

Paola Berta

Digitalisation of EU criminal law and electronic evidence: a comprehensive toolkit for cross-border digital litigation

Barcelona, 6 November 2026

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

Co-funded by the EU

The Digitalisation of EU Justice: A Borderless Paradigm



Co-funded by the European Union

Block 1 Interactive Scenario:

Question: If a national court issues a cross-border freezing or evidence request using legacy paper channels instead of mandatory digital systems under Regulation (EU) 2023/2844, can defense counsel challenge its validity?

Strategic Answer Reveal

Yes. Under Regulation 2023/2844, defense counsel can challenge procedural irregularity When mandatory secure channels like e-CODEX are bypassed, risks of data corruption, missing electronic timestamps, and chain-of-custody breaches emerge, creating valid grounds to request procedural review."

Co-funded by the European Union

Gemini Notebook

The Budapest Convention (2011): The Baseline Framework

Ratified by 70+ states, this remains the primary tool for international (non-EU) digital cooperation. Focuses on Authority-to-Authority transmission.

Step 1: Rapid Preservation (Art. 29)

Order to secure stored computer data to prevent deletion. Typically lasts 60 days to allow for a formal MLA request.

Step 2: Rapid Disclosure (Art. 30)

Releasing just enough traffic data to identify the service provider and the transmission route.

Step 3: Formal Access/Seizure

The subsequent, often slow, Mutual Legal Assistance (MLA) request to actually retrieve the data.

Limitation: Requires Dual Criminality and respects sovereign refusals (e.g., political offenses).

Co-funded by the European Union

The European Investigation Order (EIO)

1 Directive 2014/41/EU

Replaced the 2003 Framework Decision for evidence freezing. (Not applicable to Ireland/Denmark).

2 Art. 32.1: Provisional Measures

Issuance of an EIO to prevent the destruction, transformation, or transfer of an item used as evidence (Data Preservation).



3 Strict Deadlines

The requested state must communicate its decision on provisional measures within 24 hours of receipt.

4 Real-Time Collection

Arts. 28 & 30 cover real-time data collection, including the interception of telecommunications.

Co-funded by the European Union

Block 2 Interactive Scenario: The Ticking Clock



Scenario Card

The Scenario: You represent a Spanish company. A highly coordinated cyber-attack has siphoned funds. You trace the IP to a server hosted in Germany. The logs rewrite every 48 hours.

The Question: To urgently freeze the server logs and prevent deletion, do you advise the investigating judge to invoke the Budapest Convention or an EIO?

Answer Reveal

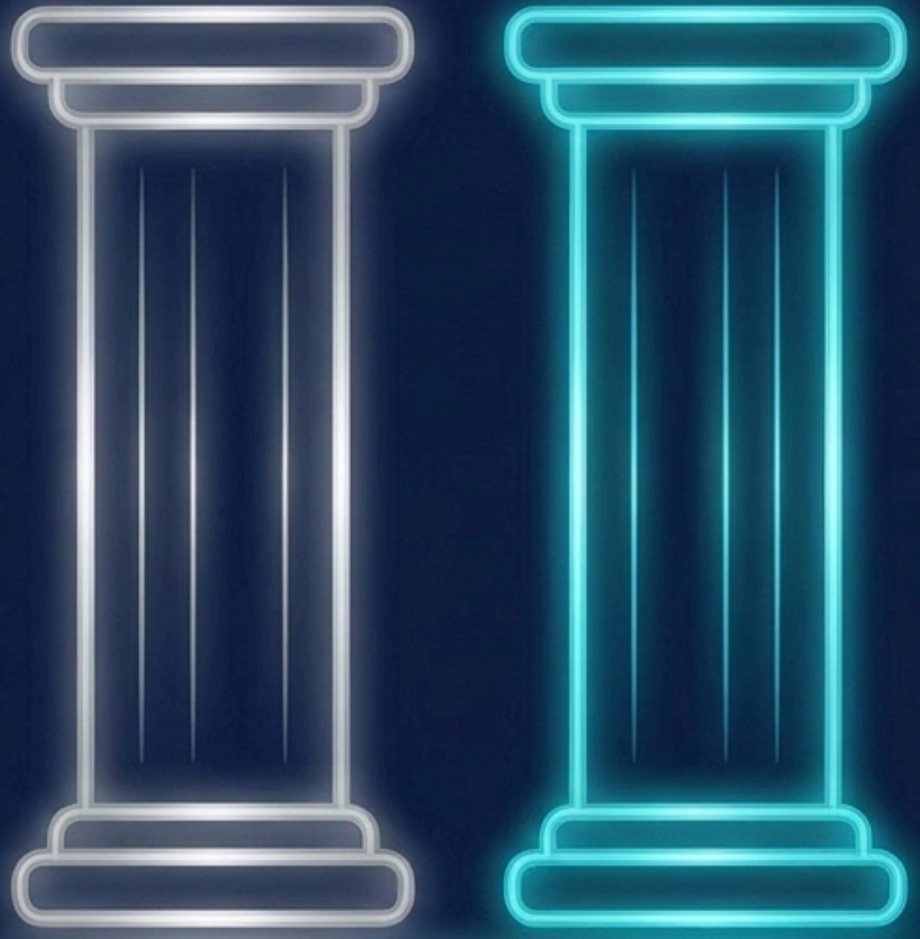
Strategic Answer: EIO (Art 32.1).

Because both are participating EU Member States, the EIO is the mandatory and fastest route. Germany must decide on the preservation measure within 24 hours. The Budapest Convention relies on slower MLA channels better suited for non-EU states.

Co-funded by the European Union

Digital Services Act (DSA): Intermediary Obligations

Applicable since Feb 17, 2024. Shifts the burden onto PSSI (Platforms, hosting, marketplaces) offering services in the EU.



Pillar 1: Reactive

Art. 10 - Orders for Information

- Providers must comply with specific orders from national judicial/administrative authorities.

- Orders must contain clear identification of the recipient, legal basis, and statement of reasons (proportionality).

Pillar 2: Proactive

Art. 18 - Notification of Suspicions

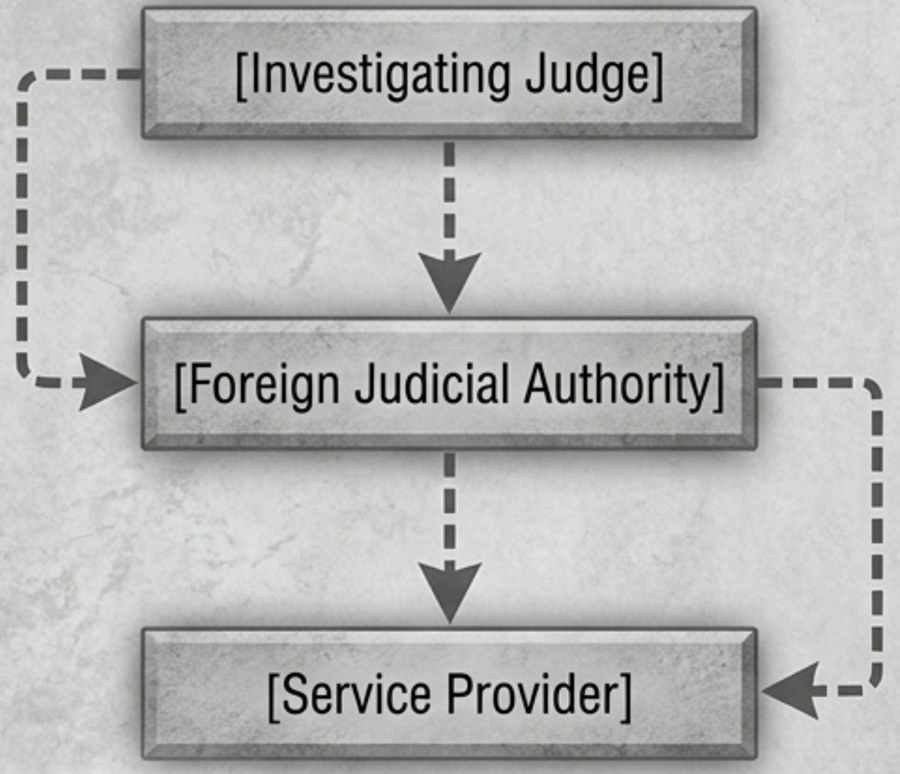
- Mandatory reporting if the platform suspects a criminal offense involving a threat to life or safety.

Co-funded by the European Union

The E-Evidence Revolution (Applicable Aug 18, 2026)

Regulation (EU) 2023/1543 & Directive (EU) 2023/1544: A fundamental paradigm shift.

The Old Method: Authority-to-Authority (MLA)



The New Reality: Authority-to-Provider

[Investigating Judge]

[Provider's Designated EU Legal Rep]

Mandate: All providers offering services in the EU must designate a legal representative by Feb 18, 2026, to directly receive binding orders.

Co-funded by the European Union

EPOC vs. EPOC-PR: The New Certificates

EPOC

European Production Order Certificate

Function: Demands the direct production of specific electronic evidence (subscriber, traffic, or content data).

Speed / Deadlines:

– Standard execution: Provider must deliver the data within 10 days.
– Emergency cases (imminent threat to life): Deadline drops to 96 hours.

EPOC-PR

European Preservation Order Certificate

Function: Demands the retention of data to prevent its deletion while a subsequent production order is prepared.

Speed / Deadlines:

– Standard execution: Provider must execute the preservation without delay.

Co-funded by the European Union

Block 3 Interactive Scenario: The 2026 Reality

The Scenario: It is September 2026. You are a Spanish lawyer defending a client in a cyber-extortion ring. You urgently need subscriber data and IP logs associated with a suspect's Instagram account. Meta is headquartered in Ireland.

The Question: Walk through the exact legal mechanism you will use, and what is the maximum time Meta has to respond?

Strategic Answer:

- You bypass the EIO and the Irish judicial authorities entirely.
- You issue an EPOC (Production Order) directly to Meta's designated EU legal representative.
- Meta is legally bound to produce the data within 10 days (or 96 hours if you certify an emergency).

Co-funded by the European Union

Synthesis Matrix: The EU Digital Evidence Toolkit

Instrument	Transmission Route	Speed/Deadlines	Best Use Case
Budapest Convention (Art 29/30)	Authority-to-Authority	Slow / 60-day preservation	Int'l / Non-EU state cooperation.
European Investigation Order (EIO)	Authority-to-Authority	24h for preservation	Current intra-EU investigations.
Digital Services Act (DSA Art 10)	Authority-to-Provider	Variable	Targeting EU platform intermediaries directly.
E-Evidence 2026 (EPOC / EPOC-PR)	Authority-to-Provider	10 days / 96h	Post-2026 intra-EU direct data production.

Co-funded by the European Union



Belén Arribas Sánchez

The Spanish Charter and the European Declaration on digital rights and principles for the digital decade

Barcelona, 6 November 2026

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

Co-funded by the EU

INDEX

Training of Lawyers on various areas of European Union Law 2

Co-funded by the European Union

#TRAVAR2

1. The Spanish Charter of Digital Rights
2. Rights related to AI
3. Guarantees and effectiveness
4. Practical cases
5. Final considerations

Training of Lawyers on various areas of European Union Law 2

Co-funded by the European Union

#TRAVAR2

CHARTER OF DIGITAL RIGHTS

Introduction

Published in July 2021, it fulfills one of the mandates of the Spain Digital Agenda 2025 and includes 26 digital rights in its six main categories, which public and private organizations, as well as citizens themselves, must respect and guarantee.

It is a pioneering initiative, presented at the United Nations and later "exported" internationally, that seeks to adapt fundamental rights to the challenges posed by the digital environment.

Before the publication of this Charter, laws already existed in Spain that contemplated various digital rights, such as the Organic Law on Data Protection and Guarantee of Digital Rights, the Organic Law on Civil Protection of the Right to Honor, Personal and Family Privacy, and Self-Image, the Organic Law regulating the right to rectification, the law on e-commerce, and the Spanish Constitution itself, among others.

The Digital Rights Charter is not a law, but a declaration; it is neither binding nor obligatory, except for those digital rights that are already contemplated, such as the right to access, to oppose, to erase and to rectify personal data (rights on privacy), the right to honor, etc.

Training of Lawyers on various areas of European Union Law 2

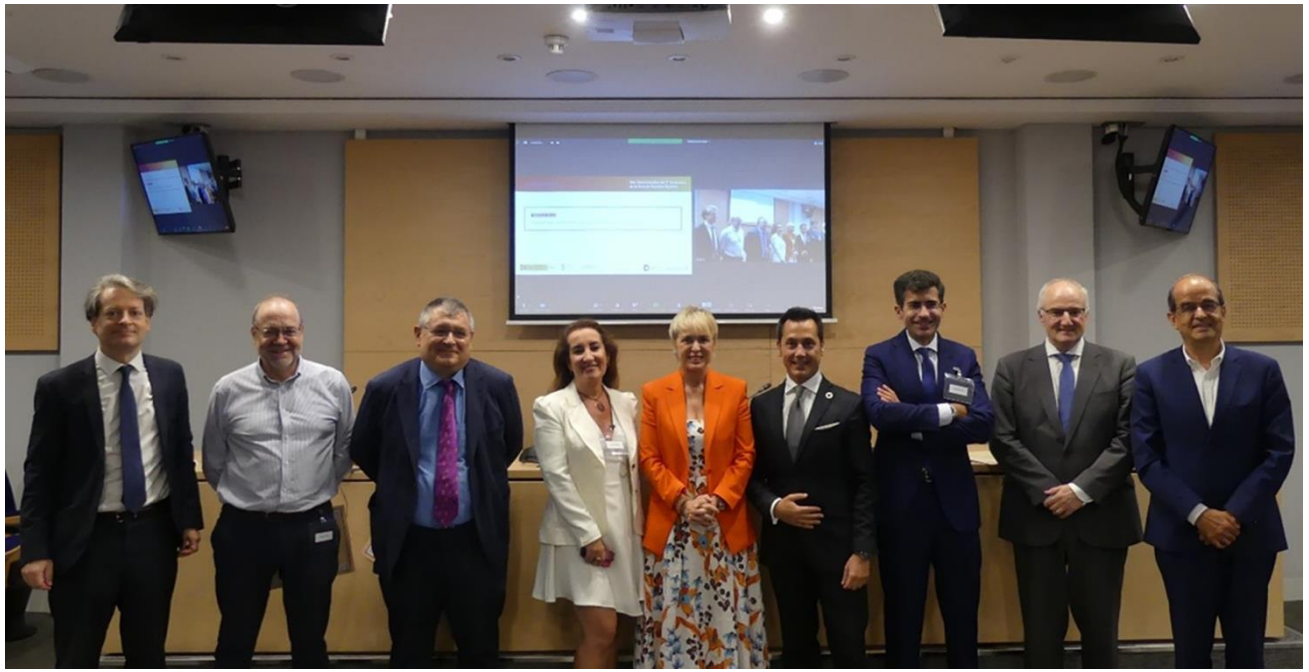
Co-funded by the European Union

#TRAVAR2

CHARTER OF DIGITAL RIGHTS

The Secretary of State for Digitalization and Artificial Intelligence, ENATIC, and the General Council of the Spanish Bar Associations (CGAE) held the commemorative event for the first anniversary of the Charter of Digital Rights in person at the Auditorium of the CGAE.

- July 12, 2022



Training of Lawyers on various areas of European Union Law 2

Co-funded by the European Union

#TRAVAR2

CHARTER OF DIGITAL RIGHTS

The Secretary of State for Digitalization and Artificial Intelligence and ENATIC held the commemorative event for the 2nd anniversary of the Digital Rights Charter in person at the Ministry of Economy Auditorium.

- July 12, 2023



Training of Lawyers on various areas of European Union Law 2

Co-funded by the European Union

#TRAVAR2

CHARTER OF DIGITAL RIGHTS

Objective

The rapid development of new technologies and the Internet means that laws regulating their use and limits are lagging behind, meaning that citizens' fundamental rights can be violated in the digital realm.

In recent years, initiatives related to digital rights have multiplied, a movement that recognizes the importance—and even urgency—of establishing new frameworks to guarantee people's fundamental rights in today's digital environment.

Thus, the Spanish Government's Charter of Rights was published in 2021, and the European Union's (EU) Declaration on Digital Rights and Principles for the Digital Decade was published in 2023.

Similarly, parallel initiatives have emerged, such as the Catalan Charter for Digital Rights and Responsibilities of the Generalitat de Catalunya and similar initiatives of the Barcelona City Council, among others.

Like the Spanish Charter, these are not binding or enforceable laws, but rather proactive regulations that can inspire future public policies and the development of new, future regulations.

Training of Lawyers on various areas of European Union Law 2

Co-funded by the European Union

#TRAVAR2

CHARTER OF DIGITAL RIGHTS

Freedom Rights

These rights recognize digital identity and the right to protect it. They are based on the rights and freedoms recognized in the Universal Declaration of Human Rights, the Spanish Constitution, the European Convention on Human Rights, the EU Charter of Fundamental Rights, and other international treaties and agreements ratified by Spain in the field of digital rights.

I – Rights and freedoms in the digital environment

II – Right to identity in the digital environment

III – Right to data protection

IV – Right to pseudonymity

V – Right of an individual not to be located and profiled

VI – Right to cybersecurity

VII – Right to digital inheritance

CHARTER OF DIGITAL RIGHTS

Training of Lawyers on various areas of European Union Law 2

Co-funded by the European Union

#TRAVAR2

Equality Rights

Related to the defense and respect for equality and non-discrimination, both from the perspective of internet access and the use of new technologies, and from the perspective of behavior and actions carried out within digital environments by organizations and citizens.

This category also includes the digital rights of children/minors and their necessary protection, as well as the existence of digital divides and the need for public administrations to address them.

VIII – Right to equality and non-discrimination in the digital environment

IX – Right of access to the internet

X – Protection of minors in the digital environment

XI – Universal accessibility in the digital environment

XII – Access divides in the digital environment

Training of Lawyers on various areas of European Union Law 2

Co-funded by the European Union

#TRAVAR2

CHARTER OF DIGITAL RIGHTS

Rights to Participation and Shaping of Public Spaces

The Digital Rights Charter recognizes the current and future problems posed by misinformation and fake news, and how the Internet, and especially social media, facilitate the dissemination of such content, which is potentially harmful to society and democratic systems. It sets out rights related to freedom of expression and information, the right to receive truthful information, and the need to educate citizens on responsible and critical use of the media. It also addresses the rights that citizens have in their relationships with public administrations.

XIII – Right to Internet Neutrality

XIV – Freedom of Expression and Freedom of Information

XV – Right to Freely Receive Truthful Information

XVI – Right to Citizen Participation through Digital Media

XVII – Right to Digital Education

XVIII – Digital Rights of Citizens in Their Relationships with Public Administration

CHARTER OF DIGITAL RIGHTS

Training of Lawyers on various areas of European Union Law 2

Co-funded by the European Union

#TRAVAR2

Labour-and business-related rights

These are digital rights applied in the workplace and business environment, which have begun to have a greater impact in recent years, especially due to the use of digital devices for the performance of work tasks, as well as for monitoring workers and remote work.

Therefore, they are digital rights intended to protect workers' rest time and their personal and family privacy, limit and regulate employer control so that their rights and those of workers do not conflict, or in order to have greater control over the development and use of algorithms applied in the workplace.

XIX – Rights at the Workplace

XX – The Company in the Digital Environment

Training of Lawyers on various areas of European Union Law 2

Co-funded by the European Union

#TRAVAR2

CHARTER OF DIGITAL RIGHTS

Digital Rights in Specific Environments

Those related to the areas of health, public interest, and culture are addressed, such as the protection of intellectual property or the freedom of creation and access to culture on the Internet. In addition, new rights regarding the use of artificial intelligence (avoiding discrimination, the need for transparency, ensuring access, use, and reliability) and the use of neurotechnologies (especially regarding data confidentiality and security and control over one's identity) are mentioned.

XXI – Right of access to data for archiving purposes in the public interest, scientific or historical research purposes, statistical purposes, and innovation and development purposes.

XXII – Right to technological development and a sustainable digital environment.

XXIII – Right to health protection in the digital environment.

XXIV – Freedom of creation and the right to access culture in the digital environment.

XXV – Rights regarding AI.

XXVI – Digital rights in the use of neurotechnologies.

Training of Lawyers on various areas of European Union Law 2

Co-funded by the European Union

#TRAVAR2

RIGHTS AS REGARDS ARTIFICIAL INTELLIGENCE

Digital Rights in Specific Environments of the Charter of Digital Rights

XXV Rights Regarding Artificial Intelligence

1. Artificial intelligence must ensure a person-centered approach and its inalienable dignity, pursue the common good, and ensure compliance with the principle of non-maleficence.

2. In the development and lifecycle of artificial intelligence systems:

a) The right to non-discrimination, regardless of its origin, cause, or nature, must be guaranteed in relation to decisions, use of data, and processes based on artificial intelligence.

b) Conditions of transparency, auditability, explainability, traceability, human oversight, and governance must be established. In all cases, the information provided must be accessible and understandable.

c) Accessibility, usability, and reliability must be guaranteed.

3. Individuals have the right to request human oversight and agency and to challenge automated decisions made by artificial intelligence systems that affect their personal and property rights.

RIGHTS AS REGARDS ARTIFICIAL INTELLIGENCE

Training of Lawyers on various areas of European Union Law 2

Co-funded by the European Union

#TRAVAR2

Digital Rights in Specific Environments of the Charter of Digital Rights

XXV Rights as Regards Artificial Intelligence

Ultimately, the Charter recognizes the impact of AI on decision-making and emphasizes the need for ethical and responsible use. From there, it outlines a series of new rights, including:

- Right to non-discrimination: AI systems must avoid biases that result in discrimination.

- Right to transparency: People have the right to understand how AI systems that significantly affect them operate.

- Right to human oversight: Decisions made by AI must be supervised or reviewable by humans.

- Right to privacy and data protection: It emphasizes that AI systems must comply with data protection regulations.

RIGHTS AS REGARDS ARTIFICIAL INTELLIGENCE

Training of Lawyers on various areas of European Union Law 2

Co-funded by the European Union

#TRAVAR2

European Declaration on Digital Rights and Principles (EU) for the Digital Decade

For its part, the EU Declaration outlines a series of elements in the section dedicated to "Freedom of Choice; Interactions with Algorithms and Artificial Intelligence Systems."

<u>In the principles section, it establishes that:</u>

- Artificial intelligence must be a tool at the service of people, and its ultimate goal must be to increase human well-being.

- Every person should be empowered to benefit from the advantages of algorithmic and artificial intelligence systems, especially to make their own informed decisions in the digital environment, as well as to be protected against risks and harm to their health, safety, and fundamental rights.

RIGHTS AS REGARDS ARTIFICIAL INTELLIGENCE

Training of Lawyers on various areas of European Union Law 2

Co-funded by the European Union

#TRAVAR2

European Declaration on Digital Rights and Principles (EU) for the Digital Decade

In the commitments section, it states:

We commit to: a) promote human-centered, trustworthy, and ethical artificial intelligence systems throughout their development, deployment, and use, in line with EU values;

b) ensure an appropriate level of transparency in the use of algorithms and artificial intelligence (…);

c) ensure that algorithmic systems are based on adequate datasets to avoid discrimination and allow for human oversight of all outcomes that affect people's security and fundamental rights;

d) ensure that technologies such as artificial intelligence are not used to preempt people's decisions in areas such as health, education, employment, and privacy;

e) provide safeguards and take appropriate measures (…);

(f) take measures to ensure that artificial intelligence research complies with the highest ethical standards and relevant EU legislation.

RIGHTS AS REGARDS ARTIFICIAL INTELLIGENCE

Training of Lawyers on various areas of European Union Law 2

Co-funded by the European Union

#TRAVAR2

European Declaration on Digital Rights and Principles (EU) for the Digital Decade

Different Approaches

While both frameworks have in common that neither focuses exclusively on AI. While the former focuses on individual rights, the latter focuses on more general digital principles and rights.

Ethical and Social Impact

While the Spanish Charter explicitly recognizes the need to avoid negative impacts of AI on society, such as bias and loss of privacy, and advocates promoting digital literacy to empower people in the use of AI technologies, the EU declaration takes a broader approach and encompasses the ethical and sustainable use of all digital technologies. It also highlights the role of AI in improving quality of life and reducing inequalities, in line with EU values.

CHARTER OF DIGITAL RIGHTS

Training of Lawyers on various areas of European Union Law 2

Co-funded by the European Union

#TRAVAR2

Guarantee and Effectiveness of Digital Rights

Section focused on guaranteeing and promoting the rights recognized therein within the scope of the Public Administrations and the Administration of Justice.

In its section "Guarantee of rights in digital environments," it mentions the creation of self-regulation and self-control mechanisms within digital environments and the use of new technologies, as well as the creation of procedures for the alternative dispute resolution that may arise in the digital environment.

The Government, within the scope of its powers, must adopt the appropriate provisions to guarantee the effectiveness of the digital rights contained therein.

Training of Lawyers on various areas of European Union Law 2

Co-funded by the European Union

#TRAVAR2

PRACTICAL CASES

There are many and varied technological and geopolitical threats that undermine the Charter of Digital Rights:

Disinformation and Digital Manipulation

Disinformation and manipulation campaigns on social media, driven by state and private actors, can affect democratic processes such as elections and referendums.

Case study: In the 2016 US elections and the UK Brexit referendum, there was evidence of foreign interference through fake news and bots. In Spain, disinformation campaigns have also affected electoral processes and political crises.

The Charter of Digital Rights establishes the right to receive truthful and pluralistic information, as well as mechanisms to strengthen digital literacy and verify information.

Training of Lawyers on various areas of European Union Law 2

Co-funded by the European Union

#TRAVAR2

PRACTICAL CASES

Cybersecurity and Attacks on Critical Infrastructure

Cyberattacks against institutions and companies have increased in recent years.

Cybercrime groups and hostile states have used ransomware to hijack information or paralyze public services.

Case study: In 2021, during the pandemic, the SEPE (State Public Employment Service) suffered a cyberattack that rendered its digital platform inoperative for days, affecting thousands of citizens during these difficult times.

The Charter recognizes the right to digital security, urging the strengthening of cybersecurity measures and the protection of critical infrastructure.

Training of Lawyers on various areas of European Union Law 2

Co-funded by the European Union

#TRAVAR2

PRACTICAL CASES

Artificial Intelligence and Algorithmic Biases

The increasing use of AI in automated decisions poses risks such as potential discrimination and a lack of transparency in decision-making.

Case study: In 2020, it was found that Twitter's algorithm was cropping images favoring white faces over black faces, thereby revealing biases in the algorithm's development.

The Charter promotes the right to non-discrimination and transparency in the use of AI, demanding explainability in automated decisions and the possibility of appeal.

Training of Lawyers on various areas of European Union Law 2

Co-funded by the European Union

#TRAVAR2

PRACTICAL CASES

Data Protection and Digital Sovereignty

Reliance on foreign platforms and massive data transfers outside the EU pose risks to privacy, information control, and regulatory compliance.

Case study: In 2020, the Court of Justice of the EU struck down the Privacy Shield, a bilateral agreement that allowed data transfers between the US and the EU, finding that it did not sufficiently protect the rights of European citizens.

The Charter recognizes, among other rights, the right to informational self-determination, strengthening control over personal data and promoting sovereign digital alternatives in Europe.

Training of Lawyers on various areas of European Union Law 2

Co-funded by the European Union

#TRAVAR2

PRACTICAL CASES

User Protection on Digital Platforms

Some of the major technology platforms have been criticized and reported for abusive practices, lack of transparency in their algorithms, and violations of digital rights.

Case study: In 2021, WhatsApp unilaterally changed its terms of use, forcing users to share more data with Facebook (now Meta). This triggered a wave of migration to apps like Signal and Telegram.

The Charter protects citizens through the right to digital privacy and transparency on platforms, establishing principles for better regulation of these practices.

Training of Lawyers on various areas of European Union Law 2

Co-funded by the European Union

#TRAVAR2

PRACTICAL CASES

Digital Labor Rights and Digital Disconnection

Teleworking and automation are rapidly transforming the labor market, but they are also creating new challenges, such as potentially excessive employee monitoring or the blurring of working/personal hours.

Case study: In 2021, Spain passed the Telework Law, recognizing the right to digital disconnection to prevent workers from having to be available outside of working hours.

The Charter reinforces this right and establishes principles to ensure fair digital working conditions.

Training of Lawyers on various areas of European Union Law 2

Co-funded by the European Union

#TRAVAR2

PRACTICAL CASES

Education and Digital Literacy

In a world where technology is increasingly crucial, digital literacy has become a key right for social and labor inclusion.

Case study: During the pandemic, thousands of students in Spain were unable to access digital education due to the digital divide and a lack of devices.

The Charter establishes the right to digital education and promotes investment in accessible digital infrastructure for all.

Training of Lawyers on various areas of European Union Law 2

Co-funded by the European Union

#TRAVAR2

FINAL REMARKS

The Spanish Charter of Digital Rights is a key instrument for addressing the technological and geopolitical challenges of the 21st century.

It is not a binding legal provision, but its influence is crucial for the development of future public policies and legislation on data protection, artificial intelligence, cybersecurity, and digital rights.

In a context of growing international polarization, including digital polarization, its implementation will allow Spain and the EU to strengthen their technological sovereignty, protect their citizens, and guarantee a safer, fairer, and more inclusive digital environment. In the current context of growing technological and geopolitical threats, such as disinformation, cybersecurity, artificial intelligence (AI), and data control by foreign actors, the Charter of Digital Rights takes on even greater relevance.

Its effective implementation is key to protecting digital sovereignty, citizens' rights, and the country's competitiveness in the digital age.



Cristina Casellas Vazquez

Artificial Intelligence in the context of criminal proceedings

Barcelona, 6 November 2026

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

Co-funded by the EU

01. EMERGING THREATS

The Deepfake Challenge: The Almendralejo Case



The Almendralejo Case

Mass generation of explicit synthetic imagery of minors using AI tools. High-profile case highlighting digital gender-based violence.

"Liar's Dividend" Effect

Perverse effect where the existence of deepfakes allows defendants to falsely claim that authentic audiovisual evidence is AI-manipulated.

EU AI Act Response

Strict prohibitions and mandatory transparency tagging for synthetic content generated without consent under the EU AI Act (Art. 50).

Everyday AI vs. Criminal Justice AI

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

Daily Life AI Adoption

- **Rapid & frictionless adoption:** Seamless integration into daily workflows and personal tasks.
- **High error tolerance:** Algorithmic hallucinations carry low personal or legal liability.
- **Commercial usage:** Unaudited models deployed without formal chain-of-custody requirements.

Criminal Justice AI

- **Extreme procedural caution:** Strictly bound by the presumption of innocence.
- **Fundamental rights focus:** Strict scrutiny over data integrity, privacy, and defense rights.
- **Explainability requirement:** Zero tolerance for "black box" decisions in judicial rulings.

Three Levels of AI in Legal Practice

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

Level 1

Generative AI

Synthesis of new content (text, audio, media).

Procedural risk: Forgery risks (deepfakes) and unsupervised draft generation.

Level 2

Contextual AI

Document discovery and data structuring.

Current judicial use: Redaction, anonymization, transcriptions, and file management.

Level 3

Agentic AI

Autonomous decision-execution systems.

Strict prohibition: Red line against "robot judges". Human oversight remains mandatory.

AI Implementation in European Criminal Courts

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

Automated Anonymization

Systems like **Anoppi** (Finland) and tools in Portugal or Spain automate personal data protection across published court decisions.

Forensic Data Mining

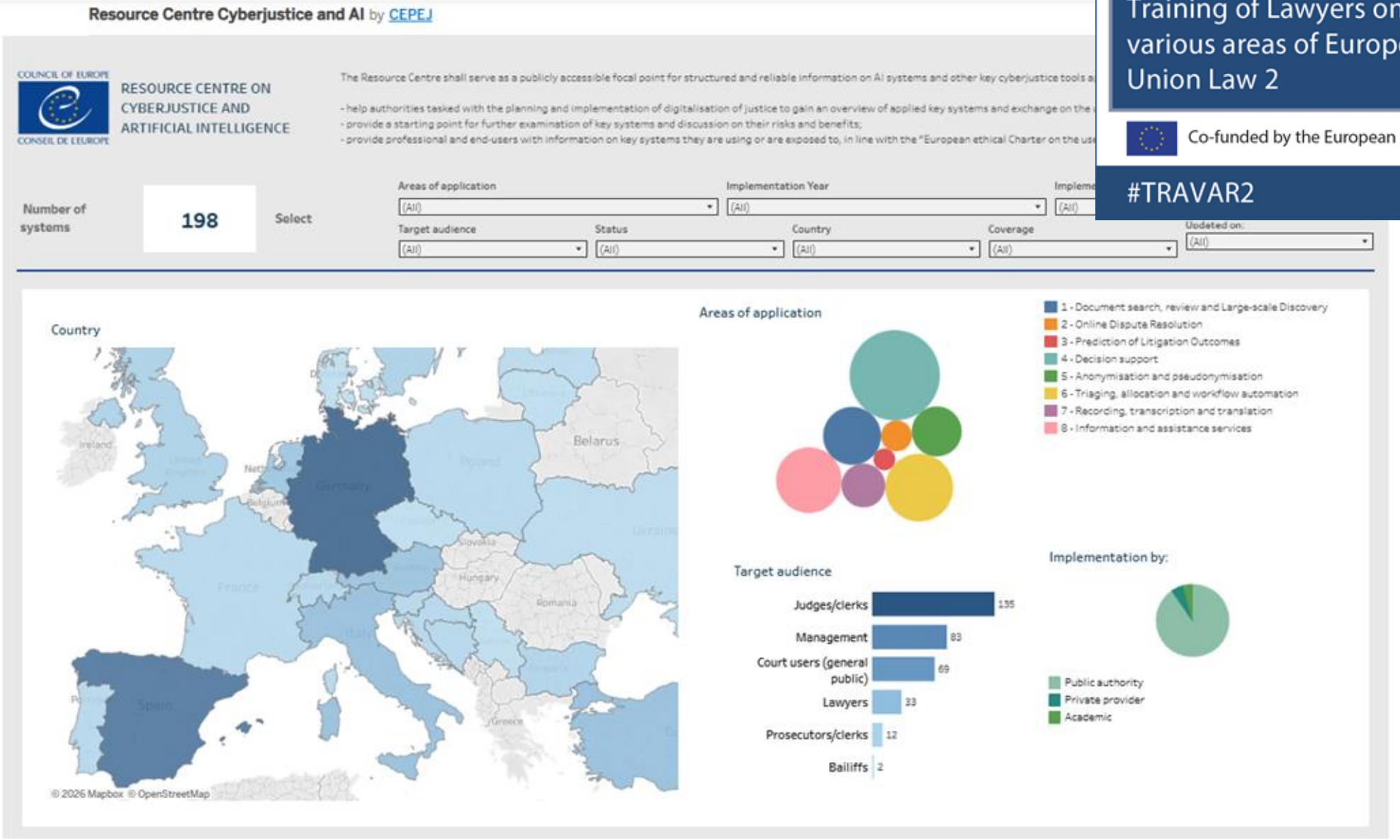
Platforms like **Hansken** (Netherlands) enable forensic analysis of massive digital data collections for criminal investigations.

Post-Delictum Risk Assessment

Systems like **VioGén** or **RisCanvi** (Spain) assess recidivism risks to assist police protection and prison management decisions.

Biometric Recognition

Identification systems like **ABIS** (Spain) or **SARI** (Italy) used in criminal investigations under strict judicial supervision.



https://public.tableau.com/app/profile/cepej/viz/ResourceCentreCyberjusticeandAI/AITOOLSINITIATIVESREPORT?publish=yes

05. INVESTIGATIVE APPLICATIONS

AI Uses in Criminal Investigation



Biometric Recognition

Automated identification using facial features, voice patterns, and fingerprint matching to locate suspects across large datasets (ABIS).

Computer Vision

Automated processing of CCTV feeds and drone footage to track suspect movements and detect suspicious behavioral patterns.

Automated Filtering

Classifiers using machine learning models to detect illegal material, such as child sexual abuse material or illicit traffic data.

06. PROCEDURAL RISKS

Deepfake Threats in Judicial Proceedings



Evidence Falsification

Total or partial synthesis of video, audio, or images capable of misleading judges and jury members regarding factual occurrences.

The "Liar's Dividend"

Erosion of trust in legitimate proof: authentic digital evidence is increasingly challenged by claims of algorithmic manipulation.

Detection Challenges

Technical complexity requiring specialized forensics (e.g., GPTZero, Deepware, Resemble Detect) to verify source authenticity.

Penal Consequences

Submitting deepfakes to court constitutes procedural fraud, identity theft, and obstruction of justice under criminal codes.

06. PROCEDURAL RISKS

Deepfake Threats in Judicial Proceedings



Audio&voice detection

Resemble Detect & VerificAudio: Advanced acoustic spectrum analyzers detecting AI-generated voice clones, pitch anomalies, and synthetic noise floor mismatches.

Visual Deepfake Detection

Deepware, Illuminarty & VerifAI: Machine learning algorithms inspecting frame-by-frame facial pixel boundaries, unnatural blinking, and lighting inconsistency.

AI Watermarking

C2PA & Cryptographic Tags: Industry standards (EU AI Act Art. 50) embedding invisible metadata and mathematical signatures at creation to trace content authenticity.

Forensic Evaluation

Digital forensics experts can provide their specialized knowledge to determine whether evidence has been fully or partially manipulated by AI.

07. EVIDENCE GENERATION

Digital Enhancement vs. AI Simulations



Digitally Enhanced Evidence

Algorithms used to clarify original recordings (denoising audio, sharpening blurry frames, adjusting exposure).

Key rule: Must preserve the underlying raw data without generating unverified synthetic pixels.

AI Simulations & Reconstructions

Generative models recreating 3D crime scenes, bullet trajectories, or skull-photo superimposition (craniofacial reconstruction).

Key rule: Treated as expert scientific testimony, not direct material evidence.

08. LEGAL FRAMEWORK

Evidentiary Value of AI & Digital Proof

Training of Lawyers on various areas of European Union Law 2

Co-funded by the European Union

#TRAVAR2

01 **Lawfulness of Acquisition (Art. 11.1 LOPJ)**

Strict exclusionary rule prohibiting any digital evidence obtained via fundamental rights violations (privacy, communications secrecy).

02 **Technical Reliability: Authenticity & Integrity**

Mandatory use of cryptographic HASH verification and rigorous chain-of-custody protocols to disprove manipulation or deepfakes.

03 **Judicial Evaluation & Forensic Expertise**

AI outputs possess no pre-assigned legal weight; judges assess them under critical reasoning supported by expert computer forensics.



Ruth Sala Ordóñez

E-evidence procedures

Barcelona, 6 November 2026

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

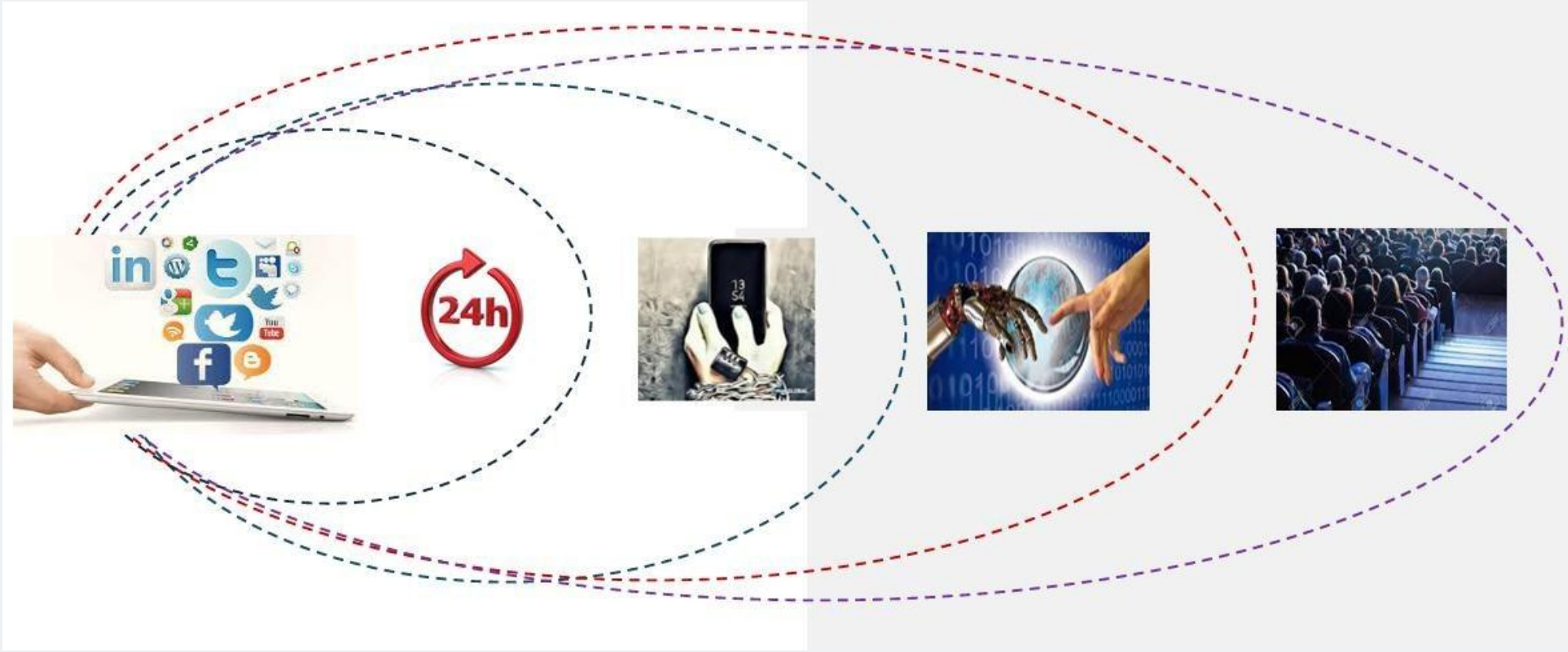
«Given the exclusively educational and eminently illustrative nature and purpose of the explanations delivered within the training programme Training of Lawyers on various areas of European Union Law 2 (TRAVAR 2), session E-Evidence Procedures, the speaker relies on Article 32 of the Intellectual Property Act in force regarding the partial use of third-party works such as images, graphics or other material and content in various slides.»

The digital context

Training of Lawyers on various areas of European Union Law 2

Co-funded by the European Union

#TRAVAR2



Technical and legal implications

Training of Lawyers on various areas of European Union Law 2

Co-funded by the European Union

#TRAVAR2

01 The speed at which evidence is created

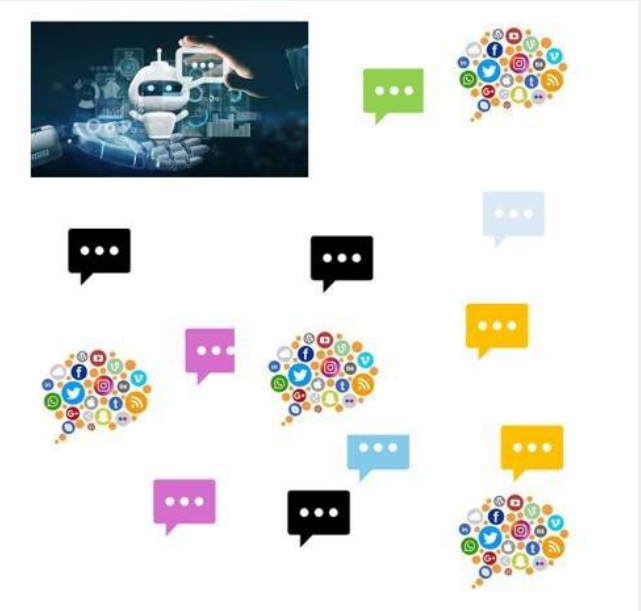
02 The extent of digital evidence

03 The need to identify **who is behind a bot**

04 The need to «listen to the network» 24/7

05 Tools to capture digital evidence with **integrity, authenticity and reliability**

06 Identifying the witnesses



Training of Lawyers on various areas of European Union Law 2

Co-funded by the European Union

#TRAVAR2

Four minors investigated for manipulating and sharing AI-generated sexual images at a Barcelona secondary school



Cataluña

ELECCIONES CATALUÑA · GENERALITAT · BARCELONA · TARRAGONA · GIRONA · LLEIDA · QUADERN

SUCESOS >

Investigados penalmente cuatro menores por manipular y compartir imágenes de contenido sexual producidas con IA en un instituto de Barcelona

Los Mossos d'Esquadra localizan una quincena de fotografías que los jóvenes difundían a través de un grupo de Telegram



SERGI LLANAS

Barcelona - 27 FEB 2025 - 09:42 CET

0

Los Mossos d'Esquadra investigan penalmente a un grupo de cuatro menores por haber realizado presuntamente un montaje de imágenes de caras de compañeras de clase en cuerpos desnudos haciendo uso de inteligencia artificial. Los hechos han ocurrido en un instituto del barrio de La Bordeta, en el distrito de Sants-Montjuïc (Barcelona?.

Source: El País · 27/02/2025

REAL CASE · 02

Five young people investigated for creating and spreading AI-generated nude images of 20 minors



Investigados cinco jóvenes por crear y difundir imágenes de 20 menores desnudas por inteligencia artificial

Sevilla

05/08/24

Saltar carrusel

GUARDIA CIVIL
Mº INTERIOR

Las fotografías generaban una gran dificultad para distinguir entre aquellas que eran auténticas y las que habían sido modificadas

La Guardia Civil ha investigado a cinco jóvenes por los delitos de pornografía infantil y revelación de secretos al manipular y difundir imágenes pornográficas de chicas menores de edad en la provincia de Sevilla.

La investigación comenzó tras la denuncia que interpusieron los padres de una de las víctimas por la difusión de imágenes manipuladas de su hija.

THE EVIDENTIARY KEY

The photographs made it very difficult to tell which were authentic and which had been altered.

Source: Spanish Ministry of the Interior · Guardia Civil

€95 million stolen from an Italian bank using a voice deepfake

Training of Lawyers on various areas of European Union Law 2

Co-funded by the European Union

#TRAVAR2

CIBERSEGURIDAD

Roban 95 millones de euros de un banco italiano mediante un deepfake de voz

Los cibermalos se sirvieron de IA para emular la voz de altos ejecutivos y un abogado. Parte del dinero se ha recuperado, pero aún siguen sin aparecer 36 millones de euros.

- EE.UU. ilegaliza la clonación de voz generada por IA en llamadas automáticas
- El phishing de clonación es capaz de engañar a los más cautos



Source: Escudo Digital · Cybersecurity

Training of Lawyers on various areas of European Union Law 2

Co-funded by the European Union

#TRAVAR2

BLOCK 1

Digital evidence in judicial proceedings



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

Judicial proceedings in the digital context

Questioning witnesses	Analysing the scenario	Studying the evidence	Assessing the expert report
↓	↓	↓	↓
Who are the witnesses?	**What is the scenario?**	**What type of evidence is there?** WhatsApp · Social media · email · mobile devices · cameras… etc.	**What does the expert report assess?** The aggressor · The victim · Reputational damage

Training of Lawyers on various areas of European Union Law 2

Co-funded by the European Union

#TRAVAR2

Digital evidence: characteristics

01 Volume

02 Alterable

03 Intangible

04 Volatile

05 Can be destroyed

06 Leaves a trace

What, how, when and how much

Training of Lawyers on various areas of European Union Law 2

Co-funded by the European Union

#TRAVAR2

WHAT

Concerns what must accompany the capture of the evidence. What type of digital evidence: social media conversations, images, video recordings, etc.

HOW

Concerns how the digital evidence is captured: through a **certification service provider** or with **technical IT professionals**.

WHEN

Concerns the best moment to capture the evidence and submit it to the proceedings: **at the outset**, when filing the complaint, or **during the investigation**.

HOW MUCH

Concerns the appropriate amount of evidence to submit to the proceedings, without it being excessive or unnecessary.

Submission to the proceedings

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

01

Notary

Notarial deed certifying the digital content.

02

Law enforcement

Police investigation and submission to the case.

03

Forensic IT expert

Technical analysis and expert report.

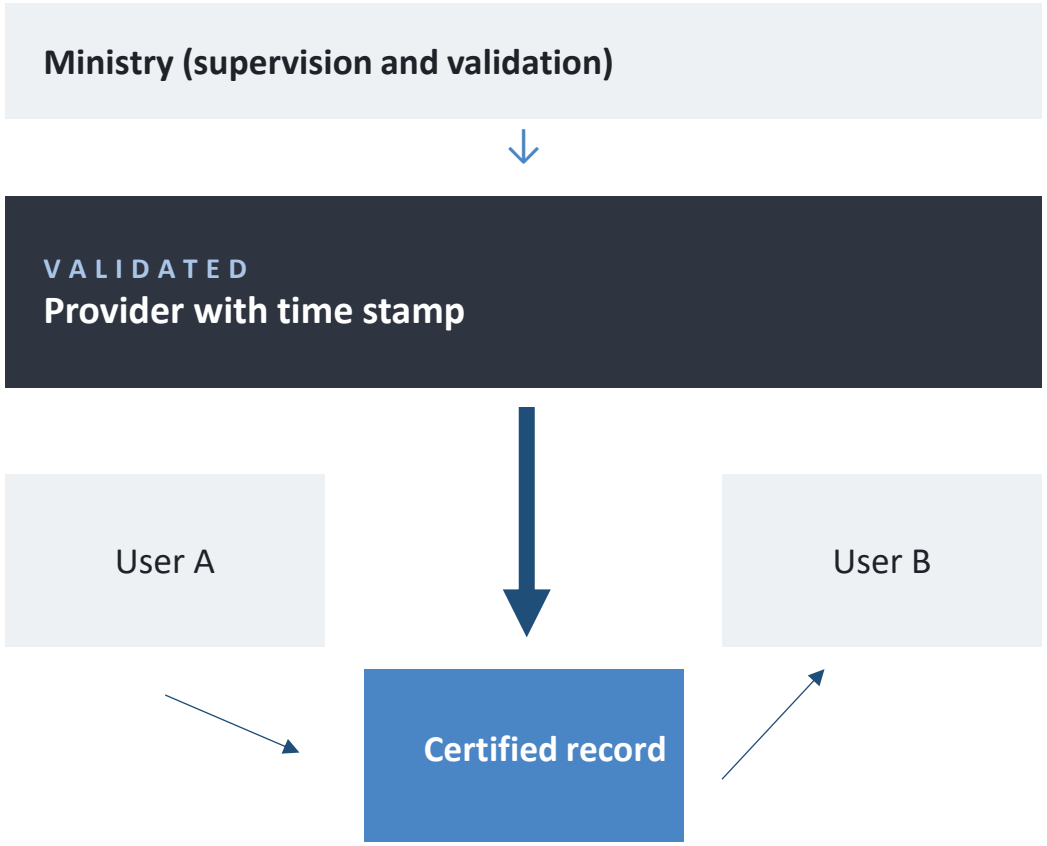
04

Certification service provider

Capture with time stamp and certified record.

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

Certification service providers



WHAT CAN BE CERTIFIED

Video	Email	Intellectual property
SMS	Digital invoice	Photographs

EXAMPLES OF PROVIDERS

eGarante	ColorIURIS	Signaturit
Eevid	Evicertia	Lleida.net

Legislative background

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

2003

Law 59/2003 of 19 December on electronic signatures

Spanish Official Gazette (BOE) no. 304, 20/12/2003. In force from 20/03/2004. Repealed.

2014

Regulation (EU) 910/2014, eIDAS

Electronic identification and trust services for electronic transactions in the internal market.

2020

Law 6/2020 of 11 November

Regulating certain aspects of electronic trust services. Repeals Law 59/2003 with effect from 13/11/2020.

2024

Regulation (EU) 2024/1183

Amends eIDAS and establishes the European digital identity framework.

Electronic trust service providers

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

Trust service provider

A natural or legal person who provides one or more trust services, either as a qualified or a non-qualified provider.

Qualified provider

Provides one or more qualified trust services and has been granted qualified status by the supervisory body.



OFFICIAL SOURCE

Qualified and non-qualified providers, and the trusted list (TSL), on the Ministry's e-office.
digital.sede.gob.es

Credibility levels when submitting an email

Training of Lawyers on various areas of European Union Law 2

Co-funded by the European Union

#TRAVAR2

1 **Expert report**

2 **Email from a certification service provider**

3 **Email with technical headers**

4 **Printed email**

Stronger evidentiary weight

Weaker evidentiary weight

HEADER EXAMPLE

```
Delivered-To: user@gmail.com
Received: by 10.115.22.20 with SMTP id …
   Tue, 2 Oct 2007 20:38:18 -0700 (PDT)
Return-Path: <sender@cox.net>
Received-SPF: pass (google.com: domain of …)
Received: from sender ([72.204.154.191])
From: "Sender" <sender@cox.net>
```

Credibility of social media conversations

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

1	**Expert + notarial deed**	E.g. access to the victim's profile by another user through digital identity theft.
2	**Notarial deed**	E.g. online harassment, attacks on honour, privacy and personal image.
3	**Certification service provider**	Certified capture with time stamp.
4	**Paper printout**	Backed by an internal witness.

Training of Lawyers on various areas of European Union Law 2

Co-funded by the European Union

#TRAVAR2

BLOCK 2

The EU e-Evidence package



From judicial cooperation to direct orders

Training of Lawyers on various areas of European Union Law 2

Co-funded by the European Union

#TRAVAR2

UNTIL NOW
Authority to authority

Mutual legal assistance and the European Investigation Order: the request goes to the authorities of the State where the provider is established. Months, sometimes years.

›

SINCE 18 AUGUST 2026
Direct order to the provider

The issuing authority sends a European Production or Preservation Order straight to the provider's designated establishment or legal representative in another Member State.

›

SAFEGUARDS
Notification and control

For traffic and content data, the enforcing State is notified and may raise grounds for refusal. Defence rights and remedies remain in the issuing State.

The new orders do not replace the EIO or mutual legal assistance: they are an additional, non-exclusive instrument.

Legislative timeline

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

2023

Regulation (EU) 2023/1543 and Directive (EU) 2023/1544

Adopted on 12 July 2023. OJ L 191, 28/07/2023. In force from 17/08/2023.

2025

Commission Implementing Regulation (July 2025)

Technical specifications of the decentralised IT system (e-CODEX) for exchanging orders and data.

Feb 2026

Directive transposition deadline: 18/02/2026

Few Member States on time. On 27/03/2026 the Commission sent letters of formal notice to 22 Member States.

Aug 2026

Regulation applies from 18/08/2026

Directly applicable in every Member State except Denmark.

Two orders, tight deadlines

Training of Lawyers on various areas of European Union Law 2

Co-funded by the European Union

#TRAVAR2

01

European Production Order (EPOC)

Hand over the data within 10 days of receipt.

02

Emergency cases

8 hours: imminent threat to life, physical integrity or critical infrastructure.

03

European Preservation Order (EPOC-PR)

Preserve the data for 60 days, extendable by 30 days.

04

Only stored data

Covers data already stored when the order is received. No general retention obligation.

Categories of data and issuing conditions

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

SUBSCRIBER DATA

Name, address, contact details, account and payment data. Any criminal offence. Judge, court, investigating judge or prosecutor.

IDENTIFICATION DATA

IP addresses and related data requested solely to identify the user. Same regime as subscriber data.

TRAFFIC DATA

Source, destination, time, duration, location. Offences punishable by at least 3 years or listed offences. Judge or court only.

CONTENT DATA

Messages, emails, images, stored files. Same threshold as traffic data. Judge or court only (or validated by them).

Notification and grounds for refusal

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

1	**Notification to the enforcing State**	For traffic and content data, unless the offence and the person are located in the issuing State.
2	**10 days to react (96 hours in emergencies)**	The enforcing authority may refuse; the data are not handed over until that period expires.
3	**Grounds for refusal (Art. 12)**	Immunities, press freedom, ne bis in idem, manifest breach of fundamental rights, double criminality.
4	**Provider's objections**	Conflicting obligations under third-country law (Art. 17), impossibility or manifest errors.

Service providers and Directive (EU) 2023/1544

Training of Lawyers on various areas of European Union Law 2

Co-funded by the European Union

#TRAVAR2

[01]

Who is covered

Electronic communications, domain name and IP numbering services, and information society services enabling communication or storage, offered in the EU wherever the provider is established.

[02]

Designated establishment or legal representative

In a Member State bound by the Regulation, with powers and resources to receive and execute orders. Joint liability with the provider.

[03]

Decentralised IT system

Secure exchange of orders and data through e-CODEX. If the system is unavailable, the most appropriate alternative means (Art. 19).

[04]

Penalties

Up to 2% of the provider's total worldwide annual turnover of the preceding financial year.

And in Spain?

Training of Lawyers on various areas of European Union Law 2

Co-funded by the European Union

#TRAVAR2

Where we are…

- The Regulation is directly applicable from 18/08/2026
- Draft bill approved at first reading by the Council of Ministers on 14/04/2026
- Urgent processing authorised
- Directive transposition deadline already missed

The draft bill…

- Amends Law 23/2014 on mutual recognition in criminal matters
- Regulates who issues EPOC and EPOC-PR in Spain
- Designates the CNMC as central authority
- Sets the sanctions regime for providers

The defence must check…

- Issuing authority and offence threshold
- Notification and grounds for refusal
- Right to information (Art. 13) and effective remedies (Art. 18)
- Chain of custody and integrity of the data received

Faster access to data must not come at the expense of the rights of the defence.

BLOCK 3

Artificial intelligence and evidence



Training of Lawyers on various areas of European Union Law 2

Co-funded by the European Union

#TRAVAR2

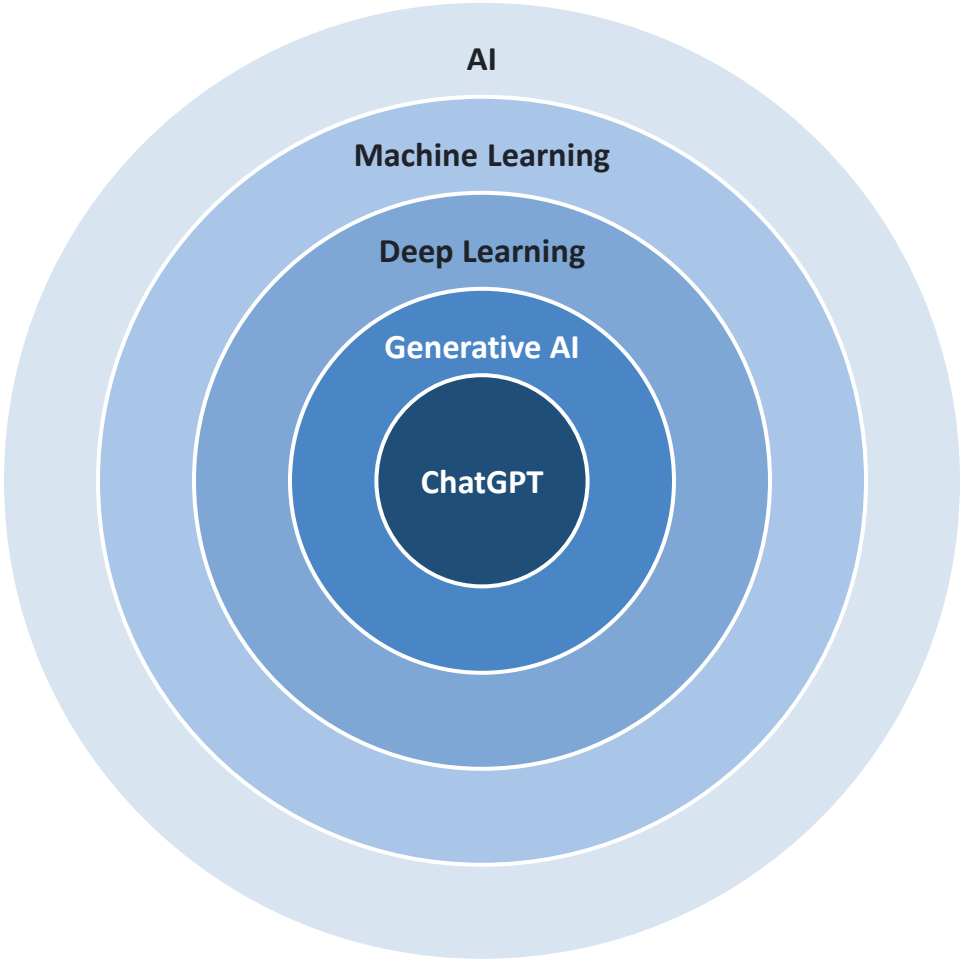
Uses of AI

Machine Learning (ML)
Self-learning from data and pattern analysis. E.g. online shopping, targeted advertising.

Deep Learning (DL)
Self-learning using a combination of neural networks. E.g. driver assistance.

Generative AI (GenAI)
Generation of original content based on pre-existing data.

Risk: bias



Threats to AI

Training of Lawyers on various areas of European Union Law 2

Co-funded by the European Union

#TRAVAR2

[01]
Infection of the underlying system
If the AI runs on a vulnerable or compromised operating system, malware can affect its operation and the integrity of the data it processes.

[02]
Manipulation of input data
Introducing manipulated text or images can lead to wrong conclusions.

[03]
Modification of the AI model
Malware with access to the server where the model is stored can alter it so that it produces incorrect and malicious results.

[04]
Data poisoning attacks
Attackers can introduce datasets intended to manipulate the model.

The main technical difficulties

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

[01]
No classic traces
Created from scratch: no lighting inconsistencies or pixel alterations.

[02]
Multimodal evidence
Photographs, conversations, cloned voices, videos and falsely attributed documents.

[03]
Partial contamination
A few seconds of synthetic audio inside a real recording can go unnoticed.

[04]
No originals
Forwarding, screenshots and compression strip metadata and technical traces.

[05]
Outdated detectors
Trained on specific models, they lose effectiveness against new generators.

[06]
Fragile metadata
A simple format conversion can remove provenance labels.

Consequence: the expert cannot rely solely on an application's percentage score. They must explain what was examined, the indicators found, the limitations of the method and the compatible hypotheses.

Three questions, three levels of certainty

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

1	**Was it generated with AI?**	In certain circumstances, yes, with varying levels of confidence.
2	**With which model or platform?**	Sometimes: if there are logs, verifiable metadata, provenance marks or specific artefacts. With statistical patterns alone, attribution is much weaker.
3	**Who created it?**	The most complex question: identifying the model does not reveal who entered the instructions.

EVEN IF THE FILE IS ON A COMPUTER, WE MUST DISTINGUISH BETWEEN…

- **The device owner**
- **The account user**
- **Who ran the program**
- **Who decided to generate and use the content**

Five plausible cases in the courtroom

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

CASE 01
The recording that sounds like a confession

An audio in which a third party appears to admit a crime. The voice could be cloned.

KEY

A similar voice does not prove that person said the words.

CASE 02
The WhatsApp message that never existed

A screenshot with threats apparently sent by someone.

KEY

Look for the messages on the devices and in the backups.

CASE 03
The real video with a fake sentence

A recorded meeting includes a few seconds of synthetic audio.

KEY

Isolate the alteration without discrediting the rest of the recording.

CASE 04
The document with a perfect chain of custody

It appears on a seized computer, with its hash documented.

KEY

Forensic integrity does not prove who wrote it.

CASE 05
Real evidence accused of being a deepfake

A party denies an authentic recording, claiming it is AI.

KEY

Provenance, originals, continuity and external corroboration.

And what if the expert is the one using AI?

Training of Lawyers on various areas of European Union Law 2

Co-funded by the European Union

#TRAVAR2

It can help to…

- Organise large volumes of documents
- Link communications
- Propose timelines
- Detect contradictions

But it can…

- Compromise data and confidentiality
- Invent facts or confuse identities
- Misinterpret timestamps
- Establish causal links without evidentiary support

That is why we must…

- Preserve the original sources
- Independently verify the relevant results
- Document the role of AI in the report
- Not upload confidential information to external services without assessing their safeguards

«AI can help locate evidence, but it must not, in itself, become the proof of what it claims to have found.»

Integrity is no longer enough

Training of Lawyers on various areas of European Union Law 2

Co-funded by the European Union

#TRAVAR2

YESTERDAY
Integrity and chain of custody

Experts certified that the digital evidence had not been altered. That obligation still stands.

›

TODAY
Evidence that never existed

Photographs of events that never happened, cloned voices, fabricated documents and conversations. We will not always know whether it is AI, and knowing does not identify the author.

›

TOMORROW
A combined methodology

Traditional digital forensics + new analysis methods + provenance verification + rigorous correlation of independent sources.

The expert and legal professions will need to combine traditional digital forensics with new verification tools.

The role of AESIA

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

Ensure compliance with the AI Act

Particular attention to high-risk tools. E.g. tools for generating or analysing digital evidence.

Certify AI tools

It could validate the tools used in judicial contexts so that they are safe, transparent and free of unacceptable risks.

Supervise and register

Supervision of compliance with the AI Act and management of a register of certified AI.

Example

An AI-powered video surveillance system will need a prior assessment guaranteeing the traceability and authenticity of its recordings.

Goal: build trust in the legal community.

The debate on regulatory interoperability

Training of Lawyers on various areas of European Union Law 2

Co-funded by the European Union

#TRAVAR2

Principle of mutual recognition within the EU
AI tools certified in one EU country can be recognised and accepted in other EU countries.

But with national discretion
Each State may interpret and apply the Regulation to its internal procedures, which may create discrepancies.

Example: an AI tool validated in France is submitted as evidence in proceedings in Spain. The judge could question whether that certification meets local standards.



Debate

Training of Lawyers on various areas of European Union Law 2

Co-funded by the European Union

#TRAVAR2

? Should there be a single EU register of AI tools, managed centrally, to avoid conflicts between countries?

? Should AESIA work with other national agencies to coordinate the mutual recognition of certified tools?

? What happens if AESIA imposes stricter criteria than other countries?

? How does the lack of harmonisation affect the validity of evidence?

Legal uncertainty

Training of Lawyers on various areas of European Union Law 2

Co-funded by the European Union

#TRAVAR2

01 Parties confronting each other with doubts over which certifications are accepted in each jurisdiction

02 Delays in judicial proceedings

03 Higher cost of tools to comply with multiple regulations



Conclusions

Training of Lawyers on various areas of European Union Law 2

Co-funded by the European Union

#TRAVAR2

01 AI redefines everything we knew about the authenticity of evidence.

02 Regulations such as the AI Act will be the benchmark for the use of AI in the legal field.

03 Regulatory interoperability is a key challenge in the European Union.

04 Lawyers must develop technical skills.

05 AI can be our ally, but it may entail ethical and legal risks.

06 The law should guarantee the balance between innovation and justice.

Organic Law 2/1986 of 13 March on the State Security Forces and Corps

Microsoft launches Windows 1.0, sold for $100.

Organic Law 2/1986 on the State Security Forces and Corps is passed.

The first virus to affect IBM PCs: «Brain», a boot-sector virus.

In early 1993, the web contained 130 pages.



1985 — **1986** — 1986 — 1993

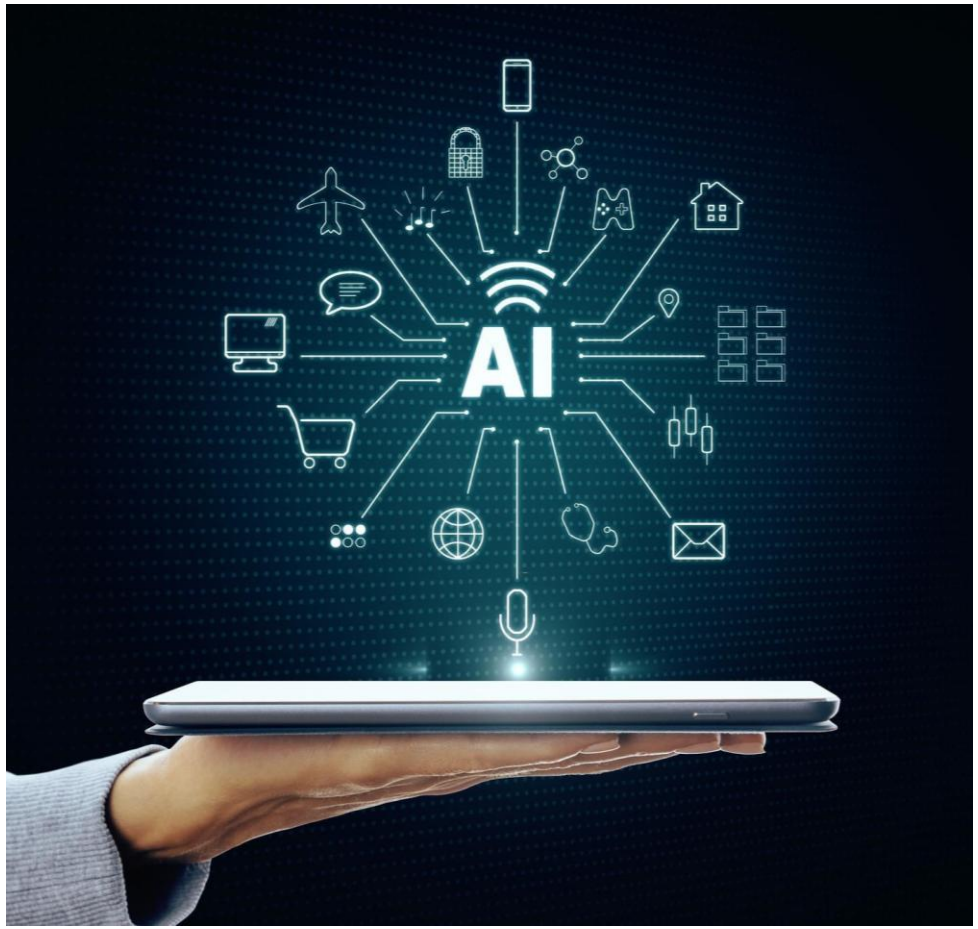
Risks

Training of Lawyers on various areas of European Union Law 2

Co-funded by the European Union

#TRAVAR2

- Bias
- Black boxes
- Lack of algorithmic transparency
- **Impact on fundamental rights**
- **Impact on procedural safeguards**



Unfinished business

Training of Lawyers on various areas of European Union Law 2

Co-funded by the European Union

#TRAVAR2

01
Validity of AI tools

02
Validity of the tools used by the forensic expert when investigating incidents caused by AI

03
European consistency in the criteria for the validity of tools

04
Transparency… or not, of the tools used by public administrations

Bibliography

Training of Lawyers on various areas of European Union Law 2

Co-funded by the European Union

#TRAVAR2

Adolescencia, redes sociales y violencia de género digital

Celia Prados García (coord.) · Tirant lo Blanch · Tirant Humanidades, 2023 · Plural collection · ISBN 9788419376923

Internet para periodistas. Kit de supervivencia para la era digital

Silvia Cobo · Editorial UOC

Keywords for online searches

Open Source INTelligence (OSINT). Investigar personas e identidades en Internet

Carlos Seisdedos · Vicente Aguilera · 0xWord, 2nd ed.

Techniques for searching online

Titles are given in their original Spanish.

Recommended bibliography

Training of Lawyers on various areas of European Union Law 2

Co-funded by the European Union

#TRAVAR2

1. ABEL LLUCH, Xavier. 2011. *Nuevas Tecnologías y Acceso al proceso.*

2. ÁLVAREZ BUJÁN, María Victoria. 2015. *Reflexiones críticas en torno a la prueba en el proceso penal español.*

3. ARMENTE DEU, Teresa. 2011. *La prueba ilícita.*

4. CARRETERO GONZÁLEZ, Cristina. 2011. *La policía judicial y las pruebas en los procesos penales.*

5. CHAMORRO BERNAL, Francisco. 2011. *Obligaciones de los Jueces y Tribunales en garantía del derecho constitucional a la prueba.*

6. GIMENO SENDRA, Vicente. 2020. *La prueba preconstituida.*

7. GONZÁLEZ MONJE, Alicia. 2013. *Nuevas Tecnologías e Investigación Penal.*

8. MENACHO DE SOLÀ-MORALES, Antonio. 2011. *La duda del abogado ante la prueba.*

9. ORMAZÁBAL SÁNCHEZ, Guillermo. 2006. *Informática y Prueba Judicial. Especial referencia a la firma electrónica.*

10. OLLER SALA, Maria Dolors. 2011. *El derecho a la utilización de los medios de prueba como factor de dinamización del derecho probatorio.*

11. ORTEGA BURGOS, Enrique. 2020. *Nuevas Tecnologías 2020.*

12. ORTEGO PÉREZ, Francisco. 2017. *La denominada prueba pericial de inteligencia policial.*

13. PÉREZ BESSIO, Ignacio. 2013. *Prueba documental electrónica en el proceso jurisdiccional: ¿estamos listos?*

14. VALLÉS CAUSADA, Luís Manuel. 2012. *La Policía Judicial en la obtención de inteligencia sobre comunicaciones electrónicas para el proceso penal.*

15. *La prueba electrónica, validez y eficacia procesal. Algoritmo Legal.*



Jean Deconinck

Digitalisation of criminal proceedings in the EU: the case of France

Barcelona, 6 November 2026

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

Co-funded by the EU

Agenda

01 Historical Introduction

Constant revision and extension· 2001 - today

02 Legislative Framework

Art. 706-71 CCP · Substantive law

03 EU & Constitutional Limits

ECHR · QPC 2026 decision

04 Advantages & Drawbacks

Overview

05 The CNB Position

Structured & constant criticism

06 The Cost-Driven Drift

Warning: systemic risk

07 Jurisprudence as Safeguard

CE 2020 · CC 2026

08 Conclusion

Key takeaways

09 Perspectives

What France needs · EU horizon

2001-2026 : constant revision and extension

2001-2021 : 8 different acts in less than 10 years, always broadening use of VC

2001 — First introduced as a strictly exceptional procedural tool - Law of 15 November 2001 : art. 706-71 of the French criminal procedure code (CPP)

2019 — Major reform: broader legislative authorization - expanded to all phases of the proceedings : investigation (custody), pre-trial detention, trial, sentencing, enforcement of sentences

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

2024 — 14th May 2024 : A prison convoy, transporting a prisoner, was attacked by criminals who managed to help the prisoner escape. Two prison officers lost their lives during the attack. In August, the Minister for Justice issues a circular calling for the widest possible use of video conferencing

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

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

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

Article 706-71 CPP : substantive law

Scope of Application

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

Key Conditions

Requires: judicial decision ; "*necessities of the investigations*" · technical guarantees (confidentiality, reliability) · consent of parties in some cases. Only a few prohibitions : judgment of serious crimes (*cour d'assises*), hearing on pre-trial detention, pretrial detention for minors

An Unstable Procedural Regime

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

The Right to Refuse

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

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

QPC n° 2026-1192 — 10 April 2026

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

Abrogation postponed to 31 October 2027.

Physical presence is a fundamental guarantee : but only effective for selected situations.

An easily overriden framework

Simplification, acceleration (modernization) and security at stake

EU Directive 2014/41

European Investigation Order

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

ECHR - Article 6

Right to a Fair Trial

Case law requires that video-hearings do not undermine the right to be heard effectively. France must ensure equivalent procedural guarantees whether physical or remote.
Analysis : very comprehensive approach towards this technology

In Marcello Viola c/ Italy, admission that “simplification” and “acceleration” of criminal proceedings can be invoked to justify VC : let States have full opportunity

Constitutional Protection

Conseil Constitutionnel

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

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

Advantages & Drawbacks

Advantages (for the judicial system)

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

Drawbacks (for the defendant)

- Impaired communication between lawyer and client during proceedings : absence of real solution provided for by confidential interview before the hearing
- Difficult choice for counsel: be at the court or beside the client? 2 lawyers ?
- Loss of solemnity - the physical trial has an irreplaceable human dimension
- Technical biases: angle, framing and image quality distort the judge's perception
- Dehumanisation of justice - the accused becomes a face on a screen
- Undermines equality of arms and the oral adversarial process

The National Bar Council: A Structured & Constant Critique

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

1 No normalisation

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

2 Defence of physical presence

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

3 Concrete risks to defence rights

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

4 Dehumanising effects

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

5 CNB's minimum requirements

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

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

Cost and safety-Driven Drift

Video-hearings are justified on budgetary and logistical grounds - not on the merits of individual cases : see Crim., 2 mars 2011, n° 10-88,524 : no justification needed

Key Risks

- Systematic use without genuine justification in each case : custodies (GAV), continuencies of pre-trial detention
- Erosion of the defendant's right to physical presence : limited to certain hearings.
- Gradual normalisation of a degraded form of justice for detained persons

CNB Reminder

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

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

The Judge as Guardian

When the legislature overreaches, courts push back.

Conseil d'Etat November 2020

Suspension of video-hearings in criminal trials

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

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

Conseil Constitutionnel April 2026

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

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

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

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

Key Takeaways

A Necessary but Limited Tool

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

Fundamental Guarantees

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

The Human Dimension

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

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

Perspectives

What France Needs

1

Mandatory advance notice

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

2

Right to counsel at remote end

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

3

Minimum technical standards

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

The EU Horizon

No unified EU standard yet

ECHR Article 6 being not very demanding, member States apply it differently. No binding EU directive setting minimum technical or procedural standards for video-hearings in criminal proceedings.

Defining minimum safeguards rights

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

The role of defence lawyers

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

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



John O’Doherty

Digitalisation of criminal proceedings in the EU: the case of Ireland

Barcelona, 6 November 2026

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

Co-funded by the EU

Contents

01 EU instruments and their digitalisation

02 Videoconferencing in criminal proceedings

03 E-evidence

04 Fundamental rights, ethics and AI

Part 1

EU instruments and their digitalization

John O'Doherty

Managing Partner
KOD Lyons LLP
Dublin

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 and 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) and conflicts of jurisdiction (2009/948)
- Criminal records and electronic evidence: ECRIS; and the e-Evidence package

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 to 2013, 2014 to 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 and 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
- Exceptions: physical or technical limits, where originals are required, or force majeure

Current situation

The system is currently being used in pilot mode for European Investigation Orders (EIOs). Further developments are underway in preparation for the entry into force of the e-Evidence Regulation.

The roll-out calendar, 2026 to 2029



- European Arrest Warrant (2002/584)
- European Investigation Order (2014/41)
- Freezing and Confiscation (2018/1805)

- Transfer of prisoners (2008/909)
- European Protection Order (2011/99)

- Confiscation orders (2006/783)
- Conflicts of jurisdiction (2009/948)

- Probation measures (2008/947)
- Supervision measures (2009/829)

Take-away

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

What it means for the defence

01 **Know the plumbing**
e-CODEX, e-EDES and the e-Justice Portal: understand how evidence now moves.

02 **Diary the deadlines**
Each instrument goes digital on its own date (2026 to 2029).

03 **Police the safeguards**
Consent, confidentiality, effective participation, identity and technical quality.

04 **Treat competence as ethics**
Digital literacy is now part of professional diligence.

05 **Build the remedy**
Challenge unlawful or unsafe digital practice under Art. 47 and the procedural directives.

Digital by default, human by design

The promise: faster, interoperable, more accessible cross-border justice. The condition: it must stay human-centric, transparent, fair, accountable and rights-respecting.



Part 2

Videoconferencing in criminal proceedings

The central question

The scenario

Romanian national in Bucharest. Criminal proceedings in Madrid. Physical transfer: months and a European Arrest Warrant. The court offers a videoconference.

Threat to the right of defence, or the right of defence made real?

Honest answer: it can be either. What matters is not the technology: it is the legal conditions under which it is used.

1. **Binding law**
   Second Protocol, EIO Directive and Regulation 2023/2844

2. **Case law**
   ECtHR (Strasbourg) and CJEU (Luxembourg)

3. **Current gaps**
   Eight risks the framework does not adequately address

Two different uses of videoconferencing

Use 1: taking evidence

Witness, expert or accused

- EU: Art. 24 Directive 2014/41/EU (EIO)
- Council of Europe: Art. 9 Second Additional Protocol (2001)
- Consent required for the accused
- Executing authority formally involved. Representative present
- Proportionality

Use 2: appearing at hearings

Bail, EAW, enforcement and trial

- EU: Art. 6 Regulation 2023/2844. In force: 1 May 2025
- Council of Europe: Art. 9 Second Protocol (2001)
- Express, free, informed consent after legal advice required
- Private lawyer channel guaranteed
- Conducting authority responsible

Common tension

Procedural efficiency vs. the right of the accused to a fair trial.

Legal framework: Council of Europe and the EIO Directive

Second Additional Protocol (2001, in force 2004)

To the 1959 Convention on Mutual Legal Assistance in Criminal Matters

- Art. 9: hearing witness or expert by videoconference when physical appearance not possible or desirable
- Judicial representative of the requested State present throughout; identity verified; witness may refuse
- Art. 9(8): written consent of accused required. Authorities of both States must agree
- Fully applies to: UK, Turkey, Ukraine, Western Balkans (non-EU Council of Europe members)

EIO Directive 2014/41/EU

Mutual recognition; narrow exhaustive refusal grounds

- The issuing authority issues the EIO; the executing authority must recognise and execute it
- Executing representative present, identity verified, proportionality (Art. 6)
- Executing State may refuse if accused does not consent: optional ground, accused only
- Art. 24(4): also refusable if not permitted in a comparable domestic case
- No unilateral videoconference: the executing authority must be formally involved

Legal framework: Regulation 2023/2844

Scope: appearances, bail, EAW and enforcement. Not evidence hearings, and not trial hearings on guilt. In force: 1 May 2025.

Article 6: three consent requirements

- Freely given
- Informed (reason stated)
- After legal advice

Three essential guarantees

- Right to interpretation
- Private channel with lawyer (before and during)
- Conducting authority responsible

Exception

Serious threat to public security or public health only

Key gap

The Regulation guarantees private lawyer-client communication but sets no mandatory technical standard for encryption, recording prohibition, or liability for breach. EU law says what must be achieved, not how.

ECtHR: building the framework

Marcello Viola v Italy (2006)

Videoconferencing is not contrary to Art. 6 if a legitimate aim is pursued and due process safeguards are in place

Sakhnovskiy v Russia [GC] (2010)

No technical obstacles, and effective, confidential communication with counsel is required

Kucera v Austria (9 Dec. 2025)

COVID-19 was a legitimate aim; no violation where counsel was present and no prior objection was raised

Six principles

- Videoconferencing is not, as such, contrary to Art. 6 ECHR (Marcello Viola)
- The legitimate aim must be justified in each individual case (Marcello Viola)
- Procedural safeguards must be in place (Sakhnovskiy)
- Technical quality: no obstacles to being effectively heard (Sakhnovskiy)
- Effective legal assistance and confidentiality (Sakhnovskiy)
- Public hearing (Kucera)

CJEU: key judgments

Gavanozov II
C-852/19, 2021

An EIO for a videoconference witness requires an effective remedy in the issuing State; fundamental rights need prior judicial review, not just safeguards during the hearing

FP and Others
C-760/22, 2024

Directive 2016/343 does not prohibit videoconferencing where the accused expressly requests it; Art. 6 ECHR safeguards are the minimum standard

Bissilli
C-325/24, 2025

An EIO may cover a videoconference appearance if it has an evidential purpose; the executing State cannot refuse solely on domestic-law equivalence. Individualised assessment always required

Key principles

- Directive 2016/343 does not prohibit videoconferencing
- Videoconferencing must comply with requirements of Art. 6 ECHR and Art. 47 Charter (FP and Others)
- Issuing an EIO for videoconferencing requires the existence of an effective remedy to challenge it (Gavanozov)
- Videoconferencing can be issued for evidentiary and for appearance purposes jointly (but not just for appearance)

Practical map: which rules apply?

Purpose of the videoconference	Situation	Applicable rules
Taking evidence	Same country	Domestic law (Art. 6 ECHR and Art. 47 Charter)
Taking evidence	Another EU State	EIO Directive, Art. 24
Taking evidence	Non-EU Council of Europe State	Second Additional Protocol 2001, Art. 9
Appearance only	Same country	National law (Art. 6 ECHR and Art. 47 Charter)
Appearance only	Bail, EAW or enforcement	Regulation 2023/2844, Art. 6
Appearance only	Trial hearing	EIO Art. 24 if for evidential also, or Second Protocol

Key distinction

The EIO requires an evidential purpose and cannot be used for pure appearance. For trial appearances without evidence, only the Second Additional Protocol (Art. 9(8)) provides a cross-border mechanism (mutual assistance, not mutual recognition).

Eight risks: gaps in the framework

1 **Confidentiality**
No encryption standard, no recording ban, no criminal sanction for breach

2 **Immediacy**
Camera distortion of judicial credibility assessment; no EU quality standard

3 **Equality of arms**
Detained accused lacks document access; unequal technical infrastructure

4 **Interpretation**
The Directive 2010/64 standard is very hard to meet across jurisdictions in videoconferencing

5 **Normalisation**
Routine post-pandemic use without an individual legitimate aim: who challenges?

6 **Vulnerable accused**
Zero specific safeguards in any binding instrument

7 **Fiction of consent**
Videoconference or in absentia? Regulation 2023/2844 lacks a verification protocol for free consent

8 **Solemnity**
The trial as a public constitutional event; a remote screen risks eroding democratic legitimacy

The CCBE's seven demands

1. **Exception principle**
   Videoconferencing is the exception for hearings on the merits; cost never justifies erosion

2. **Consent**
   Informed and free, with legal advice and effective remedy to challenge

3. **Lawyer in custody**
   An in-person lawyer at the detention site to prevent off-screen intimidation

4. **Confidentiality**
   Breach is a criminal offence; evidence obtained in breach is inadmissible

5. **Witnesses**
   Art. 6(3)(d): face-to-face examination at witness location if impossible

6. **Technical standards**
   A mandatory EU-wide minimum: a ‘true-to-life hearing experience’ and access to documents

7. **Training**
   Sufficient for competent authorities and legal practitioners

Why criminal matters demand heightened scrutiny

In criminal matters, videoconferencing is not a remote exchange. It is a mode of appearance.

- 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 and 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.

A toolkit for the defence

01 **Identify the procedural moment**
The graver the stakes, the higher the scrutiny.

02 **Object, on the record**
Where the law allows refusal, make it clear and reasoned.

03 **Demand reasons and alternatives**
Why no physical appearance? A delayed transfer or short adjournment may suffice.

04 **Protect confidentiality**
Secure a confidential channel with counsel and decide where counsel stands.

05 **Record every technical failure**
Frozen image, inaudible sound, no contact with counsel: preserve it in the record of the hearing.

Conclusions

What we have

- Basic architecture in place: Second Protocol, EIO Directive and Regulation 2023/2844
- Directly enforceable principles: legitimate aim, technical quality, confidential communications, remedies and fair trial guarantees
- Case law reactive, not preventive

What remains open

- No encryption standard, no consent verification, no safeguards for vulnerable
- Normalisation without justification: challenge it every time
- Use the law now: challenge EIOs, raise confidentiality failures, object on the record

Three converging signals

Irish constitutional law, the ECtHR and EU law point the same way: presence is the rule, remote appearance the justified exce ption. For the defence, videoconferencing is a litigation issue in its own right.



Part 3

E-evidence

What e-evidence is and why it matters

Any information generated, stored or transmitted in digital form that may later be needed to prove or disprove a fact disputed in legal proceeding (CoE Guide).



85%

of criminal investigations

Held by private service providers

Traditional tools are too slow

The European legal framework

Budapest Convention

Any offence involving digital evidence

- Core procedural powers
- International cooperation tools
- Transborder access in limited cases
- Innovative provisions: expedited preservation of stored computer data, partial disclosure of traffic data, production order, interception of content data

EU e-Evidence package

Regulation (EU) 2023/1543, Directive (EU) 2023/1544

- European Production Order (EPOC-PR)
- European Preservation Order (EPOC)
- Strict deadlines

European Investigation Order

- Used for broader investigative measures, including digital evidence
- Slower than EPOC/EPOC-PR but covers more intrusive actions

Budapest Convention: conditions and safeguards

Principle of proportionality. Judicial or independent supervision. Grounds justifying exercise of powers. Limitation of scope and duration of powers.

How to obtain e-evidence

Level	Routes
National level	National procedural powers
Between EU Member States	EPOC / EPOC-PR, EIO, MLA
With non-EU countries	Budapest Convention, Second Additional Protocol

E-evidence life cycle



Authenticity, integrity and reliability. Chain of custody.

Challenges and a checklist for lawyers

Challenge	
Diversity of legal frameworks	Lawyers must navigate a multi-layered system
Data volatility and speed	Real risk of losing evidence
Provider compliance	Inconsistent and unpredictable cooperation
Technical barriers	Data may be incomplete or unusable

Checklist for lawyers

- ✓ Data categories: different rules, threshold and safeguards
- ✓ Strict deadlines: 10 days / 8 hours (urgent)
- ✓ Fundamental rights safeguards: proportionality, necessity, judicial oversight
- ✓ Balance between right to privacy and effective investigation
- ✓ Service providers: broad definition (communication, hosting, domain…)
- ✓ Non-EU providers offering services in the EU

Case example: terrorism investigation

Encrypted message app. Multiple online accounts. Who did the suspect communicate with? Did an attack planning take place? Were others involved?

1. **Issue an expedited preservation request to the service provider**
   Freeze the data. It buys time while formal requests are prepared

2. **Obtain subscriber and traffic data**
   EPOC-PR or EIO. To identify the user behind several accounts

3. **Access content data**
   EPOC or MLA / Budapest Convention. Content can show intent, coordination and level of preparation

4. **Seizure and forensic extraction**
   Device data to corroborate provider data and fills gaps. According to legal procedures and judicial authorisation requirements?

5. **Verify authenticity**
   To demonstrate that the communications are genuine and unaltered. Assess legality

6. **Cross-border cooperation**
   Co-suspect or service provider in another EU Member State. Ensure the correct legal instrument and procedural safeguards respected

Present before the Court

Demonstrate authenticity, integrity, and lawfulness of acquisition: where the evidence came from, how it was preserved, how it was collected, that it was not altered, that it was obtained in accordance with procedural and fundamental rights safeguards.

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 and 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 device exists
- The condition is whether the relevant digital service stores, processes or enables access to the data sought

The two orders and the addressee

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
- 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

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 and 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

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.

Current routes and what e-evidence adds

Route	How it works today	Limits	Role after e-evidence
Domestic production request	A national authority orders an entity within reach to produce data	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

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, October 2026

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 18 Feb. 2026
Commission infringement package	Failure to communicate complete transposition measures	22 Member States targeted;

France: focus on a few points to clarify

- Who may issue an order?
- Who validates traffic / content orders?
- 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?

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 several 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

Necessity and proportionality

The order must be targeted and justified, and available in a comparable domestic case

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

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 and 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 and the lawyer's role

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?

Professional secrecy / privilege

Is protected material included or at risk? Arts. 5(9) to (10), 10 to 11, 12 and 18

Remedies

Can the order, the production, the preservation or the use of the evidence be challenged?

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 is not always labelled as privileged: the provider may not know, and the defence may discover it only later.

Case B: silent preservation and later disclosure

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.

A production order follows later; the defence then discovers the earlier preservation.

1 **The issue**

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.

2 **Defence requests**

The EPOC-PR, the EPOC, the dates, the scope, the preservation logs, the production history and the chain of custody.

3 **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.

two pillars of electronic evidence

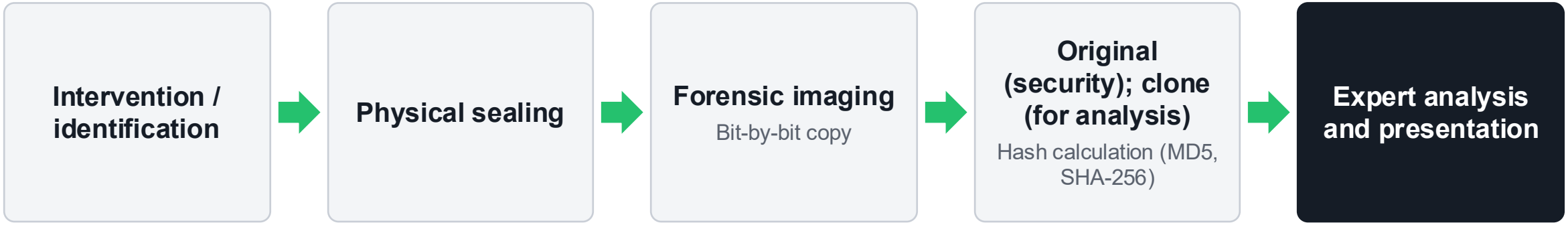
Lawfulness (legality)

- 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

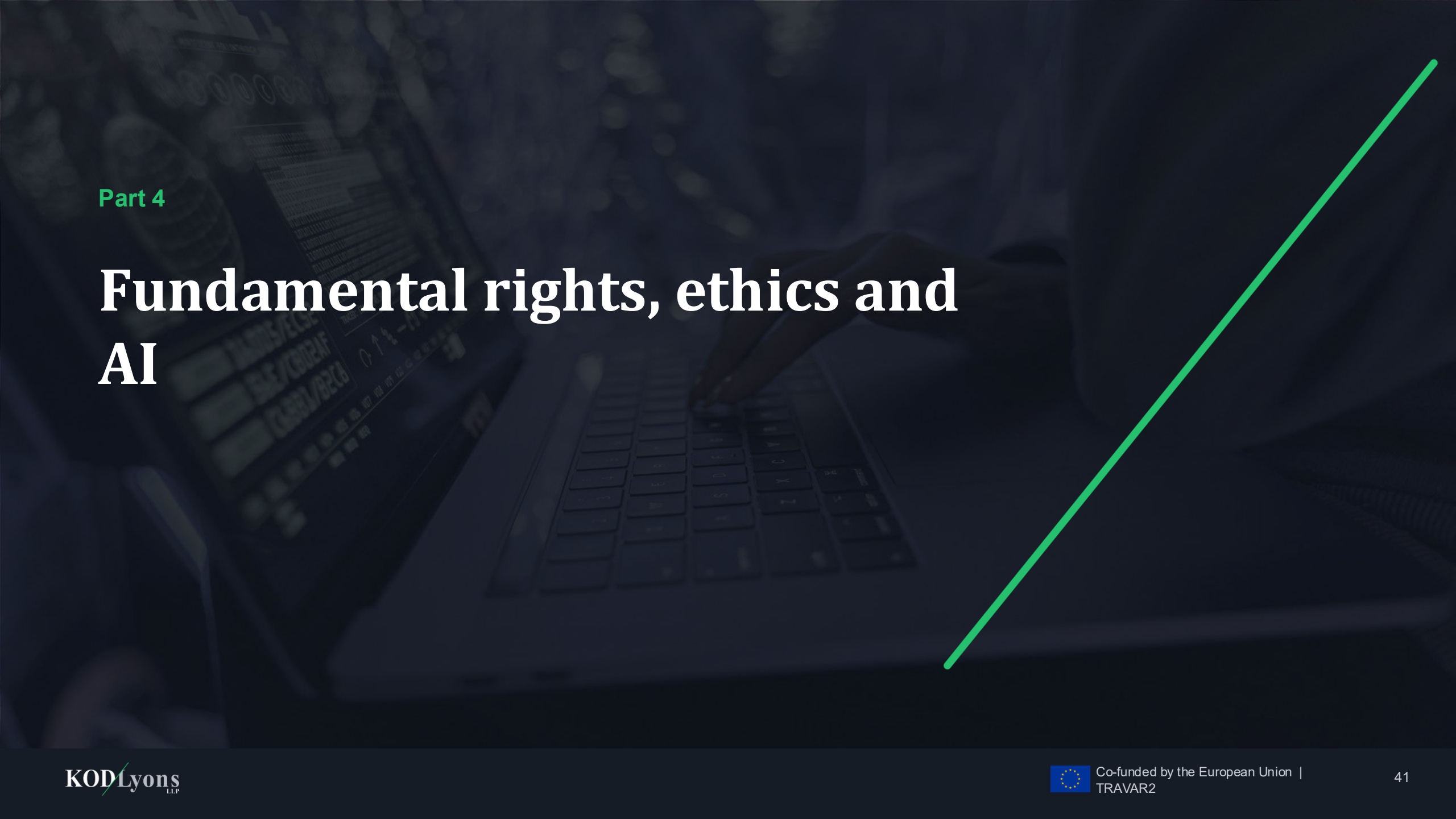
forensic chain of custody



If a single bit changes, the hash changes.

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.



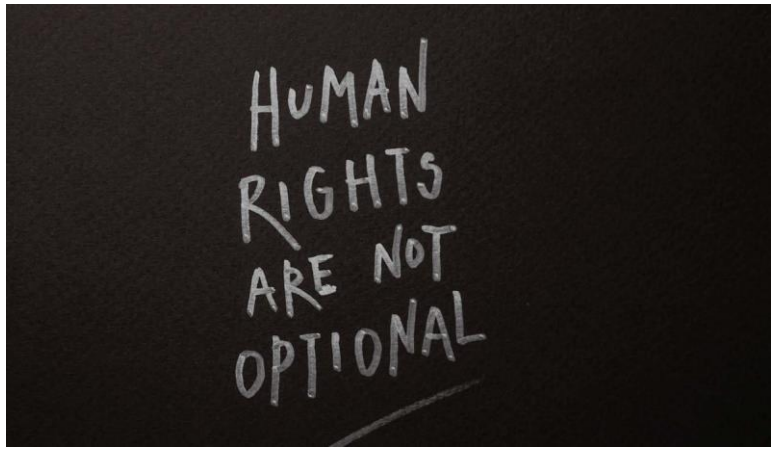
Part 4

Fundamental rights, ethics and AI

Key fundamental rights

These five rights allow us to understand the principal legal challenges posed by digitalisation:

- Article 6 ECHR: right to liberty and security
- Article 7 ECHR: respect for private and family life
- Article 8 ECHR: protection of personal data
- Article 47 ECHR: right to an effective remedy and a fair hearing
- Article 48 ECHR: presumption of innocence and rights of the defence



Key point

Digitalisation does not create new human rights, but it creates new ways of infringing them. Human rights must become the starting point of every digital transformation strategy in the justice sector.

The ethical pillars of the legal profession

We do not need a new ethics. We need to apply existing ethical principles to new circumstances.

Independence

We must ensure that technological dependence does not become professional dependence. Technology may support professional judgment, but it must never replace it

Confidentiality

Both a duty of the lawyer and a fundamental right of the client. Technology changes the way we receive, process and store information, but it does not change our obligation to protect it

Loyalty to the client

Lawyers must also ensure that the use of AI systems, digital platforms and automated tools does not compromise their independent judgement or their clients' legitimate interests

Integrity

New risks such as deepfakes, synthetic documents, manipulated evidence and AI hallucinations

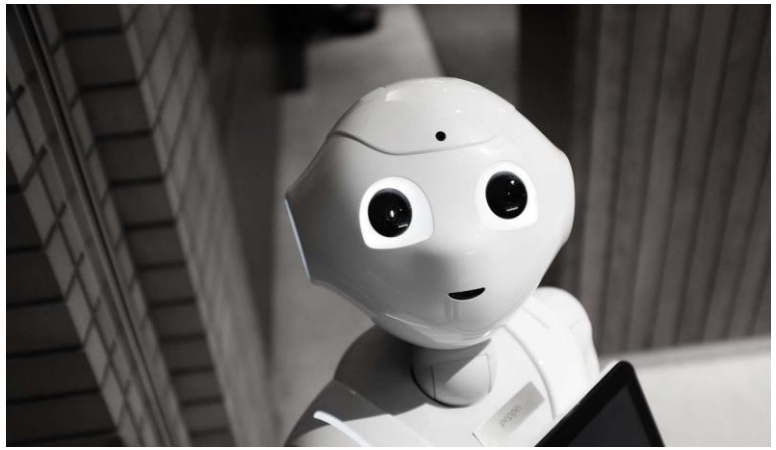
Professional competence

Lawyers are expected to understand technology sufficiently to supervise it, challenge it, explain it to clients and identify the risks associated with it

AI ethical aspects: the CEPEJ principles

In 2018, the CEPEJ of the Council of Europe adopted the European Ethical Charter on the use of Artificial Intelligence in judicial systems and their environment. CEPEJ has identified the following core principles that should be respected in the field of AI and justice, principles that continue to guide European thinking today:

- Principle of respect for fundamental rights
- Principle of non-discrimination
- Principle of quality and security
- Principle of transparency, impartiality and fairness
- Principle of user control



Key principle

Fundamental rights must not be adapted to technology. Technology must adapt to fundamental rights.

AI ethical aspects: the CCBE

AI-powered tools can support legal professionals in a wide range of activities, including:

- Legal research and the analysis of legislation, case law and legal literature
- Due diligence processes, contract review and compliance assessments
- E-Discovery and technology-assisted review
- Document automation

The report highlights the importance of:

- Human review and oversight
- Transparency and explainability
- Accountability
- The possibility of challenging AI-generated outcomes
- Judicial independence and procedural fairness

Key point

Legal responsibility cannot be delegated to an algorithm.

Responsible use, confidentiality and responsibility

Responsible use of AI systems

Blind reliance on automated outputs is incompatible with professional standards

Confidentiality and data protection

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

Non-delegable responsibility

Lawyers remain solely responsible for any document they sign or submit, regardless of whether AI has been used

Disciplinary liability and recommendations

Disciplinary liability and sanctions

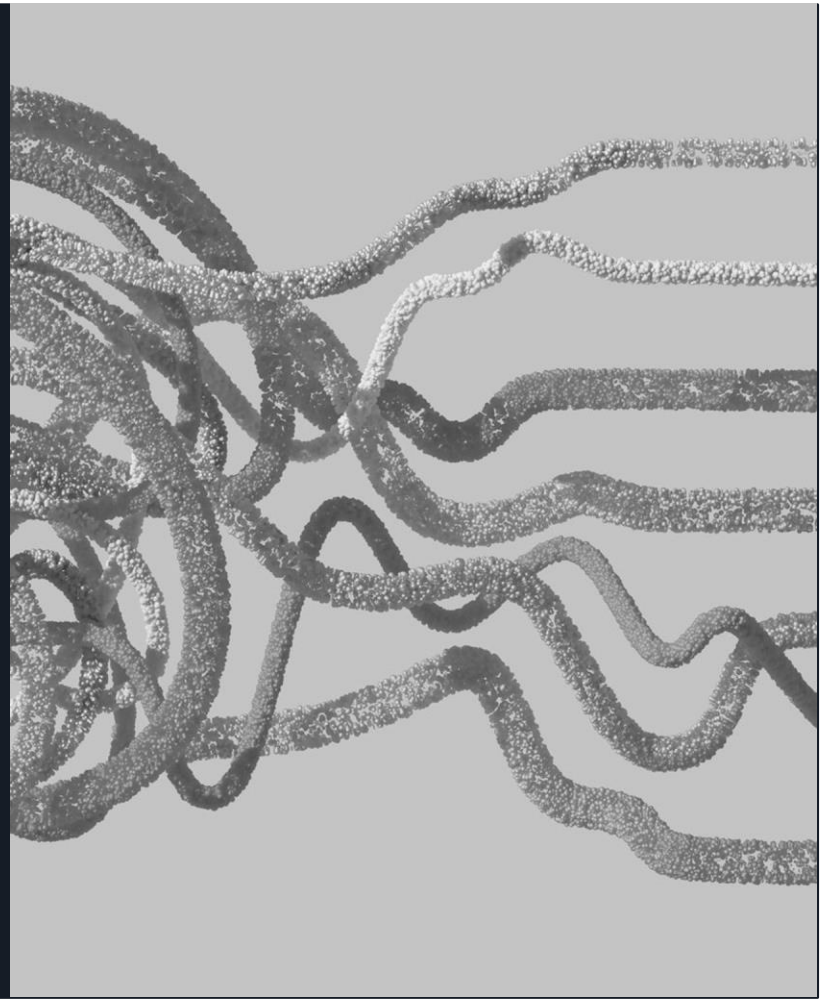
- Submitting erroneous documents or failing to verify AI-generated outputs may constitute a serious offence
- In more serious cases, especially where the conduct is repeated or causes significant prejudice to the client's defence, it may be considered a very serious disciplinary offence

Recommendations

- Understand the AI tools you use
- Never rely on AI outputs without critical review
- Always verify information against reliable legal sources
- Use AI only in areas within your expertise
- Maintain internal traceability of AI use

Final thoughts

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



The EU Charter

"Our EU Magna Carta"

Article 7

Respect for private and family life, home and communications

Article 8

Protection of personal data

Article 47

Right to an effective remedy and to a fair trial

Article 48

Presumption of innocence and rights of the defence

Article 49

Legality and proportionality of criminal offences and penalties

The European Declaration on Digital Rights and Principles (2022)

Status

- Binding: no
- Political vision: yes
- Digital rights: yes

Principles

- 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

Videoconferencing (Reg. 2023/2844): specific rights

Right to say no

Consent of the person concerned: 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

Where participation in a hearing in person poses a serious, genuine and foreseeable threat to public security or public health, and the derogation is strictly necessary. The person must have the possibility of seeking a review

Specific rights

- Confidentiality of lawyer-client communication
- Access to infrastructures
- Effective remedy

Lawyers' ethics in the digital era

Ethics: confidentiality, professional secrecy, independence, competence, diligence.

AI and algorithmic tools

- + Time-saving, quality time
- − Data protection, reliability, laziness, cost

Cybersecurity

- + Liability, data protection, competitiveness
- − Cost, competence, time-consuming, monitoring

Digital inequality

- Money privilege
- Asymmetry defence / prosecutor
- Unrepresented individuals

Specific issues

- Training
- Remote hearings vs effective client consultation
- Environmental issues

Irish legislative development

The Bill

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

The presumption of presence

01 A fundamental tenet of jury trial

02 Judge, counsel, defendant, witnesses and public are ordinarily present

03 Irish law allows limited derogations in defined circumstances

04 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

When departure from presence may be justified

01 Encroachment on the presumption of presence must have a purpose

02 Particular relevance for vulnerable victims and witnesses

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

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

Artificial intelligence: main AI dangers

Main AI dangers

- False information and hallucinations
- Bias and discriminatory outcomes
- Lack of transparency
- Confidentiality, privilege, and professional negligence risks

1 **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.

2 **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.

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."*

Manipulated evidence and safeguards

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

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

Key points

01

EU instruments

Cross-border criminal cooperation goes digital instrument by instrument between January 2026 and January 2029, through e-CODEX, the e-EDES portal and Regulation 2023/2844.

02

Videoconferencing

the ECtHR and EU law agree: presence is the rule, and remote appearance is the justified exception.

03

E-evidence

The e-Evidence Regulation applies from 18 August 2026. The defence questions start with who issued the order, its scope and its timing.

04

Rights, ethics and AI

AI can support legal work, but responsibility stays with the lawyer. As the Court of Appeal made clear in Von Geitz v Kelly & Robertson, every litigant must check what an AI tool produces.