

Lapo Gramigni

Overview of criminal law instruments and their digitalisation

Florence, 25 September 2026

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

Co-funded by the EU

1.From paper justice to paperless justice from the viewpoint an italian lawyer: a challenging work in progress

Stage 0: PAPER (an Amish Community in the Courthouses)

Stage 1DIGITISATION (the scanner era; paper begins to vanish, first, only from law offices' shelves and briefcases: stage 1.1: scannering by the lawyers; stage 1.2 scannering by the record offices)

Stage 2 DIGITAL TECHNOLOGIES AND DIGITALISATION (the rush during the COVID-19 pandemc)

2. digitalisation

Digitalisation in more detail:

- its meaning in general...
- and its application to the administration of justice.

3. Digital habits of humans and digital evidence in criminal proceedings

- The Increasing Relevance of Digital Evidence in Criminal Proceedings (either analogic or digital) and the Need to Balance Crime Detection and Prosecution Requirements with the Right to Privacy:

- A paradigmatic case: the seizure of a smartphone and the protection of the personal data stored in it

… in the decisions of the CJEU (4.10.2024 in proc,. C 548/2021)

… and in the italian Supreme Court decisions (Sez n. 44424/2026)

-

The Convention of Budapest: data are ‘things’ (art. 19).

The ***Preventive Seizure*** **of a Web Page** to Prevent Further Harmful Effects of a Criminal Offence Related to Its Content….

…in italian supreme court (Corte di Cassazione) decisions (SS.UU. 31022/2015)…

… and in CJEU decisions (Judgment 2019, october 3th, in case C-18/18)….

Segue 3. Digital habits of humans and digital evidence in criminal proceedings

The legal framework of the e-evidence

[...]

4. The crossroads

Judicial Technology vs. Technological Justice (Prof. Luca Luparìa Donati)

- **Judicial Technology**: Tools for a due process of law

- **Technological Justice**: Hardware and software that affect judicial decision-making or, more troublingly, substitute themselves for human judges in the administration of justice.

4.1 The digital instruments of judicial technologies

A. ELECTRONIC TRANSMITTING AND DELIVERY OF COMUNICATIONS, NOTIFICATIONS, SUMMONS – DIGITAL ADDRESS

- (mandatory) registered electronic address for lawyers, for companies and for professionals

B. ELECTRONIC LODGING/FILING OF CLAIMS, BRIEFS, MOTIONS, APPLICATIONS, PROSECUTOR'S OPINIONS, DECISIONS

- E-filing
- E-signature
- Born digital act and e-filing: digital first, if not digital only

C. THE ELECTRONIC CASE-FILE AND THE FULL ACCESS TO IT FOR THE PARTIES: PROBABLY THE CORE OF A (any, rather than CRIMINAL) TELEMATIC PROCEEDING

C.1 THE CURRENT ITALIAN SITUATION: A PARADOX AND A BREACH OF EQUALITY OF ARMS

D. ATTENDANCE TO HEARINGS: **remote hearings** (Judges sit in the courtroom) and **virtual hearings** (nobody sits in the courtroom)

D.1 The critical aspect of the italian regulation: the abuse of remote hearings in trials concerning defendants in detention charged with major offences (organized crime, sex assaults, murders); article 41-bis defendants and the ban on in-person attendance at hearings

4.2 Border-lines

- AI court-transcribers
- AI interpreters
- AI large language models and comprehension of recorded/wire-tapped conversations and voices

4.3 The digital instruments for a technological justice: the IA systems

- the notion of an AI system; the definition of IA system provided by regulation 2024/1689; the ***capability to infer*** (whereas 12; art. 3, n. 1)

- The legal framework of AI Systems in the administration of justice: the **High-Risk AI Systems** (whereas 9, 48, 59, 61 art. 6. annex III n. 8)

AI models for risks assessments: the **Predictive Justice**

Outlines of two applications:

COMPAS (USA)

HART (UK)

AI-made decisions: the next future scenario of a **Machine Learning trained on IA generated contents and the risks** (certainty, at the state of the art) **of model-collapse**: the photocopies example and t*he bell curve of human knowledge*

Final wishful thinkings

Let’s hope never to be Judged by a machine, as we hope never to be judged solely on the basis of statistical probabilities, without taking into account that our free will may have been stronger than the conditioning to which we was subjected, and without taking into account that we should be found guilty only if our guilt is proven beyond a reasonable doubt.

At the moment, the European legal framework appears to protect us from such risks, and that is good news.

Final wishful thinkings

Thus, let us hope that jurisdiction will not be eliminated from our democratic societies. Just as we hope that human beings will continue to elect human beings to make laws in parliaments, let us also hope that human beings will continue to interpret, enforce and apply those laws in the name of "We, the People." (“in nome del popolo” article 101 of italian Costituzione says).

So, Echoing Winston Churchill's speech before the House of Commons on 11 November 1947 (*"Many forms of Government have been tried, and will be tried in this world of sin and woe. No one pretends that democracy is perfect or all-wise. Indeed, it has been said that democracy is the worst form of Government except for all those other forms that have been tried from time to*

Final wishful thinkings

time”), adapting that reflection to our matters and turning the sentence from the past tense into the future tense, let me say that

"Decisions rendered by humans about humans are the worst form of justice, except for all those other forms of adjudication or resolution of criminal and civil disputes that artificial intelligence systems could arrange for us"



Jani Trias Arraut

Considerations of fundamental rights and lawyers' ethics regarding digitalisation

Florence, 25 September 2026

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

Co-funded by the EU

SPAIN, 1 JANUARY 2016

LexNET

The day the system goes down, the whole Spanish legal profession discovers it has a fundamental right to a coffee break.

When access to the court depends on a system, the failure of the system is not an IT incident. It is a restriction of a fundamental right.

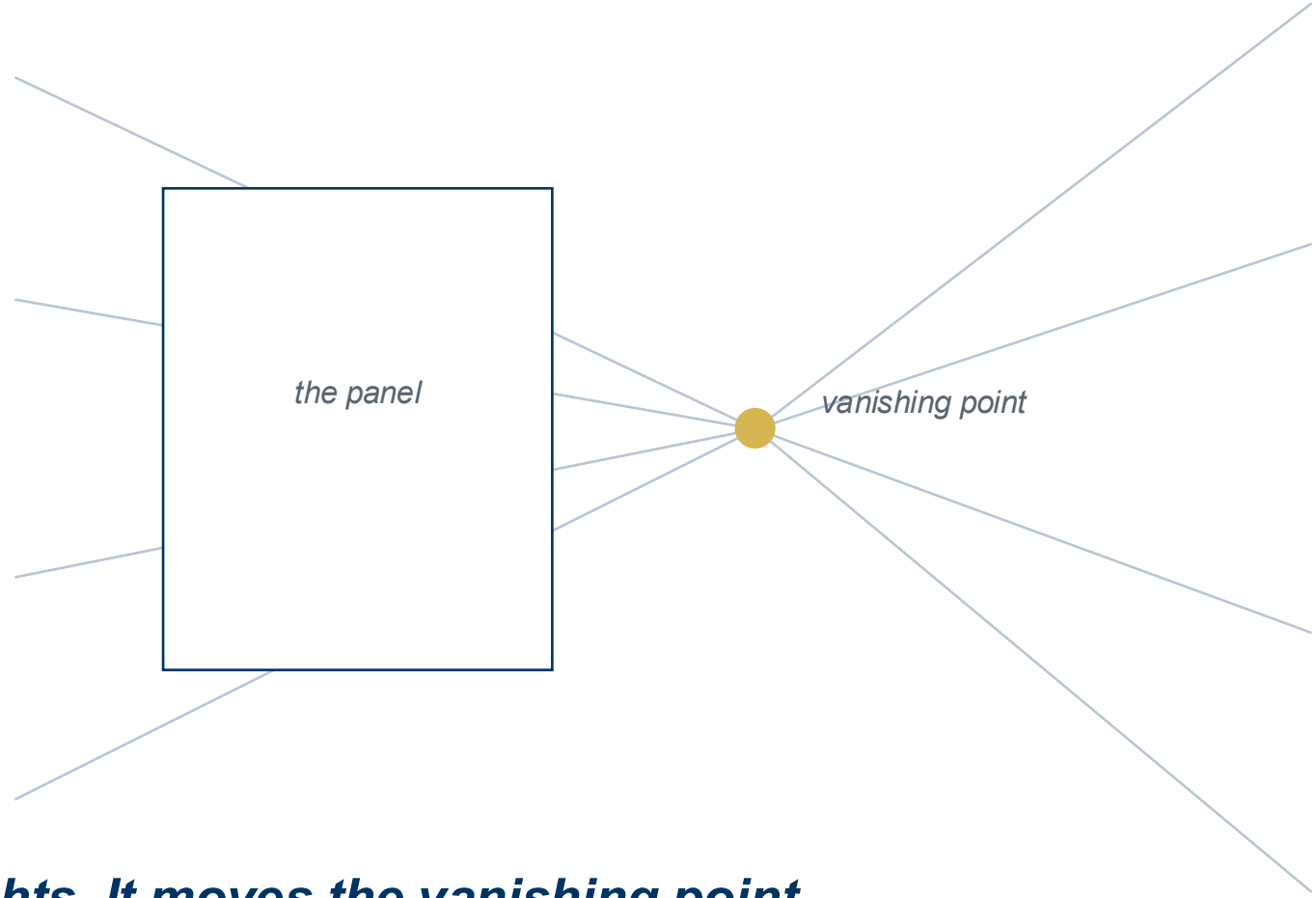
FLORENCE, C. 1415

The screen is a perspective device

Brunelleschi's panel worked from one point only.

Move your eye and the picture is wrong.

Digitalisation is not paper becoming screen. It is a change of perspective. The rights stay the same. The point from which they are exercised moves.



Technology does not change the rights. It moves the vanishing point.

THE METHOD

Five questions. Five mirror tests.

Brunelleschi did not trust his own eye

He built a test. The mirror was there so that anyone, not only the painter, could check whether the picture was right.

A mirror test is a question you put to the system, in writing if you can, whose answer tells you whether the picture is right from where your client stands.

Five tests. That is the whole talk. Everything else is footnotes, and the footnotes are verified.

1. **Is the person present?** *Federico, after the coffee*
2. **Is the conversation still confidential?**
3. **Can we argue about the evidence as equals?**
4. **What happens when the tool is ours?**
5. **Who is left outside the frame?**

None of them is about technology. From where am I looking, and who placed the camera?

THE MAP

Three shelves, three speeds

1 Instruments

Changes every year

Reg. 2023/2844 (digitalisation). Reg. 2023/1543 (e-Evidence, applicable 18 Aug 2026; 22 Member States on formal notice since March; Commission contingency guidance of July: secure email while the decentralised system is not there). Dir. 2014/41 (EIO). AI Act 2024/1689 as amended by Reg. 2026/1744 (AI Omnibus: high-risk deferred to 2 Dec 2027, Art. 50 in force since 2 Aug 2026).

2 Rights

Changes once a generation

Charter Arts. 47, 48, 7, 8. ECHR Arts. 6, 8. Roadmap directives 2010/64, 2012/13, 2013/48 (Art. 4 confidentiality), 2016/343 (Art. 8, the right to be present, covered by Federico Cappelletti after the coffee), 2016/800, 2016/1919.

3 Ethics

Should be the most stable. Has adapted worst.

CCBE Charter (2006) and Code. CCBE Guide on generative AI (2 Oct 2025) and technical guide (27 Mar 2026). ELF report on digitalisation of justice and fundamental rights (Dec 2025). CoE Framework Convention on AI (EU ratified May 2026). CoE Convention on the Profession of Lawyer (2025): needs 8 ratifications; in June 2026, 31 signatures and none.

1

Is the person present?

After the coffee, with Federico Cappelletti

Strasbourg and Luxembourg case law, Art. 6 of Regulation 2023/2844, the safeguards before a link goes live, the ECBA benchmark, the Commission's ERPO proposal of June 2026.

One thing to listen for. Everything hangs on two hinges, the consent of the person and the channel to the lawyer.

From where am I looking, and who placed the camera?

2

Is the conversation still confidential?

Mirror test 2. The mailbox test

From where am I looking, and who placed the camera?

From a folded piece of paper to the cloud

2013

Directive 2013/48, Art. 4

Confidentiality of meetings, correspondence, telephone calls and 'other forms of communication'. Written before Signal, Teams and the cloud.

2018

Laurent v France

A folded note, read by the escort. Violation of Art. 8. Lawyer-client correspondence enjoys privileged protection.

2022

Orde van Vlaamse Balies, C-694/20

Art. 7 Charter protects the secrecy of legal advice. DAC6 notification duty struck down.

2024

Ordre des avocats, Luxembourg, C-432/23

Protection 'irrespective of the area of law'. Carving out tax advice 'renders that protection devoid of its very substance'.

2024

Spain, LO 5/2024, Art. 16

All lawyer-client communications confidential; inviolability of all documents relating to the defence. All. Not 'on paper'.

QUESTION 2. E-EVIDENCE, REG. 2023/1543, APPLICABLE 18 AUG 2026

Who in the chain knows the mailbox belongs to a lawyer?

Issuing authority

Must not issue if it has 'reasons to believe' the data are privileged (Art. 5(9)-(10)). Only if it suspects.

Service provider

10 days, or 8 hours in an emergency. Fines up to 2% of turnover. Does not know, and is not asked.

Enforcing authority

Notified for traffic and content data (Art. 8). May refuse if privileged under its own law (Art. 12). Cannot check who the account holder is.

Lawyer and client

Effective remedy (Art. 18). Afterwards. After the data have been read.

No European definition of 'professional privilege'. In-house or not, client's or lawyer's, file or communication: each pillar of the bridge measured in a different unit.

Art. 1(2) lets the defence request an order too. But the defence has no issuing authority; it has to persuade one. The asymmetry is not in the text. It is in the plumbing.

A STORY FROM MY OWN PRACTICE, NAMES REMOVED

For several months, the most diligent reader of my correspondence with that client was not my client. Not the court. Not even my associate. It was a gentleman with a forwarding rule.

Nobody intercepted anything. No production order. No police officer unfolding a note. A setting in a menu that nobody had looked at.

Confidentiality is now a duty of custody. CCBE Guide (2 Oct 2025): beware of AI features 'embedded in everyday software'. My answer: a criminal file sent through an unencrypted, unaudited mailbox, with transcription switched on, is already a breach of that duty, whether or not your Bar's code has caught up.

MIRROR TEST 2

The mailbox test

One question, asked once for every criminal file and then once a year. Who else can read this?

1 Three settings

Forwarding rules on every mailbox in the firm, and on the client's if they let you look. Transcription features of every meeting tool, on by default. The assistant that came with the last update of your office software.

2 One contract

No client data into any tool without terms you have read that say two things. No retention. No training. If the provider will not put it in writing, the answer to the question is 'the provider'.

3 One question for the file

When the evidence includes communications, ask in writing whether the issuing authority checked for privilege (Art. 5), whether the enforcing authority was notified (Art. 8), and ask for the exclusion of anything that was yours.

If the honest answer to 'who else can read this' is 'I do not know', then you already know.

3

Can we argue about the evidence as equals?

Mirror test 3. The key test

From where am I looking, and who placed the camera?

QUESTION 3. ENCROCHAT AND SKY ECC

Three courts, one direction

CJEU, Grand Chamber, C-670/22 M.N., 30 Apr 2024

Device infiltration is 'interception' (Art. 31, notification).

The national court must exclude evidence if the person 'is not in a position to comment effectively' on it and it is likely to have 'a preponderant influence' on the findings of fact.

Cassazione, Sezioni Unite, 23755 and 23756 of 2024

Evidence already held abroad may be requested without prior Italian judicial authorisation.

No access to the decryption algorithm does not in itself violate fundamental rights. Unusable only if the party alleges and proves a violation.

Tribunal Supremo, Plenary, STS 854/2025, 16 Oct 2025

French EncroChat data admitted through an EIO. 'Accidental finding' doctrine extended to cross-border digital investigations.

Control of legality belongs to the receiving State. The defence had to show the illegality.

Luxembourg says the evidence goes if you cannot comment effectively. Rome and Madrid say it stays unless you prove otherwise. The burden lands on the one person without the key.

Integrity of transmission is not integrity of evidence. e-CODEX guarantees the file arrived in Florence as it left Paris. It says nothing about Paris.

MIRROR TEST 3

The key test

For any evidence that was gathered, decrypted or transmitted somewhere you cannot see.

Four questions about the chain

1. Where was it obtained, and under what authorisation?
2. How was it decrypted, by whom, and can an independent expert see the method?
3. How was it transmitted, and what exactly does the transmission guarantee? e-CODEX guarantees the file, not the facts.
4. Who verified it at the receiving end, and against what?

One written request

The raw data with its hash values. The method or, failing that, access for an independent expert under a duty of confidentiality, as in any DNA case. The Art. 31 notification if a device was infiltrated.

One rule for the refusal

The refusal goes in the file, word for word. It is the proof that the client is 'not in a position to comment effectively' (C-670/22). You do not argue the abyss. You document it.

QUESTION 3. DEEP FAKES (ACCORDION)

The evidence that looks true, and the truth that looks fake

86%

'probability of manipulation'. The detector cannot tell you why, or whether it is just compression. Another black box, in the evidence room.

AI Act, Art. 50

In force since 2 Aug 2026 (watermark grace period to 2 Dec 2026). Providers must mark AI-generated content and deep fakes. Protects you against the honest provider. Not against the criminal.

The liar's dividend

The defendant who says a genuine recording is a deep fake. No decided European criminal case with a deep fake as central evidence that I could verify. A risk, not case law. Give it two years.

4

What happens when the tool is ours?

Two cases, Florence and Barcelona. Mirror test 4. The reading test

From where am I looking, and who placed the camera?

QUESTION 4. CASE ONE

Tribunale di Firenze, 14 March 2025

Business section, R.G. 11053/2024. A trademark case.

A collaborator used ChatGPT to research case law. The brief cited Cassazione judgments that did not exist.

The court's word: 'hallucinations'. When a lawyer does it we call it a hallucination. When a witness does it we call it perjury.

Aggravated costs under Art. 96 c.p.c. refused. Good faith. The false citations 'were not objectively capable of influencing' the decision.

Two reactions. Relief. And: the court was generous, and the next lawyer will not be so lucky.

The hallucination is not a failure of the machine.

It is a failure of the lawyer who did not read.

QUESTION 4. CASE TWO

Tribunal Constitucional, 16 September 2024

19

quotations from Constitutional Court judgments, in quotation marks, as literal text. None of them existed.

A lawyer of my own Bar. An application for amparo.

Application rejected. Disciplinary proceedings opened. Lightest sanction: a formal warning. File sent to the Barcelona Bar.

Possible explanations noted by the Court: 'the use of artificial intelligence' or 'the false quotation of the lawyer's own arguments'.

The lawyer's defence: a misconfigured spreadsheet.

As a member of the Barcelona Bar, I would like to state for the record that our spreadsheets are innocent until proven guilty.

QUESTION 4. THE RULES

The third shelf has finally started to move

CCBE Guide on generative AI, 2 Oct 2025

Independence, confidentiality, conflicts, dignity, loyalty, competence, rule of law: almost every core principle under pressure.

Verify outputs 'where the use case requires'. Inform the client where 'an informed client would object'.

Three words for every ethics course: black box, automation complacency, sycophancy.

Italy, Law 132/2025, in force 10 Oct 2025

Art. 13. AI in the intellectual professions only as an auxiliary and supporting tool; the professional's own work must prevail; the client informed 'in a clear, simple and exhaustive manner'.

Art. 15. The judge always decides. AI in the courts only for organisation and support.

How do you inform 'exhaustively' about a tool its own provider cannot exhaustively explain?

AI Act, Annex III, point 8

AI intended to assist judicial authorities in researching and interpreting facts and law: high-risk. Deferred to 2 Dec 2027 by the AI Omnibus.

'Very limited aspects of the administration of justice are seen as high risk' (ELF report, Dec 2025, p. 35). Annex III looks at the judge. It does not look at the lawyer.

For the lawyer with a chatbot there is no AI Act. There is only the third shelf. There is only us.

Four controversies, four answers

1 Is the machine's error the lawyer's error?

Yes. Without qualification. The hallucination is not a failure of the machine. It is a failure of the lawyer who did not read.

2 Must the client be told?

Italy says yes, by statute. The CCBE, when an informed client would object. Spain, nothing. My answer: one sentence to the client whenever a tool has touched the substance or the data.

3 May the judge use it?

If a tool summarised the file for the court, the summary shaped the decision and is part of the materials of the case (Dir. 2012/13, Art. 7; Art. 47 Charter). Ask in open court. The summary is where the vanishing point is placed.

4 Competence

A duty to know how to use these tools, or a duty to know when not to? Both. The second is harder.

MIRROR TEST 4

The reading test

The shortest, the most boring, and the one that keeps you out of the newspapers.

1 Open the source

Every authority that leaves the office has been opened by a human being, in the original source, and read. Not the summary. Not the snippet. The source.

2 Read the contract

Every piece of client data that goes into a tool goes in under terms you have read. No contract, no data.

3 Tell the client

Every client whose case a tool has touched gets one sentence saying so.

4 The office rule

Any authority generated by a machine is verified by a human. Any authority generated by a human is verified by a second human. Any authority generated by me is verified by Andrea.

The hallucination is not a failure of the machine. It is a failure of the lawyer who did not read.

5

Who is left outside the frame?

Mirror test 5. The edge test

From where am I looking, and who placed the camera?

QUESTION 5. ACCESS

Digital by default treats equally people who are not equal

For the professional	*an obligation*	Spain, LO 5/2024, Art. 19.3: duty to use the systems established by the administration of justice.
For the person	*a right*	Art. 10.f: to deal with the courts electronically 'if they so request'. Reg. 2023/2844: European electronic access point, optional for natural persons, subject to implementing acts.
For the detained foreigner	*a wall*	No device, no language, no lawyer of his own choosing. Interpretation by video (Dir. 2010/64) and children (Dir. 2016/800) lose the most.

Art. 3.5 LO 5/2024: electronic means 'must be universally accessible and compatible with the effective exercise of the right of defence'. LexNET comes back. Art. 135.2 LEC, written after the outages, allows filing on the next working day with a certificate of the interruption. ELF report, p. 34: 'Provision should always be made for a fall-back if the system fails.'

MIRROR TEST 5

The edge test

For every digital-by-default step in your client's case, three questions.

1 Can the person opt out?

The person, not the professional. And has anyone told them so, in a language they read?

2 What is suspended when the system fails?

Automatically, and who has to prove the failure? If the answer is 'the lawyer', the rule is wrong. Say so in writing before the first outage.

3 Can the accused see his own file?

Or only his lawyer? I do not know a Member State where a detained accused can open his own file from the cell. If you do, tell me at the coffee.

Digital by default treats equally people who are not equal. The system adapts to the accused, not the other way round.

SUMMARY

Five questions, five tests

1. **Is the person present?** *Federico Cappelletti, after the coffee*
2. **Is the conversation still confidential?** *The mailbox test*
3. **Can we argue about the evidence as equals?** *The key test*
4. **What happens when the tool is ours?** *The reading test*
5. **Who is left outside the frame?** *The edge test*

None of them is a question about technology. Who sees, from where, and who placed the camera. Technology does not change the rights. It moves the vanishing point.

ONE DEMAND. NOT FOR US, FOR BRUSSELS

Binding minimum standards on professional secrecy, under Article 82 TFEU.

CCBE contribution to the High-Level Forum on the Future of EU Criminal Justice, 8 October 2025, p. 31.

Rules on searches of law offices and on technological surveillance. A rule of inadmissibility for evidence obtained in violation of professional secrecy. Rules on the lawyer as a witness or as a defendant.

Twenty-seven definitions of a privilege that now travels across twenty-seven borders in ten days. The e-Evidence Regulation was adopted under Article 82. So can the standard that protects our clients from it.
The ECBA says it in general terms, and Federico will show it after the coffee. Every new enforcement tool must be matched by defence rights. This is the narrow version.

BRUNELLESCHI NEEDED A MIRROR

We are the mirror. If the picture does not look right from where the defendant stands, it is our job to say so.

Out loud. In writing. Through whatever platform is working that day.

Thank you. Enjoy the coffee. I am reliably informed that it is real, and not virtual.

Jani Trias Arraut, Barcelona Bar. TRAVAR 2, Florence, 25 September 2026



Federico Cappelletti

Use of Videoconferencing in Criminal Matters

Florence, 25 September 2026

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

Co-funded by the EU

The proposition

A screen may widen access. It must not become a cheaper substitute for presence.

Protect liberty

Avoid arrest or detention merely to secure attendance

Preserve agency

Understand the case, instruct counsel, react and decide

Keep presence real

Retain the courtroom whenever video would weaken the defence

Remote participation is legitimate only when it protects rights.

Two uses of videoconferencing

The same screen may serve different legal functions

TAKING EVIDENCE

Witness · Expert · Suspect / Accused

- Evidential purpose required
- Executing authority formally involved
- Identity, safeguards and proportionality checked

REMOTE PARTICIPATION

Attendance at a procedural hearing

- Identify the procedural stage, legal basis and purpose
- Participation is not evidence-taking
- Consent and defence rights remain decisive

Same technology. Different legal basis. Different safeguards.

Rights floor and procedural vehicles

THE RIGHTS FLOOR

Council of Europe

- ECHR Arts 5, 6 and 8: liberty, a fair and public hearing, defence, confrontation, interpretation and privilege

European Union

- Charter, Arts. 47 - 48
- Directives 2010/64/EU, 2012/13/EU, 2013/48/EU and (EU) 2016/343

THE PROCEDURAL VEHICLES

Evidence across borders

- CoE: Second Additional Protocol to the European Convention on Mutual Assistance in Criminal Matters, Art. 9
- EU: EIO Directive 2014/41/EU, Art. 24

Remote participation in cross-border proceedings

- CoE: Second Additional Protocol, Art. 9(8)
- EU: Regulation 2023/2844, Art. 6
- Domestic: national procedural law

Procedure permits the link. Fundamental rights decide whether its use is fair.

Convention rights in remote hearings

LIBERTY · ART. 5

Avoid custody solely to secure attendance

PUBLICITY · ART. 6(1)

Keep the court open, identifiable and accountable

COUNSEL · ART. 6(3)(c)

Effective assistance through a privileged channel

CONFRONTATION · ART. 6(3)(d)

Follow and test evidence in real time

INTERPRETATION · ART. 6(3)(e)

Comprehension across every audio channel

PRIVACY · ART. 8

Secure the remote room and lawyer consultation

Effective presence is a bundle of functions, not a camera status.

Strasbourg: safeguards for fairness

2006

Marcello Viola v. Italy,
no. 45106/04,
5 October 2006

A legitimate aim and effective participation remain essential

Art. 6 – no violation

2010

Sakhnovskiy v. Russia [GC],
no. 21272/03,
2 November 2010

Quality, preparation and private consultation determine fairness

Art. 6 § 1 in conjunction with § 3 (c) - violation

2021

Dijkhuizen v. the Netherlands,
no. 61591/16,
8 June 2021

Repeated and unequivocal refusal to participate by video link may amount to a waiver of the right to attend

Art. 6 – no violation

2025

Stephan Kucera v. Austria,
no. 13810/22,
9 December 2025

A fully remote hearing is compatible with the ECHR only if fairness remains practical and effective

Art. 6 – no violation

A fully remote hearing may comply with Article 6 where it pursues a legitimate aim and practical safeguards preserve fairness.

Luxembourg: authority and remedies

Gavanozov II

C-852/19 · 11 November 2021

Directive 2014/41/EU, Arts. 6, 14 & 24(7) · Charter, Art. 47

An EIO for searches, seizures and a witness hearing by video cannot be issued where the issuing State provides no effective remedy against its substantive grounds

FP and Others

C-760/22 · 4 July 2024

Directive (EU) 2016/343, Art. 8(1)

Whether video participation is available is a matter of national law. Article 8(1) does not preclude it at the accused's express request, provided that the trial remains fair.

Bissilli

C-325/24 · 18 December 2025

Directive 2014/41/EU, Arts. 3 & 24(2)(b)

An EIO may be used to hear an accused by video at trial for a genuine evidential purpose. Refusal on fundamental-principles grounds requires an individual assessment.

Legal authority, safeguards and an effective remedy must operate together.
Strinotto (C-499/25) remains pending.

Before the link goes live

ROOM

Who is in the room with the accused?

Risk: confidentiality / undue influence

PRIVILEGE

Can lawyer and client speak privately and immediately?

Risk: legal assistance / Art. 6(3)(c)

DOCUMENTS

Does the accused have access to the same material?

Risk: equality of arms / preparation

AUDIO · VIDEO · INTERPRETATION

Can the accused see, hear and understand?

Risk: effective participation / Art. 6(3)(e)

INTERVENTION

Can the accused react and consult counsel when needed?

Risk: effective defence / confrontation

FAILURE · REMEDY

Can the hearing be stopped and physical presence restored?

Risk: fair trial / effective remedy

If one of these functions is missing, the issue is no longer technical. It is procedural.

The ECBA starting point

ECBA Statement (2020) · Renewal initiative (2026)

Virtual attendance is not equivalent to actual physical presence

DOMESTIC TRIALS

The accused retains the right to attend in person. A mandatory video link at trial should be prohibited

CROSS-BORDER CASES

Video can widen participation and reduce unnecessary coercion when the accused requests it and safeguards remain effective

Purpose and choice determine whether distance protects or weakens the defence.

A new roadmap for defence rights

ECBA's Agenda for European Criminal Justice

Enforcement powers have expanded faster than procedural safeguards

The 2009 Roadmap delivered six directives. Progress then stalled as mutual recognition, the EPPO and digital evidence transformed practice

Every extension of enforcement measures must be matched by stronger defence rights and effective remedies.

New enforcement tools require matching defence rights.

Videoconferencing and proportionality

EAW AFTER ARREST	A video hearing can test whether the warrant remains necessary or an alternative can replace it
CROSS-BORDER ATTENDANCE	Participation from the State of residence may avoid surrender, transfer or detention solely to secure attendance
TRIAL IN ABSENTIA	A secure link may preserve meaningful involvement when attendance would otherwise be lost
LEAST COERCIVE MEASURE	Video, an EIO or a European Supervision Order should be considered before arrest and physical transfer

Coercion reduction may justify video. Convenience alone cannot.

ECBA's benchmark for future EU rules

RIGHT TO REQUEST

Available in cross-border cases

PHYSICAL PRESENCE

Preserved for trial

EXPRESS CONSENT

Free, informed and stage-specific

LEGAL PRIVILEGE

Protected channel throughout

TECHNICAL PARITY

Comparable quality for the defence

EFFECTIVE REMEDY

Challenge the order and restore physical presence

A future EU instrument should be judged against these six requirements.

The Commission's ERPO proposal

WHAT THE PROPOSAL CREATES

- A mutual recognition order for participation from another Member State;
- Suspects, accused persons and victims with party status;
- One or more hearings, from investigation through appeal.

COM(2026) 313 final
23 June 2026 · 2026/0172(COD)
Legislative proposal, not yet binding law

CONDITIONS AND SAFEGUARDS

- Proportionate and appropriate in the individual case;
- Consent as the general rule;
- Lawyer in the issuing courtroom;
- Secure confidential communication, interpretation and effective remedies.

Exceptionally, an ERPO may be issued without consent in response to a serious threat to public security or health.
Children or vulnerable persons require specific safeguards.

The ERPO proposal is pending.

Conclusion

The ERPO debate should begin with the function of presence, not the convenience of the link

The Commission's proposal creates a mechanism. It remains under negotiation

ECBA provides an independent benchmark for defence rights

Consent, proportionality, effective participation and an effective remedy must underpin any final text

Digital justice must reduce coercion without diminishing presence.



Monica Szwarc

E-evidence procedures

Florence, 25 September 2026

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

Co-funded by the EU

Plan

1 **Overview of instruments concerning e-evidence**

2 **E-evidence Package (Reg. 2023/1543+Dir. 2023/1544)**

3 **European Investigation Order (Dir. 2014/41)**

4 **Challenges**

Overview

Convention on Cybercrime Council of Europe (2001) + Protocol No.2	• international cooperation tools; • Member States with third countries (68 coutries) • transborder access in limited cases only
European Investigation Order (Dir. 2014/41)	• between the Member States, (Irland and Denmark excluded - Convention on mutual assistance in criminal matters 2000) • objective – to obtain **any type of evidence** in cross-border criminal investigations • based on the cooperation **between two judicial authorities** in two Member States • **general procedural safeguards** under EIO Directive and national law
EU e-evidence package Regulation 2023/1543 Directive 2023/1544	• between the Member States (Irland – yes; Denmark – no – Convention on mutual assistance in criminal matters) • objective - to obtain **electronic evidence** in cross-border criminal investigations • based on the relations **between the investigative authority in one MS and service provider in another MS** • **detailed safeguards** tailored to digital evidence and for service providers

E-evidence package

1

Regulation 2023/1543 on European Production Orders and European Preservation Orders for electronic evidence in criminal matters

- directly and uniformely applied in the Member States from 18/08/2026;
- European Production Order and European Preservation Order cover **the data that already exist and are stored by a service provider; regardless of the location of the data**
- **in criminal proceedings** and **for the execution of a custodial sentence or a detention order of at least 4 months**, following criminal proceedings
- adressees of the obligations: service providers which offer services in the EU;

ATTENTION national provisions indispensable to establish:

- **penalties for not complying with obligations stemming for service providers from the regulation (art. 15) and**
- **effective remedies for any person whose data were requested according to the regulation (art. 18)**

E-evidence package

2

Directive 2023/1544 laying down harmonised rules on the designation of designated establishments and the appointment of legal representatives for the purpose of gathering electronic evidence in criminal proceedings

- requires implementation to national law until 18 February 2026, but only 11 Member States notified implementation (state of play on 24/09/2026)
- each Member State must ensure that service providers in the EU **designate or appoint at least one adressee** for the receipt of, compliance with and enforcement of decisions and orders issued by authorities of Member States;
- Each Member State must ensure that each service provider established or offering services in their territory notifies the **information about the establishment of legal representative**
- Each Member State must **introduce penalties for infringement** of national implementing measures (enforcement of obligations of service providers)
- directive is complementary to the Regulation, but **without proper implementation e-evidence system will not be effective**; each MS must know where to adress decisions and orders!

Definitions

European Production Order	enables judicial authorities in one Member State to directly compel a service provider in another Member State – via its designated contact point ("addressee") – to produce electronic evidence within 10 days or 8 hours in emergency cases
European Preservation Order	enables judicial authorities to request preservation of electronic evidence for 60 days to ensure it remains available for later access
service provider	any natural or legal person that provides one or more of the following categories of services: • electronic communications services • internet domain name and IP numbering services, such as IP address assignment, domain name registry, domain name registrar and domain name-related privacy and proxy services • other information society services that enable their users to communicate with each other; or make it possible to store or otherwise process data on behalf of the users to whom the service is provided, provided that the storage of data is a defining component of the service provided to the user
Offering services	„offering services" – important that the Regulation applies also to services providers who have „**substantial connection, based on the specific factual criteria**", to the Member State, either an **establishment** or there is **a significant numer of users** in one or more Member States or there is **targeting of activities towards** one or more Member States

Electronic evidence

Less intrusive e-evidence		More intrusive e-evidence	
Subscriber data Information about the identity of a subscriber or customer and type of service	**Data requested for the sole purpose of identifying the user:** IP adressess, relevant source ports and time stamp	**Traffic data:** Source and destination of a message, location of the device, date, time, duration, size route, format, the protocol, etc.	**Content data:** In digital format text, voice, video, images, sound (other than subscribers data or traffic data
Why it is important?			
European Production Order may be issued only by: • a judge, a court, an investigative judge or prosecutor; • any other investigative authority according to national law+ validation by a judge, a court, an investigative judge or prosecutor		**European Production Order may be issued only by:** • a judge, a court, an investigative judge • any other investigative authority (including a prosecutor) according to national law+ validation by a judge, a court, an investigative judge **!!! Only for serious crimes:** • Criminal offences punishable in the issuing State by a custodial sencence of a max at least three years • Other offences as explicitely mentioned	

Comparison

1

E-evidence package

- European Production Order may be issued when necessary to obtain data in possesion of a service provider in direct contact between investigating authority and a given service provider;
- does not apply to interception of telecommunication in real time
- approach to make access to e-evidence effective with less considerations for rights of individuals

2

European Investigation Order

when it is necessary to:
- carry out specific investigative measure to obtain evidence or
- to obtain evidence that is already in possession of authorities in executing Member State

- It is recognised that there are differences in national legal systems regarding standards of gathering evidence and admissibility of evidence

European Investigation Order

1

INTERCEPTION OF TELECOMMUNICATIONS art. 31

when interception of telecommunication by investigating authority in one MS **without technicat assistance of the MS where interception will take place:**

the intercepting Member State shall **notify the competent authority** of the notified Member State of the interception (…) prior to the interception in cases where the competent authority of the intercepting Member State knows at the time of ordering the interception that the subject of the interception is or will be on the territory of the notified Member State

2

C-670/22 M.N. (Encrochat)

- the concept of 'telecommunications' used in Article 31(1) is autonomous concept of EU law
- the infiltration of terminal devices for the purpose of gathering communication data, but also traffic or location data, from an internet-based communication service constitutes an 'interception of telecommunications
- must be notified to the authority designated for that purpose by the Member State
- is intended also to protect the rights of those users affected by a measure for the 'interception of telecommunications' within the meaning of that article;
- admissibility of evidence: in criminal proceedings against a person suspected of having committed criminal offences, national criminal courts are required to disregard information and **evidence if that person is not in a position to comment effectively** on that information and on that evidence and the said information and evidence are likely to have a preponderant influence on the findings of fact.

Challenges

1) For the Member States – establishment of the effective e-evidence package on national level; as long as Regulation and Directive are not fully implemented into national legal systems application of the package will be fragmented

2) For lawyers: identify the set of **applicable rules**, depending on the state and depending on the completeness of implementation of the e-evidence package

3) Depending on the data that is to be obtained: different deadlines ((several months; 120 days; 10 days/8 hours in urgent cases); different guarantees

4) make sure that **fundamental rights** are respected, in particular proportionality and judicial review; how to strike the **balance between the need of effective investigations and the right to privacy and protection of personal data**

5) What about the **admissibility of evidence** – where national rules may differ significantly – harmonisation on EU level possible?

Useful sources

Government websites in Member States informing about the e-evidence package

https://commission.europa.eu/document/download/3e44b87f-13bc-46da-9b91-3488b77068dd_en?filename=Government%20websites%20MS%20e-evidence%20package.pdf

E-EVIDENCE PACKAGE: STATE OF READINESS

https://commission.europa.eu/document/download/5b3c2ee0-4055-4694-82c3-dc265cd6f108_en?filename=Information%20on%20Member%20States%20ready%20to%20issue%20and%20or%20receive%20EPOCs%20and%20EPOCS-PR.pdf



George Dimitrov

Digitalisation of EU Criminal Law Instruments in Bulgaria

Florence, 25 September 2026

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

Co-funded by the EU

AGENDA

One hour, eight steps

1	Why Bulgaria is a useful case	4 min
2	The Union framework in outline	7 min
3	Bulgaria’s e-justice architecture	7 min
4	Instrument by instrument: EAW · EIO · freezing & confiscation · sentences · e-Evidence · videoconferencing	18 min
5	Fundamental rights and lawyers’ ethics	7 min
6	Assessment and roadmap to 2028	5 min
7	What this means for Italian lawyers working with Bulgaria	4 min
8	Conclusion and questions	8 min

Why Bulgaria is a useful case

External border, transit country

One of the Union’s longest external borders. A large share of criminal cases has a cross-border element; Italy is among the most frequent partners.

Digital courts, analogue pre-trial phase

Fully electronic court case files (ЕИСС, ЕПЕП) — yet prosecutors’ files and cross-border cooperation still travel by post, fax, e-mail and SIS.

Source of landmark CJEU case-law

Gavanozov I and II (EIO remedies), PI C-648/20 PPU (prosecutor-issued EAW). Digitalisation does not remove these questions — it accelerates them.

Three clocks now govern practice

1 May 2025

Digitalisation Regulation (EU) 2023/2844 applies

Common rules on e-communication, videoconferencing (Art. 6), e-signatures (Art. 7), legal effect of e-documents (Art. 8).

18 Aug 2026

e-Evidence Regulation (EU) 2023/1543 applies

European Production & Preservation Orders addressed directly to service providers. Directive 2023/1544 due 18 Feb 2026.

1 Mar 2028

Mandatory e-CODEX exchange: EAW · EIO · Reg. 2018/1805

Two years after Implementing Regulation (EU) 2026/101 (in force 5 Feb 2026). Remaining Annex II acts follow by 2031.

Five acts shape the digital cooperation space

Act	What it does	Timing
Regulation (EU) 2023/2844 — Digitalisation Regulation	Decentralised IT system for 11 criminal-law acts (Annex II); videoconference hearings; QES/QSeal; legal effect of e-documents	Applies 1 May 2025; Art. 3 per batch (2028–2031)
Directive (EU) 2023/2843	Inserts “means of communication” clauses (e.g. new Art. 8a FD 2002/584/JHA) and aligns rules on originals / certified copies	Transposition tied to implementing acts; BG not yet transposed
Regulation (EU) 2022/850 — e-CODEX	Legal basis for the secure exchange infrastructure; system handed over to eu-LISA; national access points; reference implementation	In force; backbone for all batches
Regulation (EU) 2023/1543 + Directive (EU) 2023/1544 — e-Evidence	European Production / Preservation Orders to service providers; designated establishments; 10 days / 8 hours; penalties up to 2 % turnover	Directive due 18 Feb 2026; Regulation applies 18 Aug 2026
Regulation (EU) 2024/3011 — Transfer of proceedings	First instrument designed for the decentralised system from the outset	Applies 1 Feb 2027

Regulation (EU) 2023/2844 — the articles lawyers must know

Art. 3 — Means of communication

Communication between competent authorities under the Annex II acts through a secure, decentralised IT system; limited exceptions (disruption, physical evidence, etc.).

Art. 6 — Hearings in criminal matters

Suspects, accused and convicted persons may be heard by videoconference only if the technology is available, the person consents and circumstances justify it; law of the hearing State applies; confidential lawyer contact.

Art. 7 — Electronic signatures and seals

Qualified electronic signatures / seals under eIDAS (Reg. 910/2014 as amended by 2024/1183) for communication through the system.

Art. 8 — Legal effects of electronic documents

No denial of legal effect or admissibility solely because a document is in electronic form.

Art. 10 & 26(3) — Implementing acts and phasing

Four batches of implementing acts (2026–2029); Art. 3 applies two years after each — 2028 to 2031.

Annex II phasing: when each criminal-law instrument goes digital

	Implementing act due	Instruments (Annex II)	Art. 3 mandatory from
Batch 1	17 Jan 2026 — adopted: IR (EU) 2026/101 (in force 5 Feb 2026)	European Arrest Warrant (FD 2002/584) · European Investigation Order (Dir. 2014/41) · Freezing & confiscation (Reg. 2018/1805)	**1 March 2028**
Batch 2	17 Jan 2027	Custodial sentences (FD 2008/909) · European Protection Order (Dir. 2011/99)	**≈ early 2029**
Batch 3	17 Jan 2028	Freezing (FD 2003/577) · Financial penalties (FD 2005/214) · Confiscation (FD 2006/783) · Conflicts of jurisdiction (FD 2009/948)	**≈ early 2030**
Batch 4	17 Jan 2029	Probation (FD 2008/947) · Supervision measures (FD 2009/829)	**≈ early 2031**

Dates for batches 2–4 assume timely adoption of the implementing acts (Art. 10(3)(b)–(d)); the mandatory date is the first day of the month following two years after entry into force (Art. 26(3)).

Legal foundation and systems

ЕИСС

Unified Information System of the Courts

Mandatory for all new cases since 2021; electronic case file; random allocation; e-signed court acts.

ЕПЕП

Unified E-Justice Portal (ecase.justice.bg)

Remote access for parties and lawyers; e-filing and e-service; login with qualified e-signature.

УИС

Prosecution's Unified Information System

Pre-trial file registry; investigators (МВР, НСлС) run separate systems; file remains largely paper.

eIDAS

Qualified trust services: signatures, seals, time stamps

Every magistrate holds a QES; mature national trust-services market; secure e-delivery via e-Government portal.

Judicial System Act, Chapter 18a (2016) — "Certifying statements and procedural actions in electronic form"

Electronic Document and Electronic Trust Services Act · Electronic Identification Act (2016) · eIDAS Reg. 910/2014 (as amended by 2024/1183) · Personal Data Protection Act, Ch. 8 (Dir. 2016/680)

Islands of digitalisation: where criminal proceedings actually stand

Court phase — electronic

- Every case registered and managed in ЕИСС; acts signed with QES
- Parties and defence counsel access the file through ЕПЕП
- Electronic filing and electronic service possible
- Videoconference rooms in courts and detention facilities
- Public registers fed automatically

Pre-trial & cross-border — analogue

- Prosecutors' and investigators' files predominantly on paper; e-copies for the court
- Defence access to the pre-trial file (Art. 227 CCP) is a physical exercise
- EAW, EIO, certificates sent by SIS alert, e-mail, fax or post
- No national back-end connected to e-CODEX for Annex II instruments (to the author's knowledge)
- No comprehensive digital criminal-file strategy (cf. Italy's Processo Penale Telematico)

4

Instrument by instrument

For each instrument, three questions: which Bulgarian act implements it · how it is transmitted today · what changes with digitalisation

- European Arrest Warrant
- European Investigation Order
- Freezing & confiscation
- Sentences · probation · supervision
- e-Evidence
- Videoconferencing

EAW — Extradition and European Arrest Warrant Act (3EE3A, 2005)

Today

- Issued by the prosecutor (pre-trial) or the court (trial)
- Executed by the district court (окръжен съд) of the place of arrest, prosecutor participating
- No central authority for EAW; Ministry of Justice only for extradition
- Transmission: SIS alert + form, Interpol, or direct by e-mail / fax / post; Bulgarian translation required

From 1 March 2028

- New Art. 8a FD 2002/584: all official communication via the decentralised IT system (Dir. 2023/2843)
- Form becomes structured data — digital procedural standard in IR 2026/101
- QES of prosecutor/judge + qualified seal of the authority
- SIS alert continues in parallel (own legal basis)
- Time-stamped, integrity-protected record of every exchange (Art. 15(2) requests)

Hearings — Art. 6

- Hearing of the requested person (Arts 18–19 FD) by videoconference only with consent, available technology and justifying circumstances
- Law of the hearing State governs; recording per national law; confidential lawyer contact
- BG: Art. 65(3) CCP already allows detained accused to appear by video with consent — 3EE3A needs an express rule

EIO — European Investigation Order Act (3E3P, SG 16/2018) and the Gavanozov lesson

2018 → 2021 → 2024

3E3P adopted

SG No 16 of 20 Feb 2018 (deadline was 22 May 2017). Prosecutor issues pre-trial, court at trial; Art. 24 Dir. → Art. 474 CCP (videoconference hearing).

Gavanozov II — C-852/19

Grand Chamber, 11 Nov 2021: Art. 14 Dir. 2014/41 + Art. 47 Charter preclude issuing an EIO for search, seizure or video-hearing where the issuing State offers no remedy. BG offered none → BG orders in principle not executable.

Remedy introduced

SG No 36 of 23 Apr 2024: challenge before the first-instance court within 14 days; decision in closed session within 7 days on lawfulness, necessity, proportionality; final; executing State informed if set aside.

Batch 1 → decentralised system mandatory 1 March 2028. Several Member States already exchange EIOs via the Commission's reference implementation (eEDES); Bulgaria's operational use is not publicly confirmed. A structured form with mandatory fields will expose the quality of orders that paper concealed.

Three legal layers, one digital channel from 2028

FD 2003/577/JHA Freezing property or evidence	BG Act of 2006 on recognition, execution and issuing of freezing orders	Batch 3 (≈ 2030)
FD 2005/214 · FD 2006/783 Financial penalties · confiscation orders	Single BG Act of 2010	Batch 3 (≈ 2030)
Reg. (EU) 2018/1805 Freezing & confiscation — directly applicable since 19 Dec 2020	Prosecutors and courts notified as competent authorities; digital standard in Annex VI IR 2026/101	Batch 1 — 1 March 2028

Civil forfeiture is outside Reg. 2018/1805

Unexplained-wealth forfeiture (КОНПИ, 2023 legislation) is a civil procedure — enforceable, if at all, under the Brussels regime.

Judicial act behind Bulgarian certificates

Pre-trial freezing under the CCP requires court authorisation — eases recognition in Italy.

Mutual recognition of sentences and alternatives to detention

Instrument	Subject	Bulgarian implementation	Digital channel
FD 2008/909/JHA	Custodial sentences / measures involving deprivation of liberty	BG Act of 2019; district courts; Ministry of Justice as central authority for practical assistance	Batch 2 (≈ 2029)
FD 2008/947/JHA	Probation measures and alternative sanctions	BG Act of 2012; district courts	Batch 4 (≈ 2031)
FD 2009/829/JHA	Supervision measures as alternative to provisional detention (ESO)	BG Act of 2012; district courts	Batch 4 (≈ 2031)



Art. 6 Reg. 2023/2844 expressly allows the sentenced / supervised person to be heard by videoconference in these proceedings — subject to consent. Bulgarian courts apply the Framework Decisions' consent and hearing rules strictly; relevant for Bulgarian citizens serving sentences in Italy and Italian citizens in Bulgaria.

Regulation (EU) 2023/1543 — a change of paradigm since 18 August 2026

European Production Order (EPOC) · European Preservation Order (EPOC-PR)

- Addressed directly to the provider's designated establishment / legal representative in another Member State
- Subscriber & identification data: any offence; prosecutor may issue
- Traffic & content data: ≥ 3 years' imprisonment or listed offences; judge issues/validates; enforcing State notified, may object within 10 days
- Compliance within 10 days — 8 hours in emergencies
- Penalties up to 2 % of worldwide turnover
- Own decentralised IT system (Art. 19, e-CODEX-based)

Person informed & remedies

Data subject informed once disclosure no longer jeopardises the case; effective remedies in the issuing State (Art. 18).

Defence asymmetry

Defence cannot issue orders; Art. 1(2) refers to national procedures — in BG, a request to the prosecutor or court under the CCP.

Legal professional privilege

Immunities and privileges in the enforcing State — including lawyers' professional secrecy — ground objection; provider may alert the authority.

Providers in scope

Telecoms, e-mail and messaging, cloud hosting, social networks, marketplaces — the executing State is replaced by the provider.

Bulgaria is lacking behind while the Regulation already applies



- 27 March 2026 — Commission letters of formal notice to 22 Member States, including Bulgaria, for failure to transpose Directive (EU) 2023/1544
- End of August 2026 (BNT, confirmed by Bulgaria's national member at Eurojust): no act designates the issuing authorities, the enforcing / notification authority, or the authority hearing providers' objections and imposing penalties
- Consequence: Bulgarian prosecutors cannot issue EPOCs through the system; Bulgarian providers face Italian or Spanish orders without a clear national interlocutor
- Until the act is adopted, the EIO remains the only route for Bulgarian authorities — 90–120 days instead of 10 days / 8 hours
- Expected: amendments to the CCP and a dedicated act; MEP Emil Radev hopes for adoption before end-2026

Proposed design (author's view): prosecutor = issuing authority for subscriber/identification data · court = traffic/content data and validation · one enforcing & notification authority in the Supreme Cassation Prosecutor's Office · judicial review of penalties on providers · remedy under Art. 18 with access to the electronic record of order and response.

Videoconferencing in the Bulgarian Code of Criminal Procedure (НПК)

Before 2020 — exceptions only

- Art. 474 — hearing of witnesses, experts or the accused by video/telephone conference at the request of a foreign judicial authority
- Art. 140 — minor witnesses
- Art. 141 — witnesses with protected identity

SG No 98/2020 — pandemic amendments

- Art. 65(3) — detained accused in detention review, with consent; identity certified by prison/arrest chief
- Art. 139(11) — protected witness
- Art. 143 — confrontation when the accused is abroad
- Conditional early release proceedings — with consent



Where: a room in a court, prison or detention facility

No participation from a lawyer's office or home; a court or prison official verifies identity. Definition from the Code of Civil Procedure: simultaneous image and sound, recordable.



Security of the link

Sofia District Court (2024): court-to-court connections through protected channels and codes, not commercial platforms — an instinct that should be codified.

Article 6 Reg. 2023/2844 sits above national rules in cross-border cases

Consent

The suspect, accused or convicted person must consent — no videoconference against the person's will.

Availability & justification

Technology must be available and the circumstances of the case must justify remote participation.

Law of the hearing State

The hearing is governed by the law of the Member State conducting it — for a Bulgarian court, the НПК.

Confidential lawyer contact

Confidential communication with the lawyer must be ensured before and during the hearing — BG law is silent on the lawyer's line.

Recording

Recording where national law requires; the recording becomes part of the electronic file — integrity must be verifiable.

To do in Bulgaria: amend НПК and ЗЕЕЗА to implement Art. 6 expressly — consent requirement, secure court-to-court connection, separate confidential lawyer channel.

5

Fundamental rights and lawyers' ethics

The Regulation digitalises the authorities. Whether it digitalises the defence is a matter of national law — and of the Bar's vigilance.

Five points for the defence in a digital cooperation space

Equality of arms	Authorities share a structured, time-stamped record; the defence sees it only if national law grants access. BG: court file yes (ЕПЕП), pre-trial file no (Art. 227 CCP). Proposal: electronic defence access to cooperation materials from the moment of charging.
Remedies	Gavanozov II: the issuing State must offer a remedy equivalent to a domestic case. Closed for the EIO in 2024; still to be written for e-Evidence (Art. 18 Reg. 2023/1543).
Authenticity & integrity of e-evidence	QES, qualified seals, time stamps, registered delivery (eIDAS as amended by 2024/1183). Proposal: every item transmitted via the system disclosed to the defence with hash value and validation report.
Data protection	Competent authorities: Dir. 2016/680 → Ch. 8 Personal Data Protection Act. Commission / eu-LISA: Reg. 2018/1725. Internal national use of the system widens the data perimeter.
Professional ethics	Bar Act + Code of Ethics: confidentiality and competence. Competence now includes QES, secure client channels, reading structured forms, spotting court-impersonation phishing. CCBE guidance as benchmark.

Bulgaria’s balance sheet, September 2026

In place

- Complete set of implementing acts for the Annex II instruments (ЗЕЕЗА 2005, ЗЕЗР 2018, Acts of 2006, 2010, 2012, 2019)
- Fully electronic court case file (ЕИСС) and portal access for lawyers (ЕПЕП)
- Mature eIDAS trust-services ecosystem; QES held by every magistrate
- EIO remedy meeting the Gavanozov II standard (SG 36/2024)
- Videoconference rooms in courts and detention facilities

Missing

- Directive (EU) 2023/1544 not transposed; no authorities designated under Reg. 2023/1543 — infringement pending
- No national back-end connected to e-CODEX for criminal instruments; no Art. 17 early-operation notification
- No digital pre-trial file; no electronic defence access to cooperation materials
- Videoconferencing confined to narrow hypotheses; Art. 6 not implemented
- Directive (EU) 2023/2843 not transposed

Five steps to 1 March 2028

End 2026

1

e-Evidence Act

Designate issuing, enforcing and notification authorities; judicial review of penalties; Art. 18 remedy.

2027

2

e-CODEX access point

Designate national access point; choose reference implementation vs national back-end; notify under Art. 17.

2027

3

Art. 6 in НПК & ЗЕЕЗА

Consent rule, secure court-to-court link, confidential lawyer channel for cross-border video hearings.

2028

4

Transpose Dir. 2023/2843

Align originals / certified-copy rules in each mutual-recognition act with Art. 8 Reg. 2023/2844.

Continuous

5

Digital pre-trial file

Electronic defence access to cross-border cooperation materials; training of magistrates and lawyers.

None of this is technically difficult; all of it is a matter of legislative attention.

Working with Bulgaria: a checklist for Italian colleagues

Your client faces a Bulgarian EAW

Ask for the underlying Bulgarian judicial act. Pre-trial EAWs are prosecutor-issued; PI (C-648/20 PPU) requires judicial review before surrender. Use Art. 15(2) requests on detention conditions and stage of proceedings.

An Italian EIO goes to Bulgaria

Executed by the prosecutor's office of the district where the measure is carried out, in Bulgarian. Substantive reasons of the Italian order are challenged in Italy; a Bulgarian order can be challenged in Bulgaria within 14 days.

Your client is a provider established in Bulgaria

Until the Bulgarian e-Evidence act is adopted there is no clear enforcing authority. Document every EPOC received and every response; invoke privilege grounds where relevant.

A video hearing of a person in Bulgaria is planned

Insist on consent, a secure court-to-court connection and a separate confidential lawyer channel — Art. 6 Reg. 2023/2844 is your legal basis.

Recommendations to the Bars

Joint training modules

Italian and Bulgarian Bars, with the ELF: Digitalisation Regulation, e-Evidence, structured EIO/EAW forms — this seminar is the model.

Qualified e-signatures for every lawyer

Access to national portals (ΕΠΕΠ) and to future defence channels depends on QES; Bars should facilitate issuance and use.

Secure lawyer–client channels

Standards for confidential communication with clients in detention and for video hearings; CCBE guidance as benchmark.

Advocacy for defence access

Press for electronic defence access to cross-border cooperation materials in national codes — the Regulation will not do it for us.

Cross-border referral networks

Rapid identification of counsel in the other State when an EAW, EIO or EPOC lands: CCBE Find-a-Lawyer, bilateral Bar contacts.

Monitoring implementation

Bars to follow national e-CODEX connection, Art. 6 implementation and e-Evidence designations; report gaps to the CCBE and the Commission.

Digitalisation is presented as an engineering project. For lawyers it is a rights project.

1 May 2025

Digitalisation Regulation applies

18 Aug 2026

e-Evidence Regulation applies

1 Mar 2028

e-CODEX mandatory: EAW · EIO · 2018/1805

The clocks measure not only how fast an order travels from Florence to Sofia, but how quickly a person in Sofia can learn of it, understand it and challenge it. Bulgaria built impressive digital courts and left cross-border criminal cooperation on paper; the next two years must close that gap — and the Bar must make sure the defence is not left on the analogue side of the line.

Thank you — Grazie — Благодаря

Prof. George Dimitrov, D.Sc. · Attorney-at-law, Sofia Bar Association

Principal sources

- Reg. (EU) 2023/2844 · Dir. (EU) 2023/2843 · Commission IR (EU) 2026/101 · Reg. (EU) 2022/850 (e-CODEX)
- Reg. (EU) 2023/1543 · Dir. (EU) 2023/1544 · Reg. (EU) 2018/1805 · Reg. (EU) 2024/3011 · Reg. (EU) No 910/2014 as amended by 2024/1183
- CJEU: C-852/19 Gavanozov II (11.11.2021) · C-324/17 Gavanozov I (24.10.2019) · C-648/20 PPU PI (10.3.2021)
- Bulgaria: НПК (Arts 65(3), 139(11), 140, 141, 143, 227, 474) · ЗЕЕЗА (SG 46/2005) · ЗЕЗР (SG 16/2018, am. SG 36/2024) · ЗСВ Ch. 18a (SG 62/2016) · ЗЕДЕУУ · ЗЕИ (SG 38/2016)
- European Commission, DigitalJustice@2030 (COM(2025) 802); formal notices of 27.3.2026 on Dir. 2023/1544; European e-Justice Portal, Member State notifications under Art. 17 Reg. 2023/2844
- Full bilingual text with references: “Digitalisation of EU Criminal Law Instruments in Bulgaria”, TRAVAR 2, Florence, 25.9.2026



Monika Szwarc

Use of videoconferencing in criminal matters in Poland

Florence, 25 September 2026

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

Co-funded by the EU

Plan

1 **European standards: ECtHR and CJEU**

2 **Videoconferencing in criminal proceedings – modest regulation and many doubts**

3 **Videoconferencing in criminal proceedings – ambitious plan for the future**

European standards on the use of videoconferencing in criminal matters

1

Art. 6 ECHR – European Court of Human Rights
Marcello Viola v. Italy (45106/04)

- a defendant's participation in proceedings by videoconference is not as such contrary to the Convention;
- nevertheless, recourse to this measure in any given case must serve a legitimate aim; and
- the arrangements for the giving of evidence must be compatible with the requirements of respect for due process, as laid down in Article 6 of the Convention.

For more guidance see

https://ks.echr.coe.int/documents/d/echr-ks/hearings-via-video-link

European standards on the use of videoconferencing in criminal matters

2

European Union Law

- **art. 24 of the directive 2014/41 European Investigation Order** + case law: C-255/23 AVVA; C-325/24 Bissili; C-499/25 Strinotto (pending)

- **art. 6 Reg. 2023/2844** – videoconferencing in crossborder criminal proceedings under selected EU instruments

- a competent authority in one Member State may request the hearing of a suspect, accused person, convicted person, or another affected person located in another Member State by videoconference or similar technology;

- such a hearing is permitted only where:

the circumstances of the case justify the use of remote technology; and
the person concerned has freely and unequivocally consented to participate remotely

! specific conditions and fair trial guarantees

Videoconferencing in Poland– present regulation

Witness/expert witness	1) **general possibility to hear witnesses and experts** in criminal proceedings during videoconference; when a witness cannot be present in person for reasons of illness, disability of other insurmontable obstacle; no other precise conditions when it is possible/obligatory; decision of the court on request of a witness or the parties **2) pre-trial proceedings** – when a public prosecutor is involved then - the witness at his/her location must be accompanied by state official (a trainee prosecutor, a prosecutorial assistant or a public prosecution service clerk) **3) court hearings** - the witness at his/her location must be accompanied by state official (a trainee judge, a judicial clerk, a judicial assistant or a clerk employed by the court in whose jurisdiction the witness is located) **4) when in prison or in a pre-trial detention** – a witness may be heard in the presence of a representative of the prison or centre's administration **5) a witness is a Polish national residing abroad** - in the presence of a consular official

Videoconferencing in Poland – present regulation

Defendant in court hearings	1) **the general right to be present at the trial**; obligation to be present - in case of serious crimes; 2) **public prosecutor may ask** for enabling his/her participation in the trial during videoconference; it is assumed that the court is obligated to organise videoconference, unless there are technical obstacles 3) **when defendant is in detention** – he/her may participate in the trial during videoconference (buy only when obligation to participate); he/her must be assisted by representative of the administration of prison or pre-trial detention centre; 4) **defence counsel may decide** to appear either at the defendant's location or in the court room; 5) when defence counsel is not with the defendant, **the court may allow a pause** (on the request of the counsel of the defendant) to enable them the contact; 6) if the **interpreter is necessary during** the trial he shall participate in the defendant's location

Summary

1) no possibility to have the trial online;
2) „videoconference" in PL means „remote participation in the court hearing";
3) 4 different situations and only before the court (the court proceedings)

- remote participation of the defendant or civil party, when he/she is detained (prison or pre-trial detention);
- remote participation of the public prosecutor;
- remote participation of the defendant who is not detained and is heard for the first time by the court;
- remote participation of a witness/expert witness

4) **!!! No specific rules for suspects** (the pre-trial proceedings)

Main concerns - today

1) How to ensure **right of defence and confidential contact between defence counsel and defendant** who is in detention (decision of the judge – 15 minutes break – telephone contact);
2) Remote participation in the court proceedings not possible for defendant or civil party who is not detained (only the first hearing before the court);
3) Discrimination of the parties in the proceedings – only a public prosecutor may request for remote participation in the hearing, the court is obligated to grant such access unless technical dificulties;
4) Problem with the remote participation of the defendant who is in detention: presence in the court is the right and not obligatotion; when there is no obligation to be present – no right to request for remote participation;
5) A witness/expert witness is usually heard remotely from the court building of their location; even if there is no problem with remote participation from other places (for example work/office/hospital) with the presence of the court's representative;
6) what about remote participation of a suspect in the pre-trial proceedings? At the moment – direct application of Art. 6 of Regulation 2023/2844

Videoconferencing in Poland - ambitious plan

Witness/expert	**1) differentiation of rules depending on the stage of proceedings** • during the pre-trial (investigative) stage, the remote examination of a witness would be permissible without restrictions; • during court proceedings, remote examination would be allowed only where there are important reasons justifying its use or where none of the parties objects; 2) the proposal assumes that **a witness's personal appearance in the court should remain the general rule** 3) **remote examination is intended to remain an exception**, as it may limit the direct interaction of the court and the parties with the source of evidence and possible when: • difficult-to-overcome obstacles preventing the witness from appearing in person; • a **risk of unlawful influence being exerted on the witness;** **4) assistance during the examination of a witness** • as a general rule, a person authorised by the procedural authority should be present at the witness's location; • **in exceptional circumstances, a witness may give evidence from their place of residence without such assistance**; • a witness staying abroad - both with the involvement of the authorities of a foreign state and without the use of formal mutual legal assistance, provided that the witness voluntarily agrees to testify and the state of residence does not object to this method

Videoconferencing in Poland - ambitious plan

Witness/expert

1) Dedicated protection of child witnesses and those requiring assistance of an expert

- the representative of the authority always required;
- to reduce the risk of third-party influence

2) Expert witnesses:

- a medical expert or psychologist assisting during the examination of a witness should be present at the same location as the witness;
- the examination of an expert witness may itself be conducted remotely from the expert's place of residence or work and, as a rule, without the need for additional supervision or assistance

3) Interpreter:

- the interpreter present at the location of the person being examined,
- remote participation of the interpreter permissible, provided that it does not jeopardise the proper exercise of the parties' procedural rights, particularly the right of defence;

4) Procedural guarantees:

- remote examination only if the party concerned by the procedural act does not object;
- in each case, the court will decide whether the remote format could undermine the right of defence or hinder the proper taking of evidence, for example where numerous documents must be presented or where the defendant has particular health-related limitations.

Videoconferencing in Poland – ambitious plan

Parties in court hearings	1) **each party of the proceedings may request remote participation** (not only public prosecutor; 7 days from the notification of the hearing date) 2) **final decision on remote participation remains in the court's hands**; a court may refuse when: • technical obstacles exist; • remote participation would hinder the proper conduct of the proceedings; • the rights of the parties could be adversely affected; • the nature of the evidence to be taken requires the participants' physical presence in court. 3) **Mandatory remote participation for** a person deprived of liberty when there is situation of serious threat to public safety or public health (even against the wishes of such a person, with due account of the fairness of the proceedings) 4) **additional conditions**: • a party or their representative participating remotely should be accompanied by a court official; • the presiding judge may exempt a participant from the requirement that a court official be present, when no doubt as to the participant's identity and where the location from which they participate is considered appropriate; • location shall be suitable: compatible with the dignity of the court (no connection from public transport, a motor vehicle, a workplace where access by third parties cannot be prevented, public places).

Videoconferencing in Poland – ambitious plan

Detained persons in court hearings	**1) detained persons** (defendants and witnesses; in prison or in remand facility) • possibility to participate in court hearings remotely from the correctional facility where they are held; • always under supervision of the official from the prison or the remand facility; • the court should assess in each case whether the presence of prison staff or other officials may have an intimidating or inhibiting effect on the participant **2) defence counsel:** • may participate: from the courtroom; from the location where the defendant is present; or from another location, such as their law office; • where legal representation is mandatory, defence counsel must be present either: in the courtroom; or at the location of the defendant **3) confidential communication defence counsel and defendant** - when a detained defendant participates remotely and the defence counsel is in a different location, direct and confidential communication between them must be guaranteed

Videoconferencing in Poland – ambitious plan

Videoconferencing in pre-trial proceedings	**1) Use of videoconferencing for**: • the questioning of a suspect; • the presentation of criminal charges; • the amendment or supplementation of previously presented charges. **2) Prohibition of the use of videoconferencing**: • technical limitations prevent the proper conduct of the interview; • the interests of the proper administration of justice require the suspect's physical presence; or the use of videoconferencing could adversely affect the procedural rights of the parties **3) Questioning a suspect**: • decision of the public prosecutor; • in general with the suspect's prior consent; • exception: a suspect is deprived of liberty and in a situation of serious threat to public security or public health (without consent but with due account of the fairness of proceedings); • In general without the representative of the procedural authority; • exception: such presence of the representative is required where: there is a risk that the suspect may be subjected to undue influence; concerns arise regarding the suspect's ability to provide statements freely and voluntarily; or doubts exist as to the establishment of the suspect's identity.

Main concerns for the future

1) How to ensure **right of defence and confidential contact between defence counsel and defendant** who is in detention (decision of the judge – 15 minutes break – telephone contact);
2) ~~Remote participation in the court proceedings not possible for defendant or civil party who is not detained (only the first hearing before the court);~~
3) ~~Discrimination of the parties in the proceedings – only a public prosecutor may request for remote participation in the hearing, the court is obligated to grant such access unless technical dificulties;~~
4) ~~Problem with the remote participation of the defendant who is in detention: presence in the court is the right and not obligatotion; when there is no obligation to be present – no right to request for remote participation;~~
5) A witness/expert witness is usually heard remotely from the court building of their location; even if there is no problem with remote participation from other places (for example work/office/hospital) with the presence of the court's representative;
6) what about remote participation of a suspect in the pre-trial proceedings? At the moment – direct application of Art. 6 of Regulation 2023/2844
7) How to verify the identity of a witness in the time of AI?