoconference with their consent and in the presence of a chosen or court-appointed defense counsel and, as the case may be, an interpreter.**

**! On May 6, 2026, the Chamber of Deputies adopted the draft law to amend the article – participation via videoconference will become the rule. The convicted person will be present in the courtroom only if the court expressly requests this.**

- **Special procedure for minors (Art. 506-510 CPP):**
- **Law no. 302/2004 international cooperation – Regulates hearings via videoconference within international judicial cooperation in criminal matters.**
- **Law no. 682/2002 on witness protection – Regulates the hearing of the protected witness via videoconference, with distorted voice and image to prevent identification.**
- **Law no. 211/2004 on the protection of victims of crimes – Provides for the possibility that the victim be heard without being present in the same room as the defendant, to avoid re-traumatization (secondary victimization).**
- **Law no. 254/2013 on the execution of sentences – the right of detainees to communicate with the courts through videoconferencing systems.**
- **Regulation (EU) 2023/2844 (Art. 6): Directly applicable to cross-border cases regarding digitalization.**

# Principles for Conducting a Videoconference

- **Procedural equivalence:** The hearing by videoconference must offer the same guarantees of legality and solemnity as physical presence;
- **Consent (general rule):** In most cases, the hearing requires the person's agreement (with the exception of convicted persons in detention, according to the law of May 6, 2026);
- **Confidentiality of the defense:** Ensuring a private communication line between the defendant and the lawyer, which cannot be intercepted by the court or the place of detention;
- **Opportunity and legitimate purpose:** The court must justify why the remote hearing is necessary and whether it does not affect the discovery of the truth;

# Mandatory Procedural Guarantees: Participant Rights

## Defendant

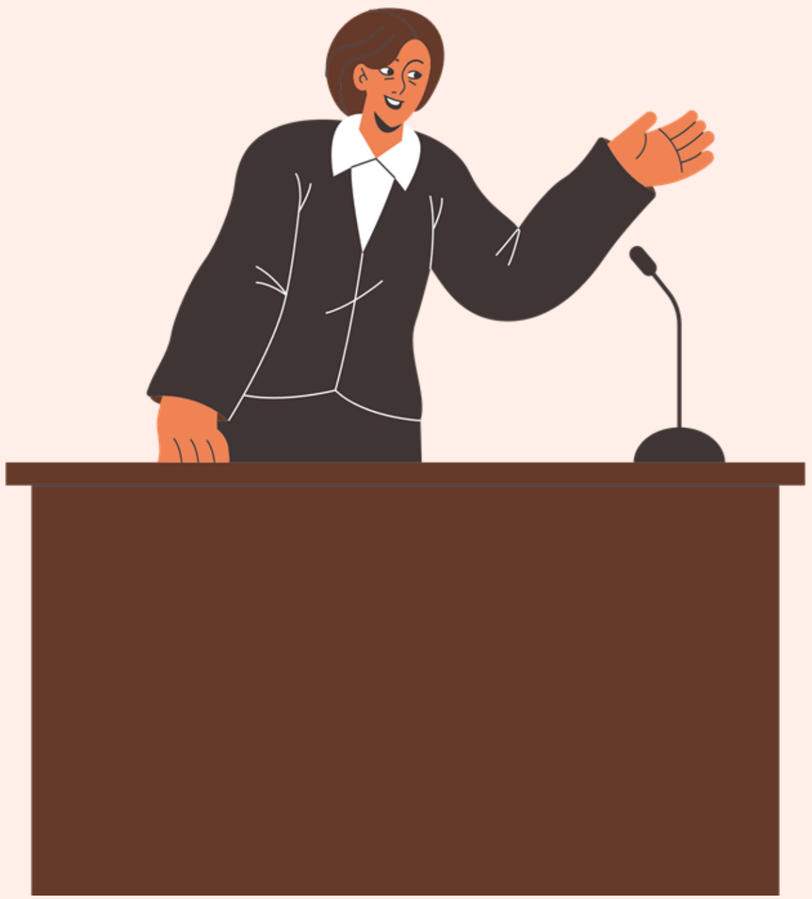
- Presence of a lawyer;
- Confidential lawyer-client communication;
- Free interpretation;
- Minimum technical quality + documentation of incidents;
- Right to procedural objections;
- Right to simultaneously see and hear all parties, witnesses, and the court;
- Right to refuse videoconferencing in cases that do not concern the sentence execution phase (with exceptions provided by law);

## Victim

- Right to identity protection (protection measure – vulnerability or threat);
- Videoconferencing facilitating voice and image distortion (protection measure);
- Hearing from a friendly environment;
- Right to be heard in a safe environment, avoiding direct visual contact with the defendant if necessary (vulnerability – special rights);
- Lawyer – injured person confidentiality;

## Witness

- Right to be assisted by a lawyer at the place of the hearing;
- Right to identity verification by a judicial authority at the place of residence.



# Hearing of minors via videoconference in Romania
# RNA National Report – "Protecting Procedural Rights of Children in the Digital Age" (2025)

- **51 specialized rooms for minors created in 2023**
- **Significant increase in online participation post-COVID**
- **Implementation is not uniform – practice differs from one court to another**

**Essential recommendations:**

- **The minor's right to choose physical or online participation;**
- **Mandatory presence: lawyer + legal representative + psychologist / social worker;**
- **Assessment of emotional state before the hearing;**
- **Friendly rooms, soundproofed, with a stable connection;**
- **Development of a unified national protocol for online hearings of minors;**
- **Continuous training for all professionals;**
- **Verify technical and confidentiality conditions before the hearing;**
- **Request the presence of the psychologist / social worker in the minor's room;**
- **Document any technical or procedural incident;**
- **Insist on the minor's right to choose the method of participation;**
- **Prepare the minor in advance (simple explanations + simulation)**

# If the testimony is interrupted:

- Suspension of the court hearing (if applicable);
- Technical remediation;
- Resumption of the testimony;
- Postponemet of the case;
- Mentions in the court record (minutes of the hearing);

## Advantages

- **Celerity (Speed of Proceedings):** Reduces trial terms by eliminating the need for transporting persons.
- **Reduced Costs:** Savings for the state budget (escort and transport expenses).
- **Security:** Eliminates the risks of escape or incidents during the transfer of detainees.

## Disadvantages

- **Perception Limitations:** Difficulty in fully observing the non-verbal language of the person being heard.
- **Technical Issues:** Risks of poor connection or equipment failure.
- **Procedural Coldness:** Diminishing the solemnity of the court hearing.
- **Reduced response time;**

## Minimum mandatory standards for videoconference hearings

- **Secure channels:** The transmission must be carried out through private networks or encryption protocols (VPN or dedicated platforms such as e-CODEX for cross-border matters) to prevent interceptions.
- **Separate line for the lawyer:** The defendant must have a private means of communication (secure telephony or encrypted chat channel) to discuss with their lawyer, without the court or database personnel being able to intercept the discussion.
- **Real-time transmission:** Image and sound must be transmitted simultaneously, without delays that affect the understanding of the testimonies.
- **Resolution:** Sufficient video quality is required to allow for the identification of the person and the observation of facial expressions (usually HD standard).
- **Acoustics:** Microphones must capture the voice clearly, and the sound system in the courtroom must allow all parties present to hear the person from a distance.
- **Recording:** The videoconference hearing is audio-video recorded, and the optical media is attached to the case file.
- **Identity verification:** At the location of the person being heard (prison, another court, or judicial headquarters abroad), there must be an official to verify the identity document before the connection begins.
- **Backup equipment:** Courts must have rapid technical support to remedy any connection failures; otherwise, the hearing will be suspended or adjourned.
- If the person being heard has hearing or speech impairments, the system must allow for the integration of an authorized interpreter into the video stream or the use of assistive technologies.

| Analysis Criterion | Directive 2014/41/EU (EIO) | Regulation (EU) 2023/2844 (Digitalization) | Romanian Legislation (CPP & Law 302/2004) | Compliance / Implementation Status |
|---|---|---|---|---|
| **Main Objective** | Obtaining evidence from another member state (including hearings). | Digitalizing the transmission of documents and participation via videoconference. | Administration of evidence and conduct of the trial. | Compliant. Romania transposed the EIO via Law 302 and adopted changes for 2023/2844 in 2026. |
| **Hearing of the Accused** | Permitted with consent; can be refused by the executing state. | Encourages the use of technology to reduce delays. | Art. 597 CPP (proposed amendment May 6, 2026): Videoconferencing becomes the rule for detainees, without required consent. | Partial divergence. Romania is more restrictive (or efficient) by eliminating detainee consent, while the EU emphasizes safeguards. |
| **Hearing of Witness/Expert** | Standard measure; does not require witness consent. | Establishes technical standards for connection quality. | Art. 126 & 345 Law 302: Aligned with EU standards for witnesses located abroad. | Compliant. The Romanian procedure strictly follows the European Investigation Order mechanism. |
| **Communication Channel** | Does not specify technology (initial email/mail). | Mandates the use of the e-CODEX system (decentralized, secure). | The draft law from Jan. 2026 implements the e-CODEX node in the Romanian judicial system. | Under implementation. Romania is in the process of total technical alignment (deadline May 1, 2025/2026). |
| **Attorney-Client Confidentiality** | Basic guarantee according to the EU Charter of Fundamental Rights. | Imposes technical requirements for private communication channels. | Recognized theoretically, but technically deficient in some prisons (lack of dedicated booths). | Partial non-compliance. Although the law provides the right, the infrastructure of some courts/prisons does not yet technically guarantee total secrecy. |
| **Grounds for Refusal** | Immunities, national security, fundamental rights. | Limits refusal to technical incapacity or violation of public order. | Law 302 lists the grounds from the Directive; internal CPP leaves it to the judge's discretion. | Compliant. The grounds for refusal in Law 302/2004 are a faithful mirror of the European ones. |
| **Right to Silence** | Must be guaranteed according to the laws of the issuing and executing states. | Does not substantially change the right, only the form of communication. | Art. 10 CPP – Explicitly guaranteed, including in the virtual environment. | Compliant. The Romanian judge has the obligation to inform the accused/suspect via video about |

Daniela Zaharia Manescu

# E-Evidence procedures

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

Co-funded by the EU

# Combating cybercrime

In Romania, in the year 2024, DIICOT sent 297 cooperation requests for cybercrime offenses (f
place).

## Cybercrime as a facilitator for:

- **Crimes within the sphere of organized crime;**
- **Infringement of intellectual property rights;**
- **Drug trafficking;**
- **Human trafficking;**
- **Terrorism and extremism;**

# Cross-border collection of electronic evidence – currently:

- To obtain electronic evidence from other states, we resort to forms of international judicial assistance in criminal matters (Law 302/2004 and the Code of Criminal Procedure);
- The use of judicial cooperation forms involves procedural formalities;
- Passing through a period of time during which there is a risk of evidence disappearing or being altered;
- The necessity of identifying, preserving, and obtaining computer data with maximum celerity;
- Differences between the legal systems of member states can lead to execution difficulties, delays, or refusals to preserve or transmit computer data;
- Available mutual legal assistance instruments do not include specific norms regarding computer data;
- Direct cooperation between judicial authorities and service providers can take place on a voluntary basis; they could refuse, could provide only partial information, or may notify the person concerned; there are no coercive means to enforce it.

# The e-Evidence Context

- **Regulation (EU) 2023/1543** (applicable and mandatory from August 18, 2026);
- **Regulation 2023/1543** represents a major paradigm shift: from slow cooperation to rapid cross-border access;
- Provides national judicial authorities with effective means for obtaining electronic; evidence, while establishing strong safeguards to ensure a high level of protection for the rights of affected persons;
- **New instruments**: preservation orders and production orders for electronic evidence;
- Increased efficiency for authorities, but significant risks to the rights of the accused;
- The lawyer plays an essential role in ensuring balance and compliance with procedural safeguards;
- Exponential growth of electronic evidence in criminal investigations (email, messaging, cloud, data traffic, etc.);
- **Old problems**: MLA (Mutual Legal Assistance) – average duration of 10 months
- Fast, direct, and secure access to cross-border electronic evidence
- **Directive (EU) 2023/1544** – designation of authorities and provider representatives

# Regulation (EU) 2023/1543: Key Elements

- **Regulation (EU) 2023/1543**, adopted on July 12, 2023, represents an essential legal instrument of the European Union, designed to accelerate the obtaining of electronic evidence in criminal proceedings.
- **European Production Order (EPOC)**
- **European Preservation Order (EPOC-PR)**
- **Applies to service providers** offering services in the EU (regardless of data location);
- **Communication** via a secure decentralized IT system;
- **Short deadlines**: 10 days (normal) / 8 hours (emergency);
- **Applicable** in criminal proceedings and the execution of custodial sentences;

# European Production Order (EPOC)

- Allows a judicial authority from one Member State to directly request a service provider (established in another Member State) to produce electronic evidence (subscriber data, traffic data, content data) without the need for formal mutual legal assistance.
- An order issued by the issuing judicial authority to a service provider in another Member State.
- Obligation to produce (~~transmit~~ → ) the requested electronic evidence.
- Conditions: proportionality + necessity + respect for fundamental rights.

# European Preservation Order (EPOC-PR)

Data preservation order (prevention of deletion)

Allows authorities to request the rapid preservation of electronic data by a service provider to prevent its deletion before a disclosure request is sent

Duration: 60 days (extendable by another 30 days)

Followed by a Production Order or another instrument (EIO, MLA)

Useful in cases where there is an imminent risk of evidence being deleted

Rapid and simplified procedure

# Guarantees and Protections

- An order can only be issued if a similar measure would have been available for a similar offense in a purely internal case, ensuring the principle of equality.
- **Proportionality and necessity** (Art. 5-6).
- **Informing the person concerne**d (Art. 13) – without undue delay.
- **Right to effective remedies** (Art. 18).
- **Right to efficient legal remedies**: Any person whose data has been requested has the right to an efficient legal remedy against the order, exercised before a court in the **issuing state**.
- **Rights of defense**: The suspect or the accused person (or their lawyer) may request the issuance of a production or preservation order as part of their right to defense, in accordance with national legislation.
- **Professional privilege**: The service provider or the executing authority may refuse disclosure if the data is protected by **immunities or privileges** (e.g., the professional secrecy of lawyers or doctors) or by rules regarding press freedom.
- **Notification of the executing state**: For traffic and content data, the state where the provider is located is notified and can raise objections if the order violates fundamental rights or national immunities.
- **Confidentiality and data protection** (GDPR + LED).
- **The possibility for the suspect/defendant or the lawyer to request the issuance of an order**.
- EU Charter Art. 7, 8, 47, 48 + Art. 6 ECHR.

# Transposition of Directive 2023/1544

- The normative act establishes the obligation for electronic service providers (which do not have a headquarters in Romania but offer services here) to designate a **legal representative** or a **designated establishment** on EU territory for receiving and executing production orders for electronic evidence.
- Romanian authorities **no longer need to send slow letters rogatory to other states**; they can directly contact the designated representative of the company (e.g., Google, Meta, cloud providers).
- The draft law provides for harsh sanctions for providers who do not designate a legal representative within the legal timeframe.
- It establishes exactly who is responsible for receiving judicial requests, eliminating ambiguities related to headquarters located outside the EU.
- **Elimination of exhaustive translations**: In the EIO (European Investigation Order) system, the entire request file had to be translated into the language of the respective state. Under the Regulation, **standardized forms** (EPOC Certificate) are used, which are much simpler and faster.
- **Prosecutor's Responsibility**: In Romania, the prosecutor gains increased power to interact with private entities across borders without going through the Ministry of Justice or foreign central authorities for every request.
- **Conflict of laws**: The Regulation offers a clear procedure for situations where a provider (e.g., an American company with headquarters in Romania) receives an order that conflicts with US laws—a situation not specifically covered by the CPP (Code of Criminal Procedure).

# Regulation in Romania

- The draft law for the implementation of Regulation (EU) 2023/1543 in Romania was **adopted by the Government in the session of April 16, 2026**;
- The transposition of Directive 2023/1544 (deadline: February 2026) is in the **final stage of adoption**;
- Expected changes in the Code of Criminal Procedure (electronic means of evidence and international cooperation);
- **Issuing authorities**: prosecutors and courts;
- The role of service providers (Meta, Google, Apple, Microsoft, etc.) — designating a legal representative in the EU;
- Connection with the **ECRIS platform** and PNRR (National Recovery and Resilience Plan) **projects for the digitalization of justice**.

# The draft normative act contains regulations regarding:

- **Norms regarding the designation of competent Romanian authorities** (issuing and for execution) of the procedures for issuing, transmitting, and executing preservation and production orders for electronic evidence;
- **Settlement of legal remedies** formulated by persons whose data is requested;
- **Procedure** in cases where the recipient does not comply with the order;
- **Judicial review procedure** requested by the provider in case of conflicting obligations;
- **Designation of central authorities;**
- **Procedures** for the urgent settlement of objections;
- **The possibility of sanctioning a recipient who does not comply** with a European preservation or production order for electronic evidence without providing accepted reasons to the issuing authority and without the executing authority having invoked any reason for refusal (judicial fine – 100,000 lei and 2% of the annual global turnover recorded by the service provider in the preceding financial year);
- **Transitory provisions;**

# According to the draft normative act:

The European Production Order for electronic evidence to obtain subscriber data, or to obtain data exclusively for the purpose of identifying the user, or data referring to content:

- By a prosecutor through an ordinance during the criminal investigation, or by a judge through a decision during the trial or after conviction;
- For any offense;
- In the cases provided for in Art. 3 para. (1) point 18 of the Regulation, production orders can be issued by the prosecutor without the judge's authorization;

Within 48 hours, the prosecutor shall notify the judge for the purpose of confirming the order;

The judge shall rule within 24 hours through a reasoned interlocutory order, pronounced in chambers, without summoning the parties.

The judge confirms or invalidates [the order] and orders the immediate withdrawal with the deletion or restriction of the use of the obtained data.

# According to the draft normative act:

The transmission by Romanian authorities of European preservation orders for electronic evidence and production orders for electronic evidence:

- The orders are transmitted directly by the issuing authority to the designated establishment or legal representative of a service provider offering services in the European Union, within the meaning of Art. 3 of the Regulation, via the order certificate;
- The certificates will be translated at the request and expense of the issuing authority into an official language accepted by the recipient or, in the absence of such information, into the official language of the Member State where the designated establishment or legal representative is located;
- Any communications or consultations necessary for the execution of European production or preservation orders for electronic evidence take place directly;
- If a foreign executing authority decides to invoke any ground for refusal from those provided for in Art. 12 of the Regulation, the issuing Romanian judicial authority, following consultations with the executing authority, may decide to withdraw or adapt the order;

# Execution by Romanian authorities of European production orders for electronic evidence:

- Romanian executing authorities in the criminal investigation phase – the prosecutor's offices competent according to Romanian law;
- In the trial phase or the execution phase of a sentence or a custodial measure of at least 4 months – the trial courts competent according to Romanian law;
- The prosecutor rules by ordinance;
- The court rules by a reasoned interlocutory order, in chambers, without summoning the parties and without the participation of the prosecutor. The interlocutory order is final from the date of pronunciation;
- The ordinance or interlocutory order is communicated immediately to the recipient and the issuing authority, no later than 10 days from the date of receipt of the notification;
- In applying Art. 10 of the Regulation, in urgent cases, if we are in the presence of a refusal, the ruling will be made within a maximum of 96 hours and the recipient and the competent authority will be notified immediately;

**OBS:** before invoking any refusal, the Romanian executing judicial authority shall consult, by any appropriate means, with the issuing authority.

In case of notification to the Romanian executing authority, the European production order will be translated into Romanian, English, or French. In urgent cases, the translation will be done exclusively in the Romanian language.

# Legal Remedies

- **Opposition by the person concerned**: The person whose data is requested, if informed regarding its disclosure, may file an opposition in accordance with Art. 18 of the Regulation.
- **Submission deadline**: The opposition is submitted in writing to the issuing authority within 3 days from the date of receiving the information.
- **Resolution during criminal investigation**: During the criminal investigation phase, the opposition is resolved within 48 hours by the chief prosecutor/first prosecutor through a reasoned ordinance.
- **Resolution during trial or execution**: During the trial phase or the execution phase of a sentence or a custodial measure of at least 4 months, the opposition will be resolved by the hierarchically superior court within 48 hours in chambers, with the participation of the prosecutor and the summoning of the recipient.
- **Finality**: The interlocutory order is final.
- **File handling**: The file will be forwarded and returned within 24 hours.

- **Art. 8 of the draft normative act** also regulates the procedure in the event that the recipient does not comply with a **European Preservation Order** or **Production Order** for electronic evidence, as follows:
- The **prosecutor** issues a ruling by way of an **order**;
- The **court** [issues a ruling] through a **reasoned interlocutory judgment** in chambers, without summoning the parties and without the participation of the prosecutor. The interlocutory judgment is **final**;
- The **Romanian executing authority** immediately requests the recipient to fulfill their obligation;
- The **recipient** may submit **objections** within **48 hours**;
- The objections are resolved within **48 hours**;
- If the Romanian executing authority finds that the recipient has **unjustifiably failed to comply** with the obligations incumbent upon them under **Art. 10, 11, and 13 para. (4)** of the Regulation, it may impose a **judicial fine** of at least **100,000 lei**, but not exceeding **2% of the total annual turnover** recorded by the service provider at a **global level** in the preceding financial year.

# Central Authorities

Specific Romanian central authority duties in the application of the Regulation are exercised by:

- **The Ministry of Justice** through its specialized department;
- **The Prosecutor's Office attached to the High Court of Cassation and Justice** through its specialized structures;

# The Lawyer's Role in the e-Evidence Procedure

- **Verifying the legality of the order** (proportionality, competence, reasoning);
- **Invoking immunities and professional privilege** - The lawyer must ensure that the data requested by authorities does not violate **professional secrecy;**
- **Challenging the production / preservation order;**

**Example: Challenging an EPO (European Production Order)** - If the Romanian prosecutor issues an EPO, the suspect's lawyer will contest the measure before the **courts in Romania**.

- The lawyer ensures that the authorities **do not collect more data than is strictly necessary**.;
- **Requesting compensatory measures** or the **exclusion of illegally obtained evidence;**
- **Assisting the client** regarding information on data processing;
- **Using the order in favor of the defense** (requesting electronic evidence);
- **Requesting evidence in favor of the client ("e-Evidence for the defense");**

# Practical challenges

- The balance between investigation efficiency and fundamental rights
- Risks of mass surveillance and abuses
- Technical and confidentiality issues
- Differences in practice between Member States
- The impact on the lawyer's professional secrecy
- Insufficient preparation of practitioners (lawyers, prosecutors, judges)

# Best practices for lawyers

- Monitoring the issuance of e-Evidence orders in the case file
- Immediate verification of the notification to the client
- Filing reasoned challenge requests (proportionality, necessity)
- Documenting any rights violations
- Continuous training regarding digital cooperation tools
- Strategic use of e-Evidence in favor of the client

# Comparison of Current National Legislation vs. New EU Regulation 2023/1543

| Comparison Criterion | Current National Legislation (CPP & EIO) | New Regulation (EU) 2023/1543 |
|---|---|---|
| **Cooperation Model** | **Indirect (State-to-State):** The Romanian authority requests help from a foreign authority (e.g., BKA in Germany), which then requests data from the provider. | **Direct (State-to-Private):** The Romanian authority sends the order directly to the headquarters/representative of the provider (e.g., directly to Meta/Google in the EU). |
| **Order Recipient** | Another judicial authority (foreign prosecutor or judge). | The designated headquarters or the legal representative of the service provider. |
| **Execution Deadline** | **EIO:** 30 days for recognition + 90 days for execution (in practice, often much longer). | **Standard:** 10 days. **Emergency:** Maximum 8 hours (imminent danger to life/integrity). |
| **Data Location** | It is crucial. If data is on a server in another state, the classic cross-border procedure is mandatory. | Irrelevant. The provider must deliver the data regardless of where it is stored (cloud, external servers). |
| **Offense Criterion** | **EIO:** Any offense for which a warrant can be issued in the issuing state. | **Traffic/content data:** Only for offenses with a minimum 3-year sentence or cybercrime/terrorism. |
| **Role of the Executing State** | **Active:** The foreign authority verifies and executes the request according to its own laws. | **Passive/Supervision:** The host state is only notified and can intervene only for reasons of immunity or fundamental rights. |
| **Legal Remedies** | Challenged at the court that issued the measure (in Romania) or the one that executed it (abroad). | **Clarity:** The right to legal action is ensured in the Issuing State (Romania), regardless of where the data is located. |
| **Sanction Mechanism** | Diplomatic/Institutional (through Eurojust or the European Commission). | **Financial:** Member States (including RO) set fines of up to 2% of the provider's global turnover. |

Within the framework of the **e-Evidence Regulation (EU 2023/1543)**, obligations target a specific category of entities called **service providers**. Many Romanian companies in the tech, telecommunications, and online services sectors fall directly under the scope of this law.

**Which Romanian companies are targeted?**

1. **Electronic communications providers:**

- **Telecommunications operators (voice and internet):** Digi (RCS & RDS), Orange Romania, Vodafone Romania, Telekom.
- **Messaging and VoIP services (Over-the-Top):** Romanian chat applications or platforms, locally implemented customer support, domestic email services (e.g., hosting providers offering mail servers to clients, such as Găzduire.ro, Hosterion, Chroot).

**2. Internet domain name and IP address providers:**

- **Registries and registrars:** RoTLD (Romanian Registry for .ro domains), domain registration companies, and DNS/IP service providers.

**3. Information society service providers (Cloud and Digital Marketplaces):**

- **E-commerce platforms (online marketplaces):** eMAG (Dante International), Fashion Days, Olx.ro. These platforms store user data, messages between buyers/sellers, and traffic data.
- **Cloud and Web Hosting providers:** Romanian companies offering data storage or hosting (e.g., M247, GTS Telecom, Synopsys).
- **Ridesharing and Delivery applications:** Bolt Romania, Uber Romania, Tazz, Glovo (their local legal entities that process data regarding users, routes, and transactions).

Alexis Anagnostakis

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

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

Co-funded by the EU

## The First Remote Criminal Trial in Greece

**January 2026** — Mixed Jury Court of Syros

Three witnesses testifying live from the Greek Embassy in Dublin.

Press cameras. Excitement. A palpable sense of history.

Then the link started.

The smiles froze.

The image froze.

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

*— Alexis Anagnostakis*

## SECTION 2 — THE LEGAL FRAMEWORK: ARTICLE 238A CCP

### What the Law Says

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

Physical attendance remains the default.

Videoconference is the exception.

### Who Can Order It

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

A threshold must be met.

***→ This is where the protection gap begins.***

### What Has Changed in Practice

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

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

SECTION 3 — THE PROTECTION GAP

# Four Concrete Vulnerabilities

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

# 1 Vulnerability 1 — The Defendant Is Not Notified

## The Problem

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

## Why It Matters

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

## In Practice

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

# 2 Vulnerability 2 — No Lawyer at the Remote End

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

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

**Who ensures the witness is not being prompted?**

**Who guarantees confidentiality?**

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

**ECtHR Standard**

Effective participation via videoconference requires:

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

# 3 Vulnerability 3 — Poor Technical Quality & No Remedy

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

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

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

### ⚠ The Syros Case

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

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

# 4 Vulnerability 4 — The Translation Compound Problem

**The Compound Failure**

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

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

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

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

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

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

- No dedicated interpretation channels
- No separate audio feed requirement

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

## Article 6 ECHR — The Three-Part Test

### Justified Case

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

### Legitimate Aim

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

### Effective Participation

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

**The Deeper Constitutional Question**

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

SECTION 5 — CONCLUSION

# What Justice Requires

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

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

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

**What we need is not less videoconferencing.**

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

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

Maitane Valdecantos

# Electronic case files and measures in response to the emergence of AI as key pillars of digital justice in Spain

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

Co-funded by the EU

# Justice Folder

# Carpeta Justicia (Justice Folder)

*Carpeta Justicia* is a personalised service that facilitates access to the services, procedures and information of the Administration of Justice.

It is designed for citizens when they are party to proceedings or can show a legitimate interest, as well as for professionals.

Its use requires prior identification by both the citizen and the authorised professional.

# Carpeta Justicia (Justice Folder)

It must ensure compliance with procedural law, confidentiality and data protection.

It is established as compulsory minimum content of the General Access Point of the Administration of Justice (Central integration).

# Carpeta Justicia: core functions

Personalised services | Information management | Access to the case file | Deployment models | Functional guarantee

It must provide access to service of documents (pending/ completed) and the option to sign them electronically.

# Carpeta Justicia: core functions

| Personalised services | Information management | Access to the case file | Deployment models | Functional guarantee |
|---|---|---|---|---|

It includes access to a personalised diary of procedural steps (hearings, deadlines), tailored information from the Single Judicial Notice Board and judicial appointment management.

# Carpeta Justicia: core functions

| Personalised services | Information management | Access to the case file | Deployment models | Functional guarantee |
|---|---|---|---|---|

It guarantees access to the Electronic Judicial Case File, enabling consultation of electronic documents.

# Carpeta Justicia: core functions

| Personalised services | Information management | Access to the case file | Deployment models | Functional guarantee |
|---|---|---|---|---|

It may be provided through a common centralised system managed by the Ministry of Justice or through decentralised services operated by the electronic judicial offices of each autonomous community.

# Carpeta Justicia: core functions

| Personalised services | Information management | Access to the case file | Deployment models | Functional guarantee |
|---|---|---|---|---|

If the autonomous communities opt for their own system, it must be interoperable and provide the same services as the State system, ensuring a single digital window for end users.

# Users' electronic identification and signature

The use of digital judicial services requires prior electronic identification, ensuring that users are properly authenticated before carrying out any procedural action.

Electronic identification and signature systems, governed by national legislation and the eIDAS Regulation, guarantee the validity, integrity and authenticity of digital acts.

Electronic signatures certify the user's intention and consent.

# Users' electronic identification and signature

Under our national legislation, citizens may access services using the electronic National Identity Document and other authentication devices, while legal persons may act through electronic signatures or electronic seals.

The State Technical Committee for the Electronic Judicial Administration (CTEAJE) prepares essential technical guides which supplement the legal framework.

# Traceability and Legal Certainty

The Spanish justice system incorporates strict safeguards to ensure traceability, accountability and legal certainty.

Spanish legislation requires judicial systems to retain a record of all processing activities (collection, consultation, alteration and deletion of data).

This record must make it possible to identify the date/time, the operator and the justification for each operation.

# Traceability and Legal Certainty

Recording functions apply to every user interacting with the system, including maintenance staff and automated actions.

Any exceptional access to the systems requires prior authorisation from the competent court.

# Digital-First Judicial Proceedings

Spanish legislation establishes a digital-first model for judicial proceedings.

Filing documents, procedural communications and consultation of case files are generally carried out electronically, while procedural guarantees and formal legal requirements remain fully applicable.

The only significant exception concerns certain natural persons, who may still choose to communicate on paper.

# Procedural Safeguards and Deadlines

Procedural acts of communication must always be carried out by electronic means, subject to certain exceptions.

The issue of a filing receipt is guaranteed, recording the content, date and time of submission.

This ensures legal certainty where there are doubts about deadlines.

# Procedural Safeguards and Deadlines

The register operates twenty-four hours a day and throughout the entire year.

If a document is filed on a non-working day or at a non-procedural hour, it is deemed to have been filed at the first minute of the next working day.

# The electronic judicial case file

The electronic judicial case file constitutes the core element of digital judicial activity.

It integrates all documents, procedural actions and audiovisual recordings relating to a case, regardless of their original format.

Each case file includes an electronic index and a unique identification number, ensuring integrity, traceability and efficient management across the entire judicial system.

# Remote Proceedings and Digital Access

Spanish legislation also regulates remote appearances in judicial proceedings, particularly in criminal matters, while preserving procedural guarantees and the protection of vulnerable victims.

A new article is introduced to regulate remote appearance in criminal matters.

# Remote Proceedings and Digital Access

The defendant is required to appear in person at the seat of the judicial body in trials for serious offences and in Jury Court proceedings.

It is guaranteed that victims of gender-based violence, sexual violence, human trafficking, or child victims and victims with disabilities will always take part remotely.

# The Justice Folder mobile application

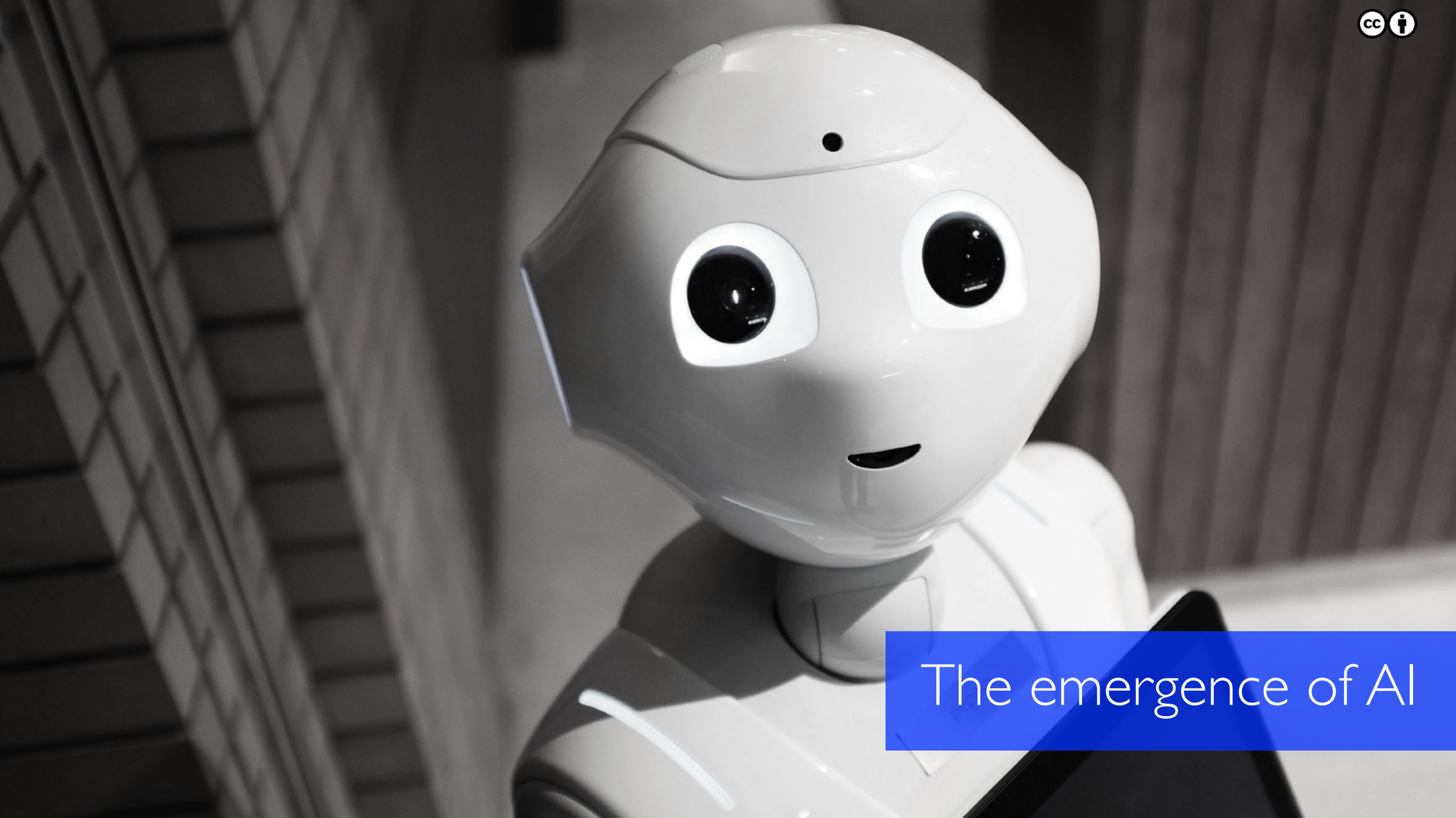
Citizens, representatives of legal persons and/or entities without legal personality, regulated justice professionals (lawyers, court representatives or social-labour law graduates) and other groups can access the Justice Folder mobile application through Cl@ve.

# The Justice Folder mobile application



If we tap on "folder", we see a menu with all the main options available in the mobile application:

- Upcoming events, hearing listings, judicial notice board, powers of attorney, case-file status, certificates, appointments and notifications.



# The emergence of AI

# Response of the CGAE

# Response of the General Council of Spanish Lawyers

The rapid development of AI has posed significant challenges to the legal profession, particularly in terms of professional responsibility and ethical standards.

In response, the CGAE has issued a White Paper on Artificial Intelligence and adopted Guidance Note 3/2026 to guide lawyers in the responsible use of these technologies.

# Purpose of the White Paper

The White Paper provides technical, legal and ethical guidance on the impact of Artificial Intelligence in legal practice.

It identifies the main uses of AI, analyses associated risks, and offers recommendations to ensure that its use remains aligned with professional standards, emphasising the need for human supervision.

# Purpose of the interpretative circular 3/2026

The Guidance Note 3/2026 addresses new professional risks arising from generative AI, particularly the submission of legal documents containing errors.

It clarifies how existing deontological rules apply to this new technological context, reinforcing professional obligations.

# Human oversight

# Core Principle: AI as an Auxiliary Tool

Both the White Paper and the Circular establish that Artificial Intelligence must function solely as an auxiliary tool.

Legal reasoning, decision-making and responsibility remain exclusively human tasks, requiring continuous supervision and control.

# Duty of Diligence and Professional Care

The use of Artificial Intelligence reinforces the lawyer's duty of diligence, integrity and professional care.

Lawyers must carefully review all AI-generated outputs and ensure their legal accuracy, as any lack of supervision may constitute a breach of professional duty.

# Hallucinations

# Duty of Verification

All AI-generated content must be critically verified before use.

This is essential because AI systems may produce plausible but incorrect information.

Failure to verify such content is considered a lack of diligence and may lead to disciplinary consequences.

# Responsible Use of AI Systems

Lawyers must use Artificial Intelligence in a responsible and informed manner, understanding its limitations and risks.

Blind reliance on automated outputs is incompatible with professional standards, and AI must remain subject to professional judgement.

# Confidentiality and Data Protection

The use of Artificial Intelligence must comply with professional secrecy and data protection obligations.

Lawyers must ensure that AI tools provide adequate safeguards to prevent the disclosure or misuse of sensitive client information.

# Non-Delegable Responsibility

The lawyer is solely responsible for any document they sign or submit, regardless of whether AI was used.

Responsibility cannot be transferred to technology providers, and arises from the lawyer's duty to supervise and verify all outputs.

# Disciplinary Liability and Sanctions

Improper use of Artificial Intelligence may result in disciplinary liability.

Submitting erroneous documents or failing to verify AI outputs may constitute a serious offence, and in severe cases, a very serious offence, depending on negligence and harm caused.

# Summary

Artificial Intelligence does not alter the fundamental principles of the legal profession.

On the contrary, it reinforces the need for diligence, supervision and accountability, as lawyers remain fully responsible for their professional actions at all times.

# Training will always prevail over sanctions


The General Council of Spanish Lawyers has complemented its response to Artificial Intelligence with a strong commitment to professional training and digital skills development.

# Digital Skills and Training for the Legal Profession

The UPRO programme was launched as a large-scale training initiative aimed at preparing lawyers for the technological transformation of the legal sector.

The programme offers 150 hours of specialised training in areas such as Artificial Intelligence, cybersecurity, digital justice, blockchain and data management, combining online and in-person learning.

# Response of the CGPJ

# Judicial Institutional Response to AI

As with the response adopted by the CGAE, the General Council of the Judiciary (CGPJ) has addressed the challenges posed by Artificial Intelligence through Instruction 2/2026.

Its approach is specifically focused on safeguarding judicial independence, the integrity of decision-making and the protection of fundamental rights within the exercise of judicial functions.

# AI as a support tool in judicial activity

In line with the approach taken for the CGAE, Artificial Intelligence is conceived as a support tool that may assist in tasks such as legal research, document analysis or case preparation.

Nevertheless, judging remains an exclusively human function that cannot be delegated to automated systems.

# Core Principles Governing the Use of AI

Similarly to the obligations imposed on lawyers, the Instruction establishes that the use of AI must be subject to human control, responsibility and strict limitations.

Judges must retain full control over the process and AI cannot operate autonomously in decision-making, fact assessment or legal interpretation.

# Specific safeguards: Judicial independence

Beyond general obligations, the Instruction introduces specific safeguards linked to the judicial function.

It emphasises the need to preserve judicial independence and to prevent any influence of AI on the judge's freedom of decision, while ensuring full respect for fundamental rights such as equality and non-discrimination.

# Specific safeguards: Authorisation and control

Unlike the regime applicable to lawyers, the Instruction establishes a stricter regime for judges.

They may only use AI systems that have been officially provided or authorised by competent authorities, and these systems must be subject to quality control and auditing.

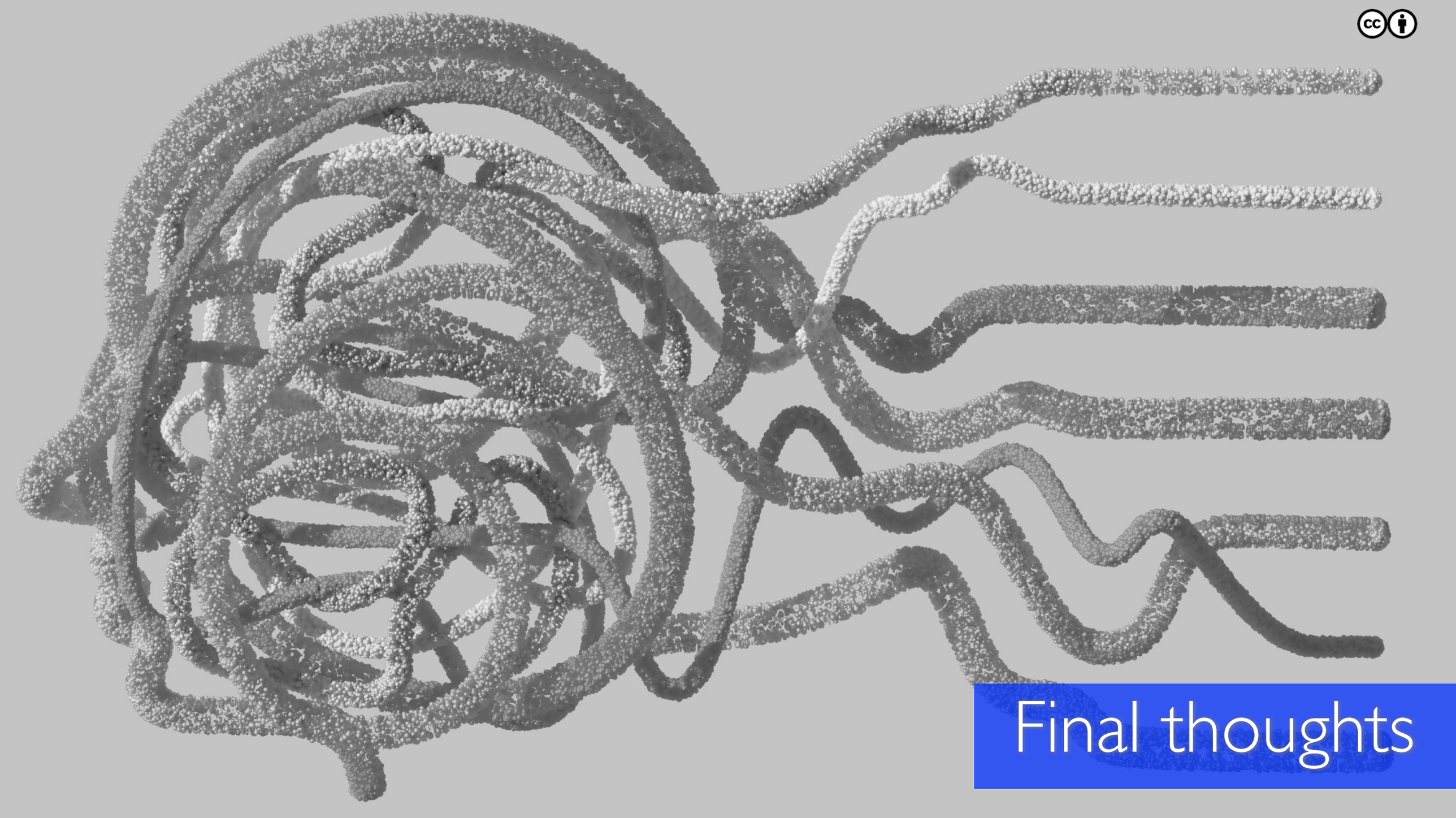
# Drafting of Judicial Decisions

AI may assist in drafting judicial decisions, but any draft must be subject to a complete, personal and critical review by the judge.

These drafts do not constitute automated decisions and must be freely modified before being validated as judicial resolutions.

# Summary

While both the CGAE and the CGPJ adopt a similar approach based on human control and responsibility, the use of AI in the judiciary is framed by stricter safeguards aimed at preserving independence, protecting fundamental rights and maintaining public trust in the administration of justice.



# Final thoughts

The danger is not that machines are becoming more and more like us.

The danger is that we start becoming like them.

# We are professions that uphold safeguards


HUMAN
RIGHTS
ARE NOT
OPTIONAL