326DT003
Seminar #Digitalisation and #AI in Criminal Justice

Table of Contents:

#DIGITALISATION and #AI in Criminal Justice

Tech&Law, OSINT, AI and machine learning

Zagreb, 15-16 June 2026

FACE-TO-FACE

EXCELLENCE IN EUROPEAN LAW

Speakers and chairs

Sandor Bosch, Court of Appeal Den Bosch, The Netherlands

Laviero Buono, Head of Section for European Criminal Law, ERA, Trier

Rainer Franosch, Prosecutor, Deputy Director-General for Criminal Law and Criminal Procedure, Head of Cybercrime Division, Ministry of Justice, German Federal State of Hesse, Wiesbaden

Muthupandi Ganesan, Barrister at Law & Partner, Aliant Law, London

Rūta Jašinskienė, Intelligence Analysis Expert, NRD Cyber Security, Vilnius

Julija Kalpokienė, Lawyer, Rickert.Law, Bonn

Sabina Klaneček, Councel, Supreme State Prosecutor's Office, Ljubljana

David Silva Ramalho, Defence Lawyer, Morais Leitão, Galvão Teles, Soares da Silva & Associados; Lecturer, Faculty of Law, University of Lisbon

Michael Rothärmel, Head of Unit, Fight against Terrorism and Extremism, Ministry of Justice, Munich

Leonarda Stanarević, AI Consultant for Digital Forensics, INsig2, Zagreb

Key topics

- Technical issues (internet caches, proxy servers, encryption, deep/dark web, etc.)
- Legal issues (evaluation of the search results, reliability and credibility of authentication, search across jurisdictions)
- Presenting internet searches in court
- Videoconferencing
- Artificial intelligence (AI)

Language
English

Event number
326DT003

Organisers
ERA (Laviero Buono) in cooperation with the Croatian Judicial Academy

Judicial Academy

Co-funded by
the European Union

european.law

#DIGITALISATION and #AI in Criminal Justice

Monday, 15 June 2026

09:00 Arrival and registration of participants

09:30 **Welcome and introduction to the programme**
NN & Laviero Buono

I. PART I: TECHNICAL ISSUES AND BASIC UNDERSTANDING OF THE INTERNET ACHITECTURE AND CONCEPTS

Chair: Laviero Buono

09:35 **Digital evidence: Open-Source Intelligence (OSINT)**
- Introduction and the role of OSINT
- Efficient dialogue with search engines
- How OSINT is used by hackers
- Use case scenarios

Rūta Jašinskienė

10:45 Discussion

11:00 Break

11:30 **How Retrieval-Augmented Generation (RAG) can be applied in legal practice**
- RAG in legal practice
- AI connected to internal documents
- Knowledge retrieval and contract review
- Source-based answers and reduced hallucinations
- Privacy, confidentiality, ethics

Leonarda Stanarević

12:15 Discussion

12:30 Lunch

II. PART II: LEGAL ISSUES RELATED TO THE COLLECTION AND THE PRESENTATION OF E-EVIDENCE IN COURT

Chair: Rūta Jašinskienė

13:30 **Evolving definition of crimes:**
- How AI transforms criminal proceedings // Cyber crimes 2.0
- Pretty-Good-Privacy phones: developments in the admissibility of data

Sandor Bosch

14:15 Discussion

14:30 Break

15:00 **Artificial intelligence and handling electronic evidence in courts**
- AI impact on investigations
- Trial considerations: methods of presentation and admissibility tests
- Criminals' new *modus operandi*
- Case studies

Rainer Franosch

15:45 **Is mandatory disclosure of digital access fair? Evaluating e-evidence, pins and passwords**
Muthupandi Ganesan

16:30 Discussion

16:45 End of the first day

19:30 Dinner offered by the organisers

Objective

This seminar addresses various challenges linked to digitalisation that judges, prosecutors and lawyers in private practice working in the field of EU Criminal Justice will have to face for the years ahead. Some of these challenges such as the exchange of electronic evidence, videoconferencing, use of open-source intelligence, artificial intelligence, digital technology, etc. are there to stay and will become the 'new normal'.

This event is part of a large-scale project sponsored by the European Commission entitled 'Judicial training to prepare criminal justice professionals to #digitalisation and #artificialintelligence'. It consists of 12 seminars to take place in various EU cities over the period 2024-2027.

Who should attend?

Judges, prosecutors, court staff and lawyers in private practice, who are citizens of eligible EU Member States participating in the EU Justice Programme (Denmark does not participate), Albania, Bosnia and Herzegovina, Kosovo*, Moldova and Ukraine.

* This designation is without prejudice to positions on status and is in line with UNSCR 1244/1999 and the ICJ opinion on the Kosovo declaration of independence.

Venue

Hotel Academia
Ul. Ivana Tkalčića 88
10000 Zagreb

CPD

ERA's programmes meet the standard requirements for recognition as Continuing Professional Development (CPD). Participation in the full programme of this event corresponds to **9 CPD hours**.
A certificate of participation for CPD purposes with indication of the number of training hours completed will be issued on request. CPD certificates must be requested at the latest 14 days after the event.

Tuesday, 16 June 2026

III. PART III: VIDEOCONFERENCING, DATA RETENTION AND ARTIFICIAL INTELLIGENCE IN CRIMINAL JUSTICE

Chair: David Silva Ramalho

09:30 **Presenting evidence in court: e-files, videoconferences and remote trials**
- Remote trials during and after the pandemic
- E-files
- Witness videoconferences
- Vulnerable victims

Sabina Klaneček

10:00 Discussion

10:15 **Data retention – data protection vs. the risk of systemic impunity**
- Significance of data retention for the investigation and prosecution of crimes committed online and offline
- Case law of the CJEU
- State of play of legislation on EU and national level

Michael Rothärmel

10:45 Discussion

11:00 Break

Chair: Sandor Bosch

11:30 **Technical insights for the preparation, identification and preservation phase**
- The importance of the chain of custody in handling electronic evidence
- Case studies

David Silva Ramalho

12:00 Discussion

12:15 **From Identity to Content to Evidence: Is Our (Mis)Trust Misplaced in the Age of Deepfakes and Agentic AI?**
- From “seeing in believing” to synthetic reality
- Deepfakes and generative AI: the state of the art
- Automation and agentic AI: scaling deception and crime
- Implications for digital crime and criminal justice
- Rethinking the evaluation of evidence

Julija Kalpokienė

12:45 Discussion

13:00 End of the seminar and light lunch

For programme updates: **www.era.int.**
Programme may be subject to amendment.

Your contacts

Laviero Buono
Head of Section
European Criminal Law

Julia Reitz
Event Coordinator
Tel.: +49(0)651 9 37 37 323
E-Mail: jreitz@era.int

Apply online for “#Digitalisation and #AI in Criminal Justice”: **www.era.int/event/digitalisation-and-ai-in-criminal-justice-3**

This programme has been co-funded by the European Union

Application

#DIGITALISATION and #AI in Criminal Justice

Zagreb, 15-16 June 2026 / Event number: 326DT003

Terms and conditions of participation

Selection

1. Participation is only open to judges, prosecutors, court staff and lawyers in private practice from eligible EU Member States participating in the EU Justice Programme (Denmark does not participate) including Albania, Bosnia and Herzegovina, Moldova, Ukraine and Kosovo* *(this designation is without prejudice to positions on status and is in line with UNSCR 1244/1999 and the ICJ opinion on the Kosovo declaration of independence).* The number of places available is limited (30 places). Participation will be subject to a selection procedure.
2. Applications should be submitted before **16 February 2026**.
3. A response will be sent to every applicant after this deadline. **We advise you not to book any travel before you receive our confirmation**.

Registration Fee

4. €135 including documentation, coffee breaks, lunches and dinner.

Travel and Accommodation Expenses

5. Participants will receive a fixed contribution towards their travel expenses and are asked to book their own travel. The condition for payment of this contribution is to sign all attendance sheets at the event. Participants are required to provide supporting documentation demonstrating that the travel has taken place. The amount of the contribution will be determined by the EU unit cost calculation guidelines, which are based on the distance from the participant's place of work to the seminar location and will not take account of the participant's actual travel costs.
6. Travel costs from outside Croatia: participants can calculate the contribution to which they will be entitled on the European Commission website (https://era-comm.eu/go/calculator). The distance should be calculated from their place of work to the seminar location.
7. For inter-Member States return journeys between 50 and 400 km (Austria €58, Bulgaria €36, Czech Republic €36, Germany €65, Hungary €36, Italy €50, Romania €36, Slovenia €37). Please note that no contribution will be paid for travel under 50km. For more information, please consult https://era-comm.eu/go/unit-cost-decision-travel (COM Decision C(2021)35).
8. For those travelling within Croatia the contribution for travel for a distance between 50km and 400km is fixed at €36. Please note that no contribution will be paid for travel under 50km. For more information, please consult https://era-comm.eu/go/unit-cost-decision-travel (COM Decision C(2021)35).
9. Accommodation costs: International participants travelling more than 50km one-way will receive a fixed contribution of €208. National participants will receive an overall fixed contribution of €104. For more information, please consult https://era-comm.eu/go/unit-cost-decision-travel (COM Decision C(2021)35).
10. Successful applicants will be sent the relevant claim form and information on how to obtain payment of the contribution to their expenses. Please note that no payment is possible if the registered participant cancels their participation for any reason.

Participation

11. Participation at the whole seminar is required and participants' presence will be recorded.
12. A list of participants including each participant's address will be made available to all participants unless ERA receives written objection from the participant no later than one week prior to the beginning of the event.
13. The participant will be asked to give permission for their address and other relevant information to be stored in ERA's database in order to provide information about future ERA events.

Accommodation

1. ERA neither provides nor endorses any accommodation options for this event. Kindly consult your preferred accommodation provider for options.

Apply online for "#Digitalisation and #AI in Criminal Justice":
www.era.int/event/digitalisation-and-ai-in-criminal-justice-3

Venue

Hotel Academia
Ul. Ivana Tkalčića 88
10000 Zagreb

Language

English

Contact

Julia Reitz
Event Coordinator
Tel.: +49(0)651 9 37 37 323
E-Mail: jreitz@era.int

ERA -- European Academy of Law | Croatian Judicial Academy

Co-funded by the European Union.
Views and opinions expressed are however those of ERA only and do not necessarily reflect those of the European Union or European Commission.
Neither the European Union nor the granting authority can be held responsible for them.

Digital evidence: Open-Source Intelligence (OSINT)

#Digitalisation and #AI in Criminal Justice - Zagreb, 15 June 2026

Session Overview

01

The OSINT Landscape

Definition, sources, legal tensions

02

Efficient Search Techniques

Engines, operators, specialist tools, advanced tips

03

OSINT - Enabler of Crimes

How criminals weaponise OSINT

04

Case Study

financial fraud

05

Take Away

The five questions every legal professional must ask

PART I

The OSINT Landscape

What it is, where it comes from, and why criminal justice professionals must understand it

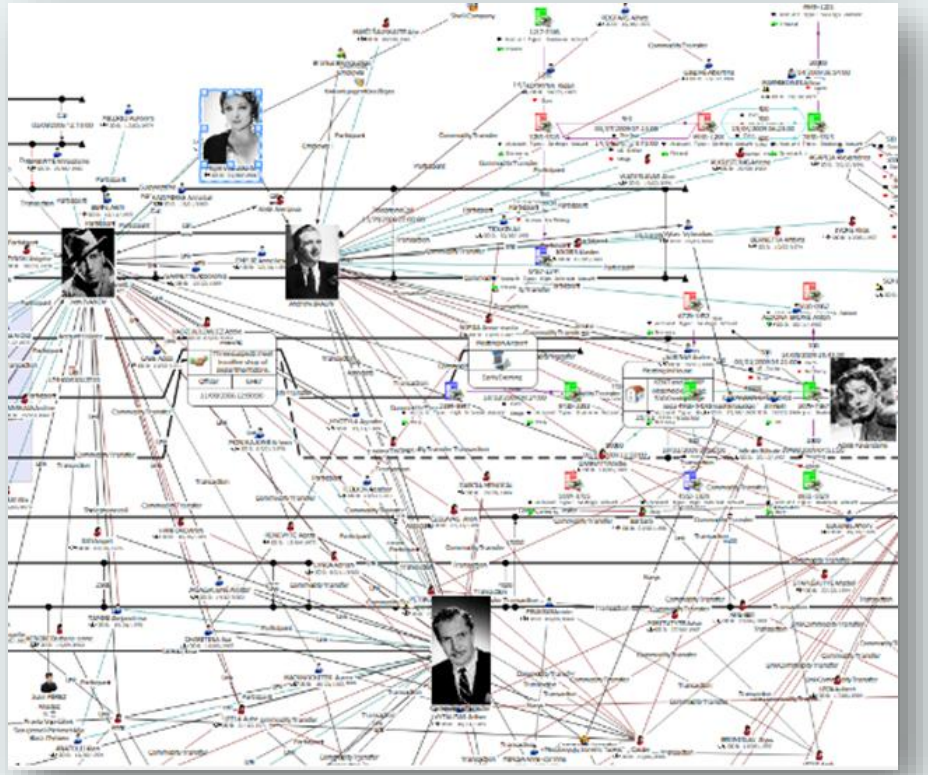
Intelligence

- The process by which specific types of data and information important to investigation are collected, analysed, and provided for decision making.

Don't jump to conclusions – take the right steps!

Open-source Intelligence (OSINT)

- Intelligence derived from publicly available sources of information



What is OSINT and what not?

- NOT limited to web-based information
- NOT surveillance
- NOT a technical discipline
- NOT hacking
- NOT static
- IS legally complex

OSINT Benefits

Why OSINT does NOT a Silver Bullet?

- Overwhelming
- Reliability
- Validity
- Inadequate training and investment
- Legal and ethical boundaries
- Attribution uncertainty
- Adversarial manipulation

The OSINT Source Universe

Geospatial Data

Leaked Databases

Social Media - SOCMINT

Web & Archives

Public Registries

Traditional Media

PART II

Efficient Search Techniques

Search engines, specialist tools, advanced operators and professional OSINT tradecraft

Search Engines-How it Works?

Search Engine Market Share — 2023 -2026

Engine	2023	2025	2026	Change 2023→2026	Bar chart comparison
Google	92.57%	91.43%	90.04%	▼ -2.53 pp	Scale: 0–100%
Bing	3.04%	3.30%	4.31%	▲ +1.27 pp	Scale: 0–5%
Yandex	1.00%	1.49%	1.45%	▲ +0.45 pp	Scale: 0–5%
Yahoo!	1.24%	1.33%	1.86%	▲ +0.62 pp	Scale: 0–5%
Baidu	0.72%	0.91%	0.89%	▲ +0.17 pp	Scale: 0–5%
DuckDuckGo	0.58%	0.70%	0.72%	▲ +0.14 pp	Scale: 0–5%

Sources: StaCounter / WebpageFX (2023, 2025, 2026) |

Standard Search Engines Reach Only the Visible Tip

Surface web

Google, Bing, Yahoo, Yandex, Wikipedia, Reddit, news sites
Indexed by standard search engines

5%

Search engine limit

95%

Deep web

Cloud storage, patent data, research articles, legal docs, financial records, private DBs
Requires credentials or special tools

Dark web

Onion sites, hidden markets, anonymous forums

OSINT reach

Google + Bing + Yandex all index this layer differently — cross-reference for full coverage

OSINT reach

Shodan, Maltego, Wayback Machine, public registries, OpenCorporates, ExifTool

OSINT reach

Ahmia.fi, IntelX — passive monitoring. Legal caution required.

Why Google Alone Is Not Enough

Engine	Best for	Watch out for
Google	People, news, general web, image search	*Filter bubbles; personalises results; hides some content*
Bing	Different index; better video search than Google	*Microsoft ecosystem bias; smaller index*
DuckDuckGo	No personalisation; unfiltered results view	*Smaller index; limited advanced operators*
Yandex	Russian-language content; best reverse image search	*Russian-centric; state filtering of some results*
Baidu	Chinese-language OSINT — no substitute exists	*Heavy state filtering; Chinese-centric index*
Startpage	Google results without tracking or personalisation	*Purely a privacy proxy; same index as Google*

Each search engine has a different index, different strengths — and different blind spots

2lingual

lithuanian drug trafficker - 2ling

2lingual.com/2lingual-google-search?qt=1&q=lithuanian+drug+trafficker&btn=2lingual+Google+Search&lr1=lan...

2lingual

lithuanian drug trafficker

2lingual Google Search

Search pages written in: English and Norwegian

powered by Google

English results for **lithuanian drug trafficker**

24 members of international **drug trafficking** group arrested - Eurojust

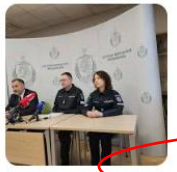
www.eurojust.europa.eu

10 Feb 2026 ... An organised crime group suspected of **trafficking drugs** to Iceland from across Europe and South America has been dismantled by **Lithuanian**, ...

Thirty-three to stand trial over human, **drug trafficking** spanning ...

www.lrt.lt

5 Feb 2026 ... Thirty-three **Lithuanian** nationals will stand trial on charges related to a large-scale criminal organisation accused of human **trafficking**, ...



Spanish police dismantle **Lithuanian drug** transporting network

www.euronews.com

27 Feb 2026 ... Spanish police have dismantled a **Lithuanian drug trafficking** organisation that used lorries loaded with building materials to smuggle ...

Norwegian results for **litauisk narkotikasmugler** - [Translated **lithuanian drug trafficker** from English to Norwegian] - Turn off automatic query translation

Did you mean: litauisk ***narkotikas mugler***

Byggevarehus i Moss: Litauere dømt for **narkotikasmugling** - NRK

www.nrk.no

29 May 2024 ... Da kom en 25 år gammel **litauisk** mann for å sjekke om stedet egnet seg for lagring av tørrvarer. Osloveien 366. Kameraer på utsiden av ...

(+) Fulgte etter hasj-vogntog fra **Litauen** med drone

www.at.no

4 Jul 2025 ... Oppdag hvordan politiet i Norge brukte en drone for å avsløre en stor **narkotikasmugling** fra **Litauen**. Les om den dramatiske jakten og ...

Fant 400 kilo hasj i lastebilgulv: – Første gang - VG

www.vg.no

Dramatisk Narkotikasmugling

at.no/transport/fulgte-etter-hasj-vogntog-fra-litauen-med-drone/1101268

AT.no Anlegg Transport Bygg Nytt om navn Hva skjer?

Norwegian English

Google Translate

HASJ I GRØFTA: Pakker med hasj slik de lå bak hengeren da politiet kom til stedet. Bildet er hentet fra dommen ved Follo og Nordre Østfold tingrett. Politiet

Fulgte etter hasj-vogntog fra Litauen med drone

MILLIONFUNN: Ulovlig last forsøkt smuglet over grensa ved Ørje.

Fredrik Saugstad

at.no/transport/fulgte-etter-hasj-vogntog-fra-litauen-med-drone/1101268

AT.no Facilities Transportation Barley News about What's going on? Position available Log in Subscribe

HASHIN IN THE DITCH: Packages of hashish as they lay behind the trailer when the police arrived at the scene. The image is taken from the judgment at Follo and Nordre Østfold District Court. Police

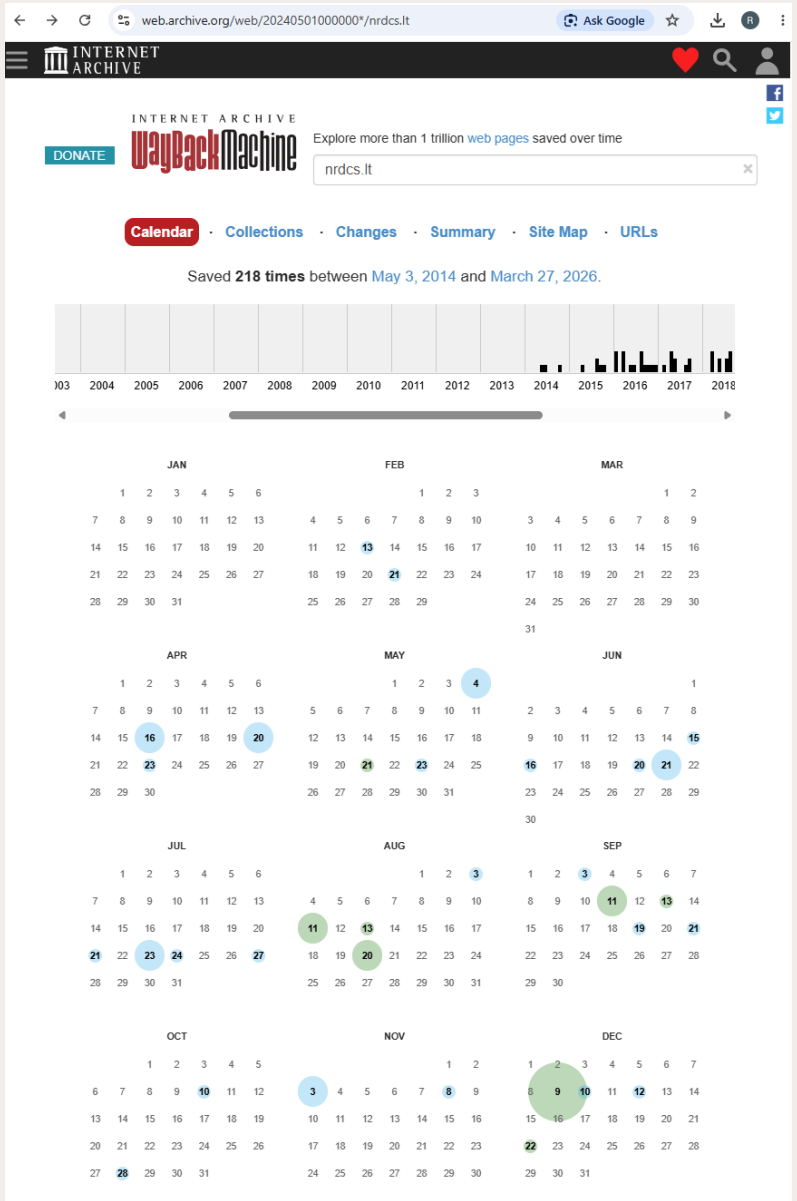
Followed hashish truck from Lithuania with drone

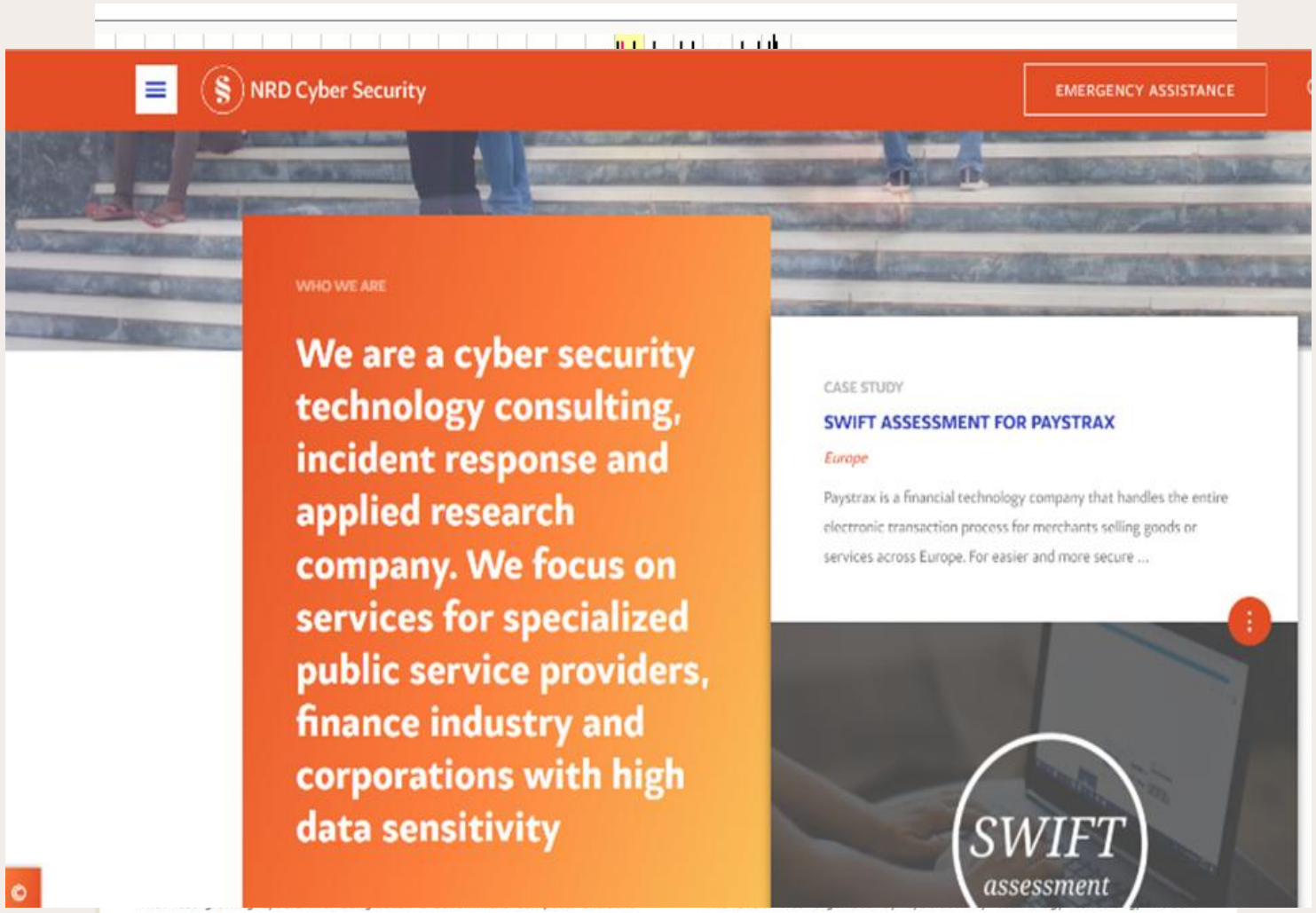
MILLION FINDING: Illegal cargo attempted to be smuggled across the border at Ørje.

Fredrik Saugstad

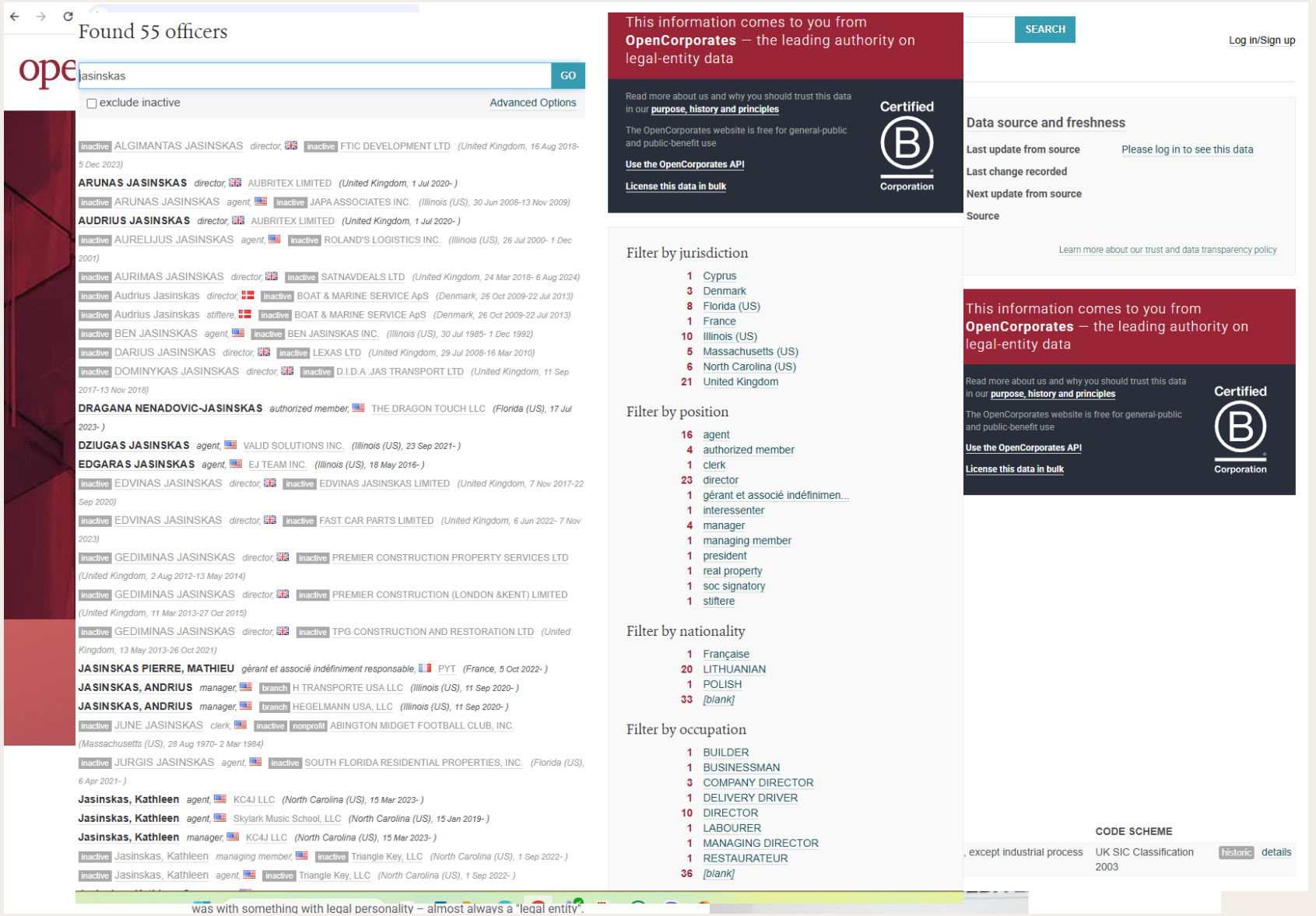
PUBLISHED 04.07.2025 - 13:00

Archive.org


web.archive.org/web/20240501000000*/nrdcs.lt
Ask Google
INTERNET ARCHIVE
INTERNET ARCHIVE
DONATE
WaybackMachine
Explore more than 1 trillion web pages saved over time
nrdcs.lt
Calendar · Collections · Changes · Summary · Site Map · URLs
Saved 218 times between May 3, 2014 and March 27, 2026.
2003 2004 2005 2006 2007 2008 2009 2010 2011 2012 2013 2014 2015 2016 2017 2018
JAN
FEB
MAR
APR
MAY
JUN
JUL
AUG
SEP
OCT
NOV
DEC


NRD Cyber Security
EMERGENCY ASSISTANCE
WHO WE ARE
We are a cyber security technology consulting, incident response and applied research company. We focus on services for specialized public service providers, finance industry and corporations with high data sensitivity
CASE STUDY
SWIFT ASSESSMENT FOR PAYSTRAX
Europe
Paystrax is a financial technology company that handles the entire electronic transaction process for merchants selling goods or services across Europe. For easier and more secure ...
SWIFT
assessment

opencorporates.com



Found 55 officers

jasinskas GO

exclude inactive Advanced Options

inactive ALGIMANTAS JASINSKAS director, inactive FTIC DEVELOPMENT LTD (United Kingdom, 16 Aug 2018- 5 Dec 2023)

ARUNAS JASINSKAS director, AUBRITEX LIMITED (United Kingdom, 1 Jul 2020-)

inactive ARUNAS JASINSKAS agent, inactive JAPA ASSOCIATES INC. (Illinois (US), 30 Jun 2008-13 Nov 2009)

AUDRIUS JASINSKAS director, AUBRITEX LIMITED (United Kingdom, 1 Jul 2020-)

inactive AURELIJUS JASINSKAS agent, inactive ROLAND'S LOGISTICS INC. (Illinois (US), 26 Jul 2000- 1 Dec 2001)

inactive AURIMAS JASINSKAS director, inactive SATNAVDEALS LTD (United Kingdom, 24 Mar 2018- 6 Aug 2024)

inactive Audrius Jasinskas director, inactive BOAT & MARINE SERVICE ApS (Denmark, 26 Oct 2009-22 Jul 2013)

inactive Audrius Jasinskas stiftere, inactive BOAT & MARINE SERVICE ApS (Denmark, 26 Oct 2009-22 Jul 2013)

inactive BEN JASINSKAS agent, inactive BEN JASINSKAS INC. (Illinois (US), 30 Jul 1985- 1 Dec 1992)

inactive DARIUS JASINSKAS director, inactive LEXAS LTD (United Kingdom, 29 Jul 2008-16 Mar 2010)

inactive DOMINYKAS JASINSKAS director, inactive D.I.D.A .JAS TRANSPORT LTD (United Kingdom, 11 Sep 2017-13 Nov 2018)

DRAGANA NENADOVIC-JASINSKAS authorized member, THE DRAGON TOUCH LLC (Florida (US), 17 Jul 2023-)

DZIUGAS JASINSKAS agent, VALID SOLUTIONS INC. (Illinois (US), 23 Sep 2021-)

EDGARAS JASINSKAS agent, EJ TEAM INC. (Illinois (US), 18 May 2016-)

inactive EDVINAS JASINSKAS director, inactive EDVINAS JASINSKAS LIMITED (United Kingdom, 7 Nov 2017-22 Sep 2020)

inactive EDVINAS JASINSKAS director, inactive FAST CAR PARTS LIMITED (United Kingdom, 6 Jun 2022- 7 Nov 2023)

inactive GEDIMINAS JASINSKAS director, inactive PREMIER CONSTRUCTION PROPERTY SERVICES LTD (United Kingdom, 2 Aug 2012-13 May 2014)

inactive GEDIMINAS JASINSKAS director, inactive PREMIER CONSTRUCTION (LONDON &KENT) LIMITED (United Kingdom, 11 Mar 2013-27 Oct 2015)

inactive GEDIMINAS JASINSKAS director, inactive TPG CONSTRUCTION AND RESTORATION LTD (United Kingdom, 13 May 2013-26 Oct 2021)

JASINSKAS PIERRE, MATHIEU gérant et associé indéfiniment responsable, PYT (France, 5 Oct 2022-)

JASINSKAS, ANDRIUS manager, branch H TRANSPORTE USA LLC (Illinois (US), 11 Sep 2020-)

JASINSKAS, ANDRIUS manager, branch HEGELMANN USA, LLC (Illinois (US), 11 Sep 2020-)

inactive JUNE JASINSKAS clerk, inactive nonprofit ABINGTON MIDGET FOOTBALL CLUB, INC. (Massachusetts (US), 28 Aug 1970- 2 Mar 1984)

inactive JURGIS JASINSKAS agent, inactive SOUTH FLORIDA RESIDENTIAL PROPERTIES, INC. (Florida (US), 6 Apr 2021-)

Jasinskas, Kathleen agent, KC4J LLC (North Carolina (US), 15 Mar 2023-)

Jasinskas, Kathleen agent, Skylark Music School, LLC (North Carolina (US), 15 Jan 2019-)

Jasinskas, Kathleen manager, KC4J LLC (North Carolina (US), 15 Mar 2023-)

inactive Jasinskas, Kathleen managing member, inactive Triangle Key, LLC (North Carolina (US), 1 Sep 2022-)

inactive Jasinskas, Kathleen agent, inactive Triangle Key, LLC (North Carolina (US), 1 Sep 2022-)

was with something with legal personality – almost always a "legal entity".

This information comes to you from **OpenCorporates** – the leading authority on legal-entity data

Read more about us and why you should trust this data in our purpose, history and principles

The OpenCorporates website is free for general-public and public-benefit use

Use the OpenCorporates API

License this data in bulk

Certified B Corporation

Filter by jurisdiction

1 Cyprus
3 Denmark
8 Florida (US)
1 France
10 Illinois (US)
5 Massachusetts (US)
6 North Carolina (US)
21 United Kingdom

Filter by position

16 agent
4 authorized member
1 clerk
23 director
1 gérant et associé indéfinimen...
1 interessenter
4 manager
1 managing member
1 president
1 real property
1 soc signatory
1 stiftere

Filter by nationality

1 Française
20 LITHUANIAN
1 POLISH
33 [blank]

Filter by occupation

1 BUILDER
1 BUSINESSMAN
3 COMPANY DIRECTOR
1 DELIVERY DRIVER
10 DIRECTOR
1 LABOURER
1 MANAGING DIRECTOR
1 RESTAURATEUR
36 [blank]

SEARCH

Log in/Sign up

Data source and freshness

Last update from source Please log in to see this data

Last change recorded

Next update from source

Source

Learn more about our trust and data transparency policy

This information comes to you from **OpenCorporates** – the leading authority on legal-entity data

Read more about us and why you should trust this data in our purpose, history and principles

The OpenCorporates website is free for general-public and public-benefit use

Use the OpenCorporates API

License this data in bulk

Certified B Corporation

CODE SCHEME

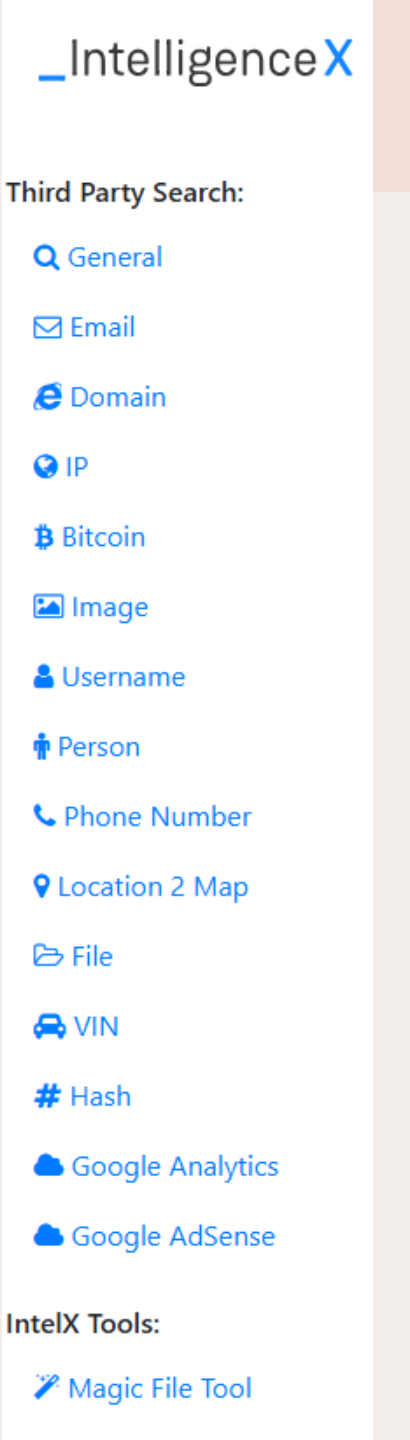
, except industrial process UK SIC Classification 2003 historic details

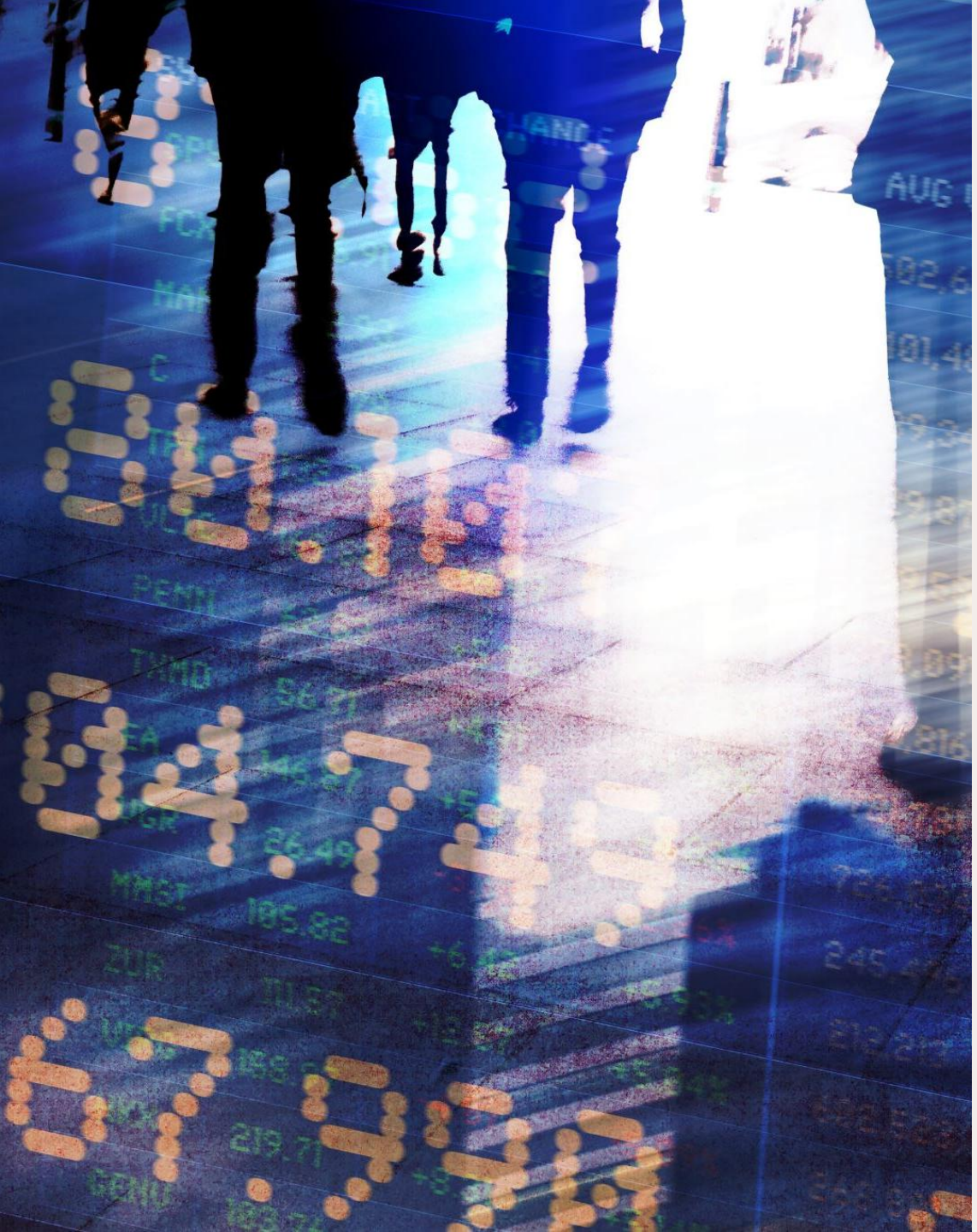
IntelligenceX

- **The search works with selectors**, i.e. specific search terms such as email addresses, domains, URLs, IPs, CIDRs, Bitcoin addresses, IPFS hashes, etc.
- **It searches in places such as the darknet, document sharing platforms, whois data, public data leaks** and others.

Intelligence X searches billions of selectors in a matter of milliseconds. Here are some examples of Intelligence X's power:

- Research the Trump Organization's email server reported by ArsTechnica
- Research the Austrian Parliament
- Investigate a Bitcoin address
- Investigate a Social Security Number
- List all .com email addresses on North Korean websites
- Read the Hillary emails (FOIA/UNCLASSIFIED)





Reverse Image Search

- Identifying the Original Source of an Image
- Verifying Image Authenticity
- Geolocation and Context Discovery
- Identifying Individuals
- Tracking Criminal Activity Across Platforms

Reverse Image Search -Google

oogle

Add to your search

AI Mode | All | Exact matches | Visual matches | About this image | Feedback

Pristatau dar vieną straipsnį ir dar kartą prisistatau . Nuo ... - Instagram

9 Apr 2026 · 640x1 136

Instagram

Šiemet gimtadienio dovaną gavau tokią, kuri dar ilgai gyvens širdyje ...

1 Sept 2025 · 640x1 136

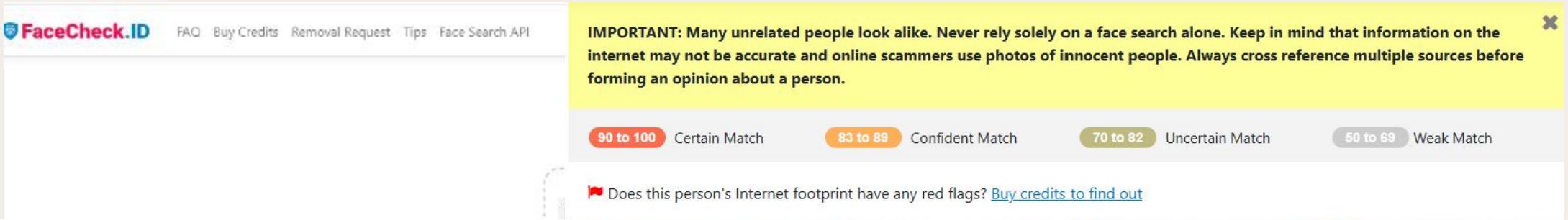
Instagram

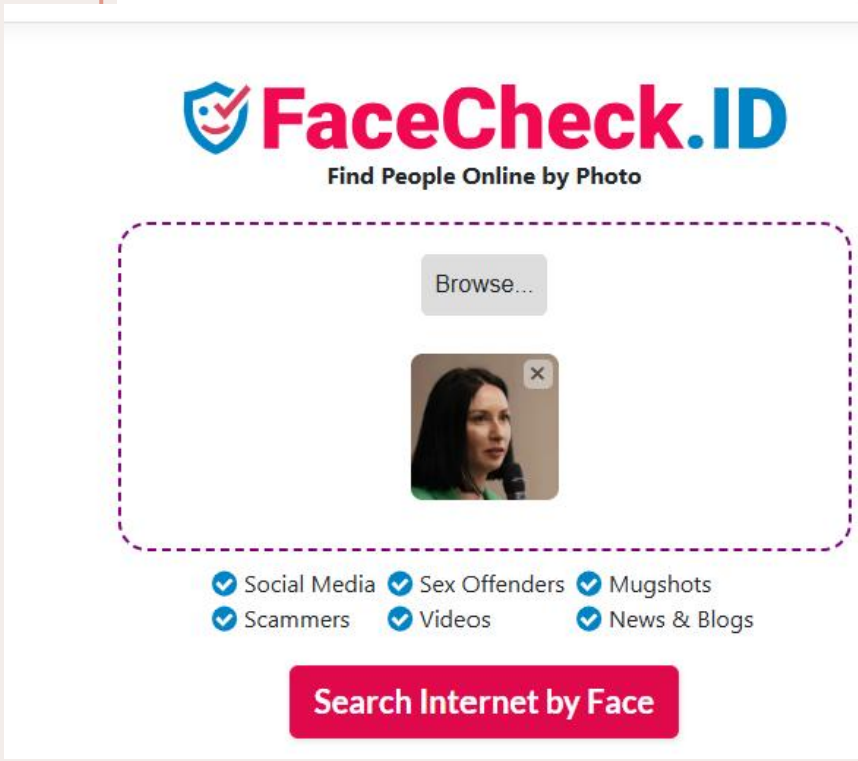
4 dienos, 3 regionai – Abruzzo, Umbria ir Emilia-Romagna. Ryškiai ...

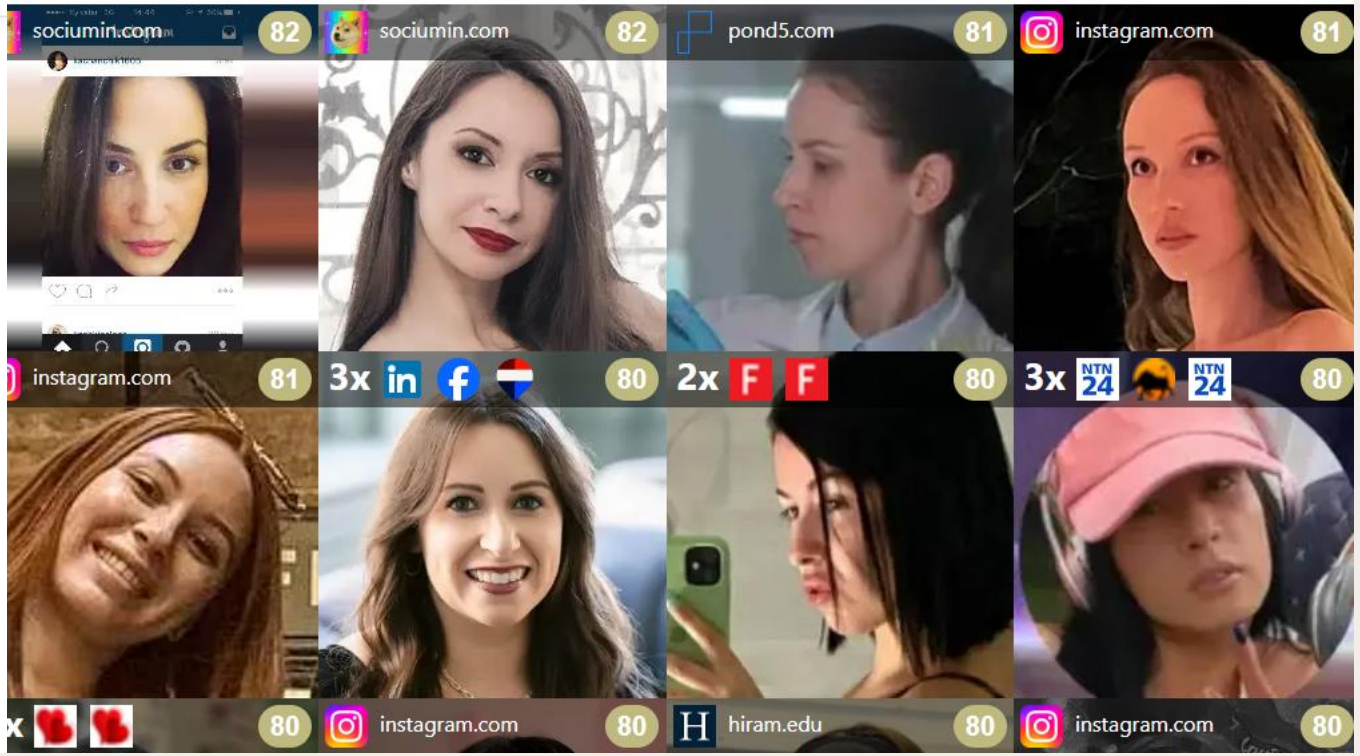
14 Oct 2025 · 640x1 136

Instagram

People search







platesmania.com

License plates found **12**

You have searched:

andre

« 1 2 »

Discover more

- Vehicle Specs, Reviews & Comparisons
- Jeep Grand Cherokee
- Jeep

Germany

Ferrari F355

1st gen Spider (F129), 1995–2000

EM LI 3

Brescia,Italy
16/06/2021

cannoutt — Jun 16, 2021, 10:10:18 PM

20 0

Germany

Ferrari F355

1st gen Spider (F129), 1995–2000

EM LI 3

National Double Spot (Brescia - Monteriggioni)

Monteriggioni (SI), Italy

Sciaccalex — Jun 17, 2023, 3:07:

5 0

Poland

Mercedes-Benz EQS

1st gen Liftback (V297), 2021–

G7 ANDRE

Gdańsk

belugin — Mar 9, 2026, 3:03:32 PM

4 0

Poland

Opel Insignia

2nd gen Liftback (B; Z18), 2017–2022

G6 ANDRE

16.10.2025.
Gdańsk, województwo pomorskie, Polska

#OpelCarsDay6

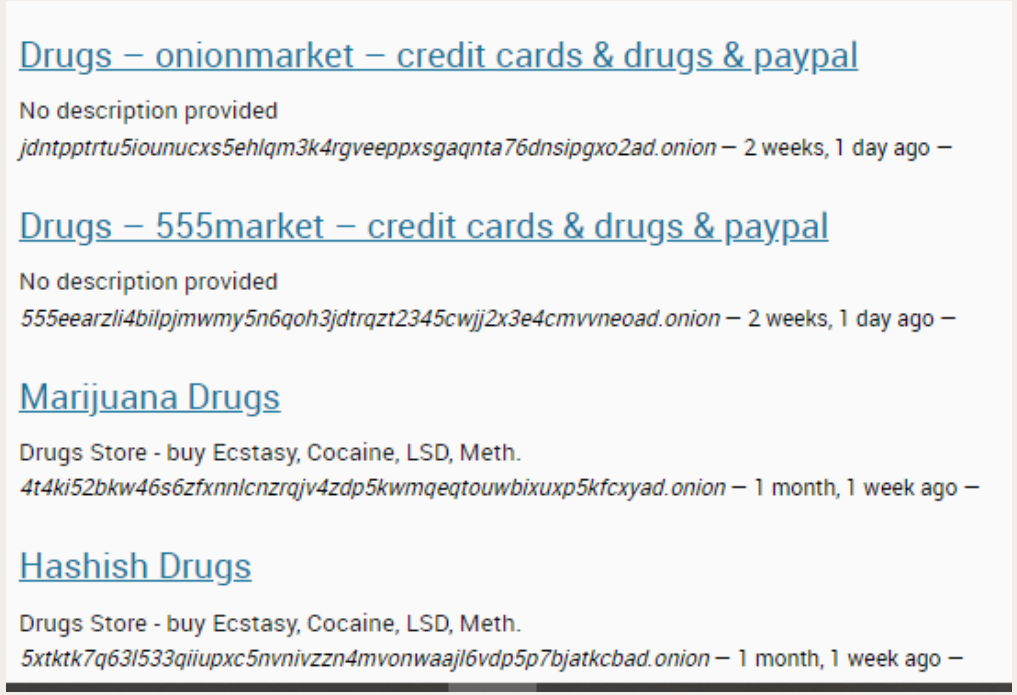
a_wiskari — Nov 28, 2025, 11:51:48 PM

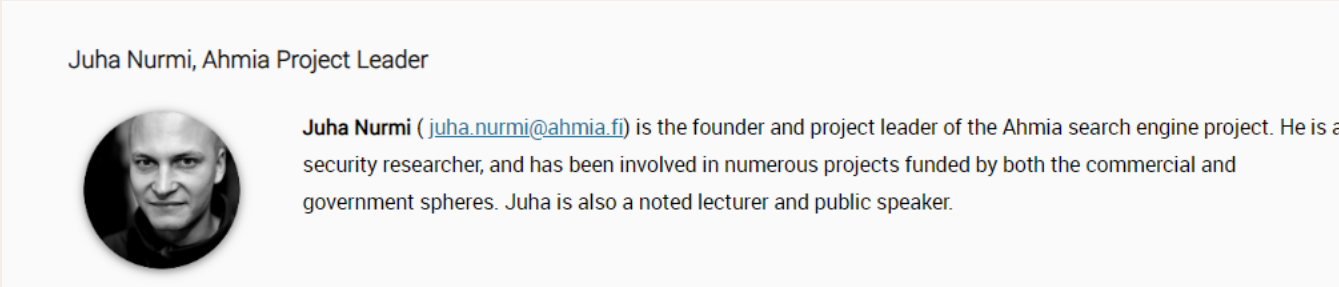
12 0

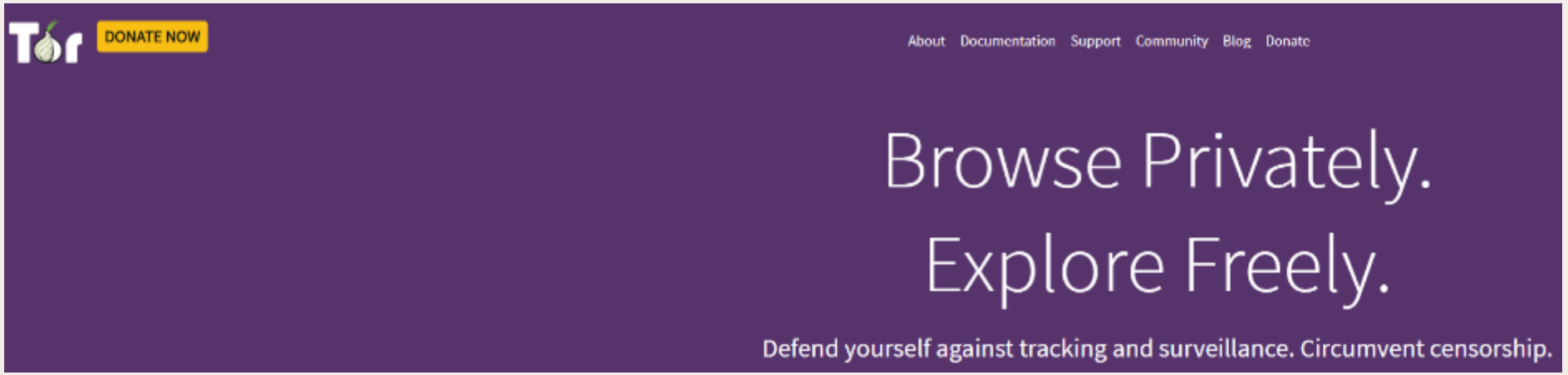
Ahmia.fi

“Ahmia's mission is to create the premier search engine for services residing on the Tor anonymity network. In doing so, we hope to share meaningful statistics, insights, and news about the Tor network and the Tor project.

Contributors to Ahmia believe that the Tor network is an important and resilient distributed platform for anonymity and privacy worldwide. By providing a search engine for what many call the "deep web" or "dark net", Ahmia makes onion services accessible to a wide range of people, not just Tor network early adopters.”



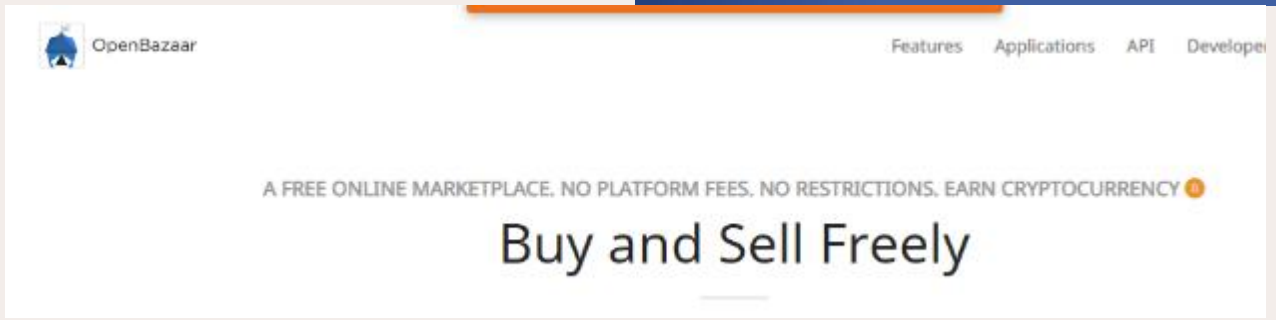



Tor
DONATE NOW
About Documentation Support Community Blog Donate
Browse Privately.
Explore Freely.
Defend yourself against tracking and surveillance. Circumvent censorship.


ZeroNet
Open, free and uncensorable websites,
using Bitcoin cryptography and BitTorrent network


FREENET
Browse websites, post on forums, and publish files within Freenet with strong privacy protections.


I2P
Download About Donate


OpenBazaar
Features Applications API
A FREE ONLINE MARKETPLACE. NO PLATFORM FEES. NO RESTRICTIONS. EARN CRYPTOCURRENCY
Buy and Sell Freely

PART III

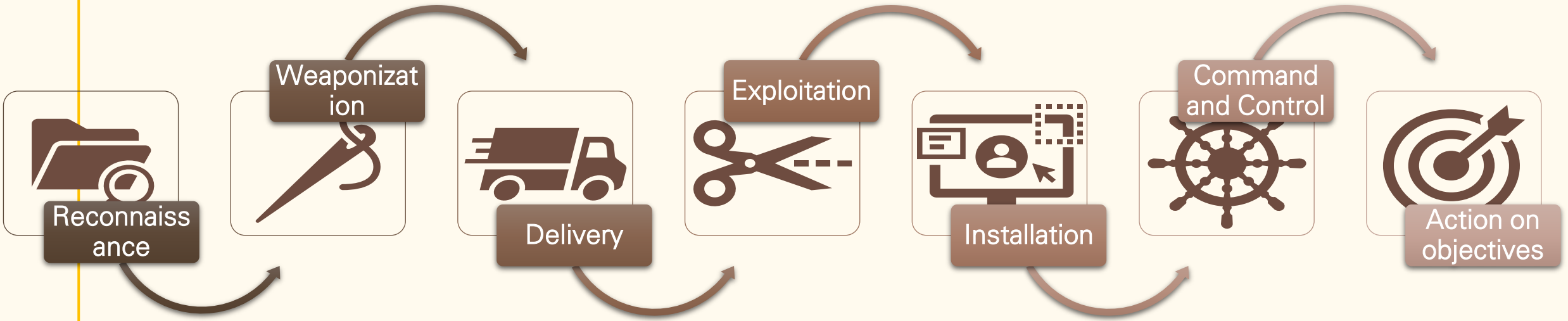
OSINT - Enabler or Co-author

How criminals weaponise the same open sources

Examples of Use Cases by Criminals

- Phishing & Social Engineering: Scraping social media and company sites to craft convincing, personalized phishing emails (e.g., CEO impersonation)
- Credential Harvesting: Monitoring leaked credentials on the dark web and using them for credential stuffing
- Infrastructure Reconnaissance: Using tools like Shodan to find exposed devices and unpatched systems
- Identity Theft: Collecting personal details for harassment or impersonation
- Supply Chain Attacks: Analyzing third-party vendors' security weaknesses to breach larger organizations

OSINT and Cyber Kill Chain



INVESTIGATOR

→ Maps suspect's network to identify associates

→ Locates suspect from geotagged photos

→ Builds timeline from post history

→ Identifies witnesses from event photos

→ Verifies alibis against public check-ins

vs

CRIMINAL

→ Maps target's network to find weak links

→ Locates target's home from geotagged photos

→ Builds victim profile from post history

→ Identifies vulnerable employees from photos

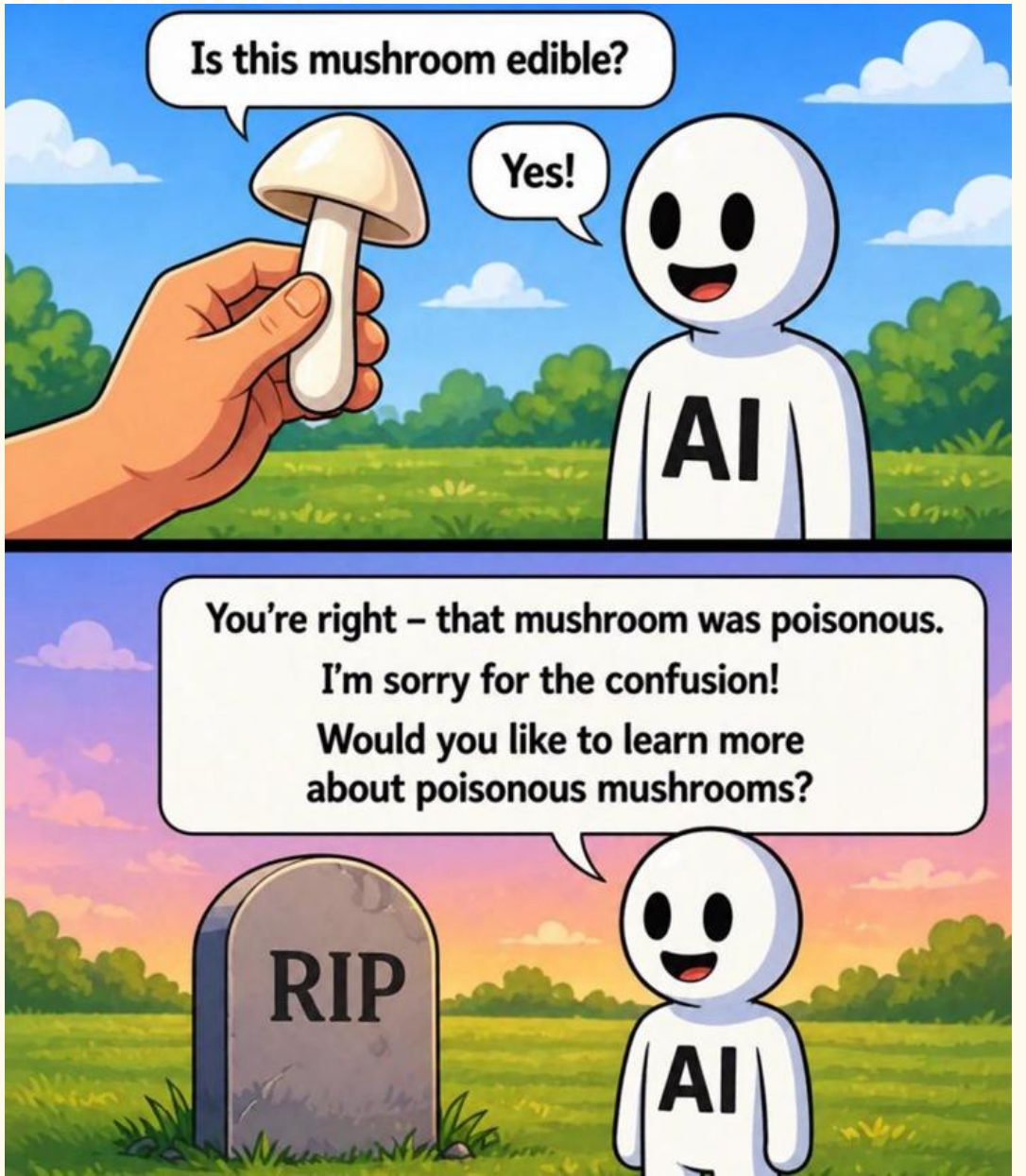
→ Crafts phishing using personal details found online

The gap between a criminal's OSINT toolkit and an investigator's is very small. The difference lies in intent and legal authority.

The AI will do that for me….

AI characteristics

- **Speculative** – when data is lacking, AI tends to fantasize (hallucinate) or speculate, which is why answers vary.
- **Flattering**. AI tends to act in a way that aligns with the user's opinion or beliefs, even if it isn't objectively true.
- **Evolving**. AI learns from new data, so it can change its answers as a result.



PART IV

Case Study

Operation “Ghost Invoice”

How a €2.3M wire fraud unfolded through open sources alone

€2.3M

Transferred in 3 payments

3 hrs

Total reconnaissance time

0

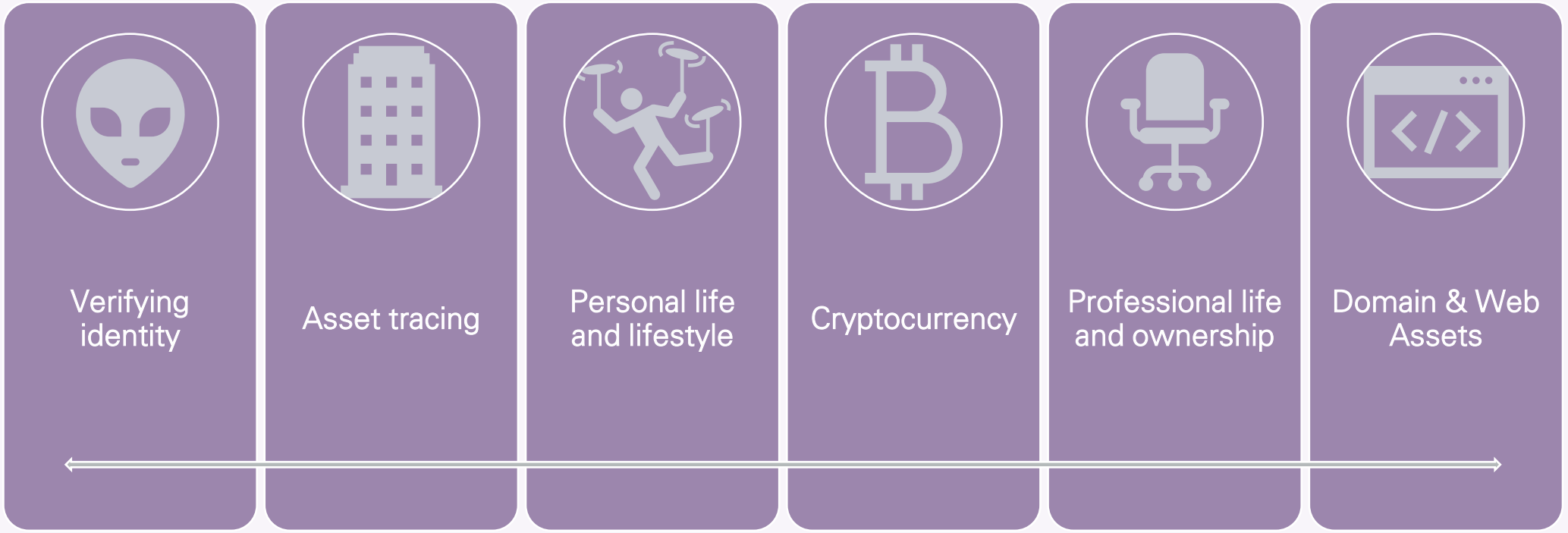
systems hacked

PART V

Take Away

You do not need to be an OSINT expert — you need to be an intelligent, critical evaluator

Use cases of the OSINT



Professional search principles

1	Always cross-reference	Run the same query on at least 3 different engines — results will differ significantly
2	Date your searches	Results change daily; always record when you searched, not just what you found
3	Use incognito mode	Prevents personalisation from distorting results and avoids alerting suspects
4	Document everything	Screenshot URL + content + timestamp. Unsaved browser tabs are not evidence

The Five Questions Every Judge and Prosecutor Must Ask

1	How was this collected, and when?	Was it preserved before or after the suspect became aware of the investigation? What tool? Is there a methodology report?
2	Has it been preserved and authenticated?	Is there a cryptographic hash? Has the content been independently verified? Is the source URL documented and accessible?
3	Could it have been manipulated or fabricated?	Has deepfake/editing analysis been conducted? Could metadata be spoofed? Has an independent expert reviewed the raw file?
4	What fundamental rights issues arise?	Was collection proportionate? Was GDPR/LED complied with? Were any special category data collected? Was a legal basis established?
5	Is the person presenting it qualified to interpret it?	OSINT evidence should be presented by trained practitioners with a clear methodology — not whoever found it under time pressure.

Questions & Discussions

You can contact me at rj@nrdcs.lt

HOW CAN RETRIEVAL-AUGMENTED GENERATION (RAG) BE APPLIED IN LEGAL PRACTICE

Leonarda Stanarević, MSc

AI Consultant for Digital Forensics

INsig2 d.o.o.

Co-funded by the European Union.
Views and opinions expressed are however those of ERA only and do not necessarily reflect those of the European Union or European Commission.
Neither the European Union nor the granting authority can be held responsible for them.

~~HOW CAN RETRIEVAL-AUGMENTED GENERATION (RAG) BE APPLIED IN LEGAL PRACTICE~~

ASK THE FILE, CHECK THE SOURCE

Leonarda Stanarević, MSc

AI Consultant for Digital Forensics

INsig2 d.o.o.

Leonarda Stanarević

- AI Consultant for Digital Forensics @ INSIG2
- Advising, training and generating AI-driven solutions

INSIG2

About INsig2

- Established in 2004, HQ in Zagreb
- 80+ highly educated employees
- Educational & Training centre

Education & Training Centre in Zagreb, Croatia

- Accommodates up to 15 people per classroom
- Equipment, forensic tools & materials provided

INsig2

- Three business units
- „One-stop-shop” in the field of Digital Forensics

E-learning platform

- Customized courses
- For legal entities, law enforcement, and private sectors
- Courses on deeper aspects of digital forensics and forensic value of the evidence while collecting, processing, and presenting digital evidence in criminal and administrative proceedings
- Website: https://insig2-and-zyberglobal.learnworlds.com/

Fundamentals of digital forensics for lawyers and judges

This course is intended for lawyers, judges and public prosecutors in order to help them understand the basics of digital forensics.

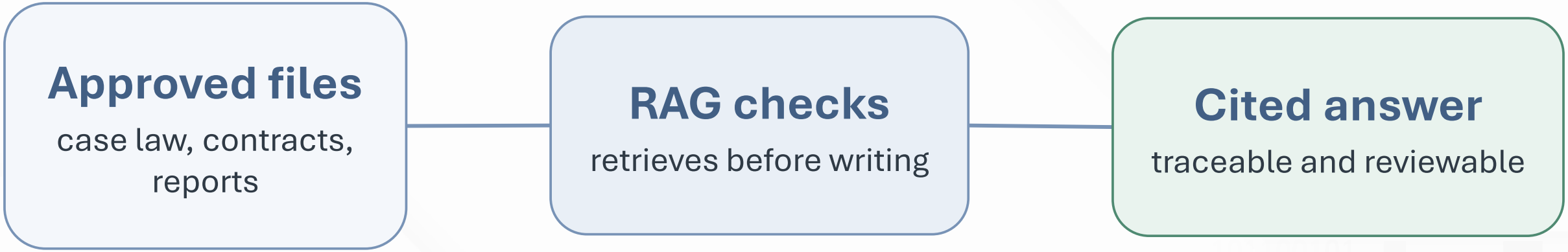
Fundamentals of digital forensics for private sector

This course is intended for various industry professionals working in private sector such as IT administrators, managers, IT security

Password Management

This course covers different lock security methods, guidelines on securely storing your passwords, various password managers and

Ask the file

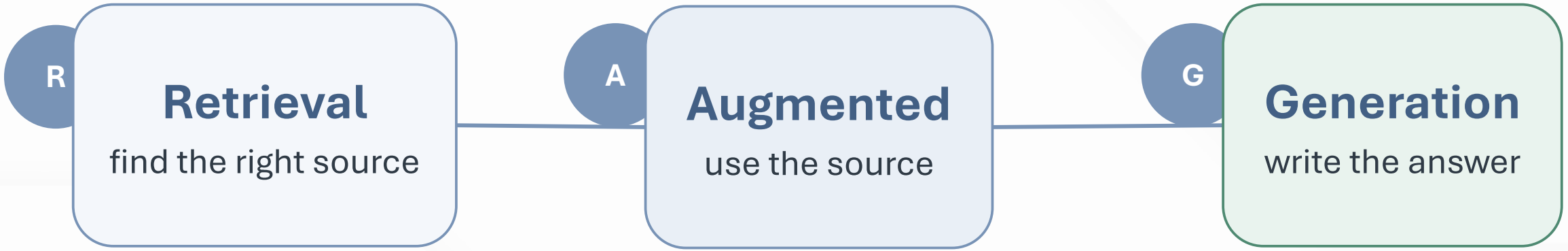


The legal value is not "AI wrote it" ...
It is "the answer points back to the source"

INSIG2

RAG = Retrieval-Augmented Generation

What does RAG mean??



Order matters: source first, answer second

RAG = Retrieval-Augmented Generation

What does RAG mean??

R **Retrieval**
find the right source

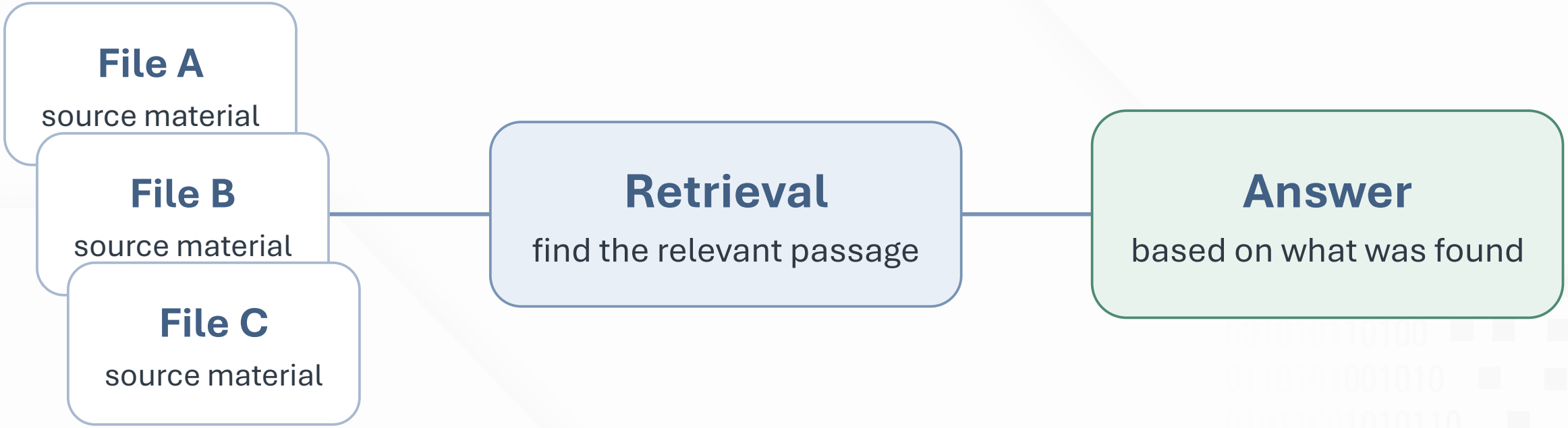
A **Augmented**
use the source

G **Generation**
write the answer

Order matters: source first, answer second

RAG = Retrieval-Augmented Generation

The answer is already *in there*



The problem is not always legal reasoning
It is often finding the exact page, clause, date, or paragraph **fast enough**

RAG = Retrieval-Augmented Generation

Why retrieval comes first

Without retrieval

The model guesses from general knowledge.

With retrieval

The file controls the answer.

Legal fit

Less speculation, more reviewability.

RAG = Retrieval-Augmented Generation

Why retrieval comes first

Without retrieval

The model guesses from general knowledge.

With retrieval

The file controls the answer.

Legal fit

Less speculation, more reviewability.

INSIG2

RAG = Retrieval-Augmented Generation

If you can’t check it, don’t trust it

Weak answer

“The deadline was probably extended”

Better answer

“See email from March 14th and Annex 2”

The lawyer verifies the source
The tool only accelerates the path to it

RAG = Retrieval-Augmented Generation

If you can’t check it, don’t trust it

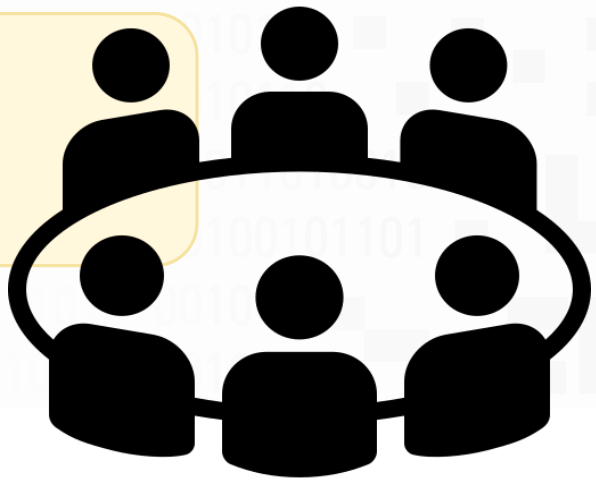
Weak answer

“The deadline was probably extended”

Better answer

“See email from March 14th and Annex 2”

The lawyer verifies the source
The tool only accelerates the path to it



INSIG2

RAG = Retrieval-Augmented Generation

Polished is not the same as *reliable*

Polished

Fluent answer
Confident tone
May be unsupported

≠

Reliable

Source-linked answer
Scoped to the file
Reviewable
Conclusion stays with counsel

RAG = Retrieval-Augmented Generation

The first red flag

Red flag

“We can’t upload this online”

Access first

Who can see documents, prompts and logs?

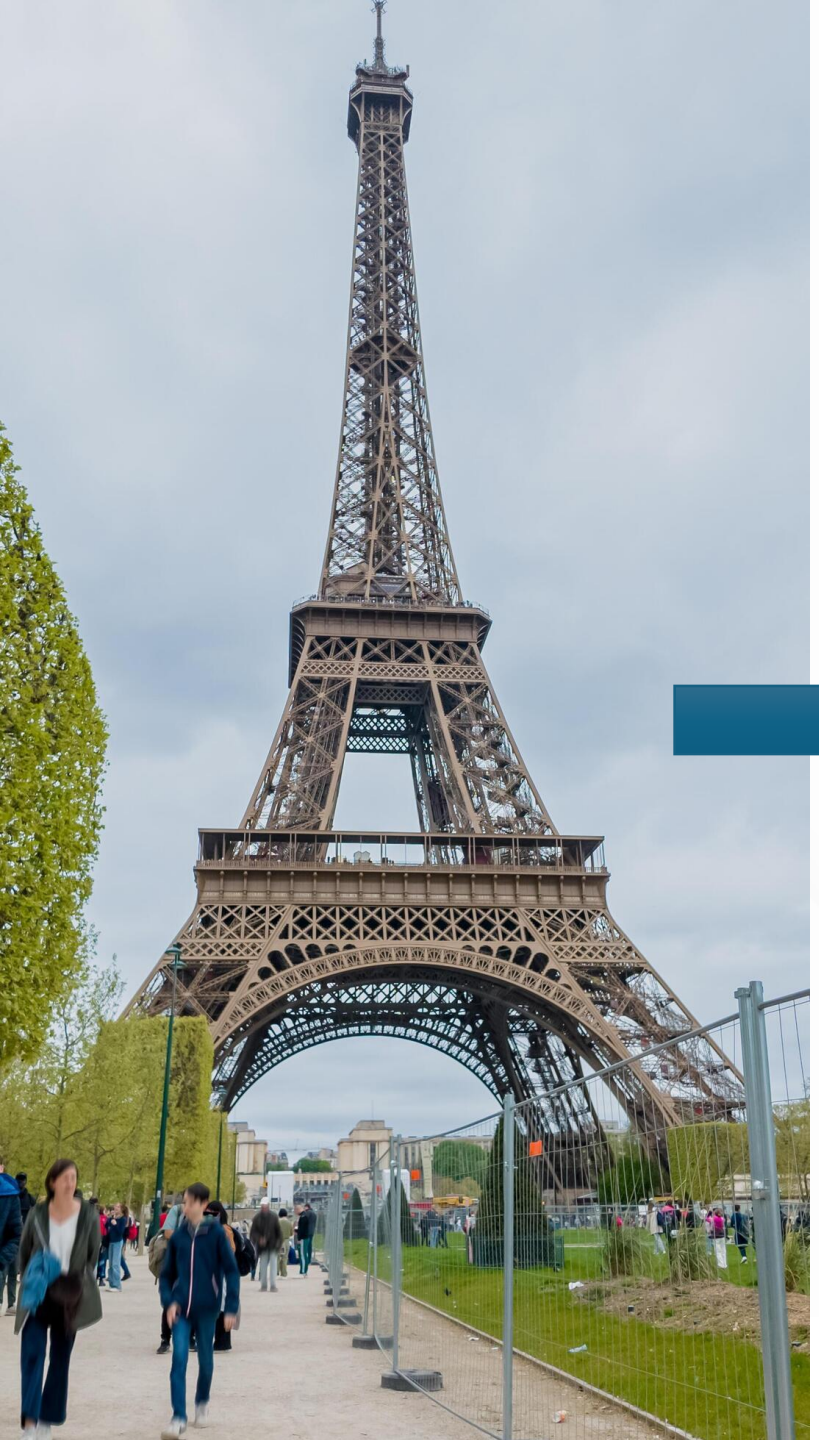
Risk areas

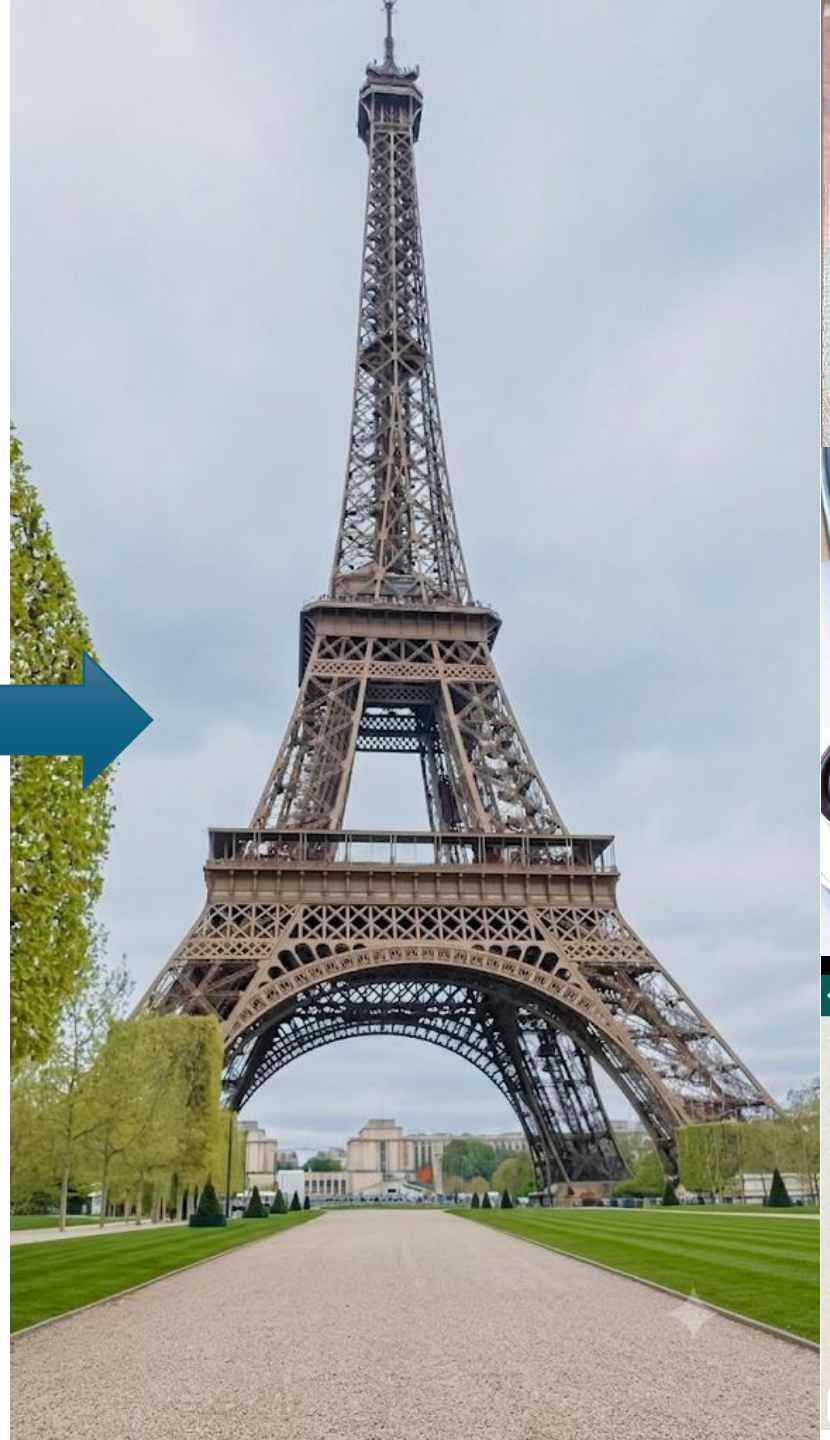
Privilege
Personal data
Evidence handling

Confidentiality is not an afterthought

INSIG2

RAG = Retrieval-Augmented Generation





REPUBLIKA HRVATSKA/REPUBLIC OF CROATIA/RÉPUBLIQUE DE CROATIE

PUTOVNICA
PASSPORT
PASSEPORT

Vrsta/Type/Type: P
Oznaka države/Country code/Code du pays: HRV
Br. putovnice/Passport No./Passeport N°: 007007007

Prezime/Surname/Nom
SPECIMEN

Ime/Given name/Prénom
SPECIMEN

Državljanstvo/Nationality/Nationalité
HRVATSKO

Datum rođenja/Date of birth/Date de naissance
25.12.1982.

Spol/Sex/Sexe: F
Mjesto rođenja/Place of birth/Lieu de naissance: ZAGREB

2014

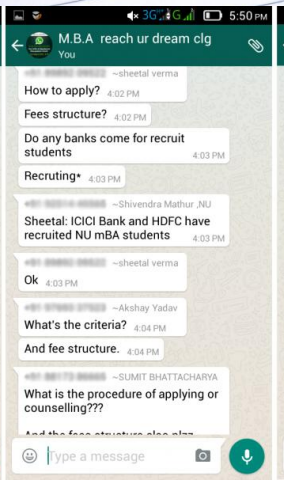
RH

Datum izdavanja/Date of issue/Date de délivrance
01.07.2009.

Izdana od/Issued by/Délivré par
PU/ZAGREB

Datum isteka valjanosti/Date of expiry/Date d'expiration
01.07.2014.

Vlastoručni potpis/Holder's signature/Signature du titulaire



The first red flag

Red flag

“We can’t upload this online”

Access first

Who can see documents, prompts and logs?

Risk areas

Privilege
Personal data
Evidence handling

Confidentiality is not an afterthought

INSIG2

RAG = Retrieval-Augmented Generation

Three ways to use RAG

Public RAG

Published law

Public sources

Lowest document risk

Private RAG

Approved internal repositories

Controlled access

Offline RAG

Isolated/local case materials

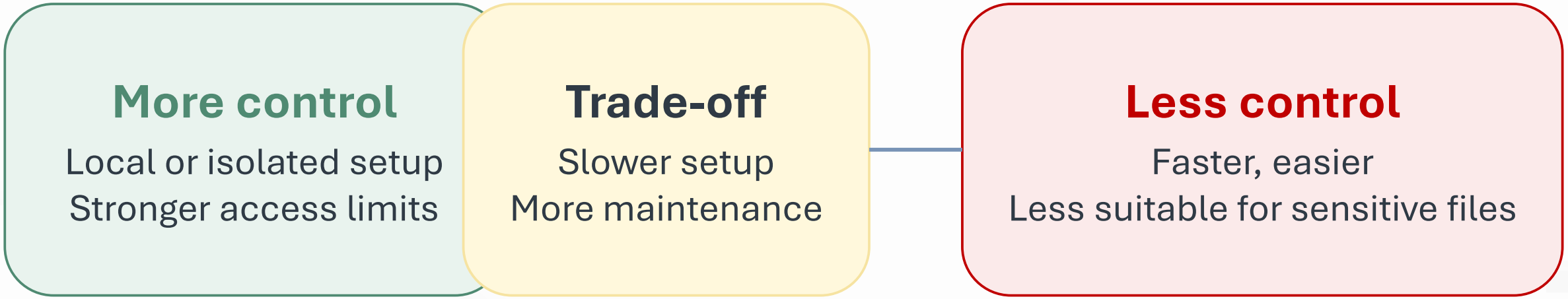
Highest control

Match the system to the document risk

INSIG2

RAG = Retrieval-Augmented Generation

Control has a cost



The "best" option is the one that fits
confidentiality
priviledge
evidence risk

RAG = Retrieval-Augmented Generation

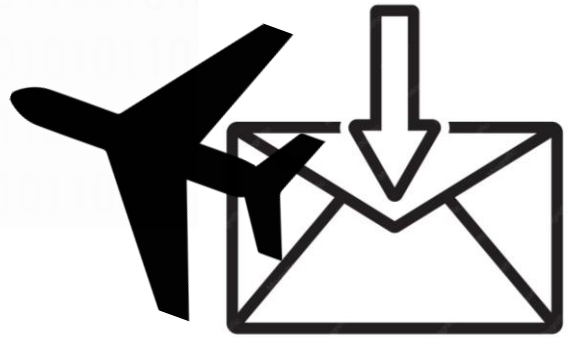
Where RAG really helps

Find passages
pinpoint relevant text

Compare versions
surface differences

Prepare faster
first-pass work product

Check faster
review with source links



INSIG7

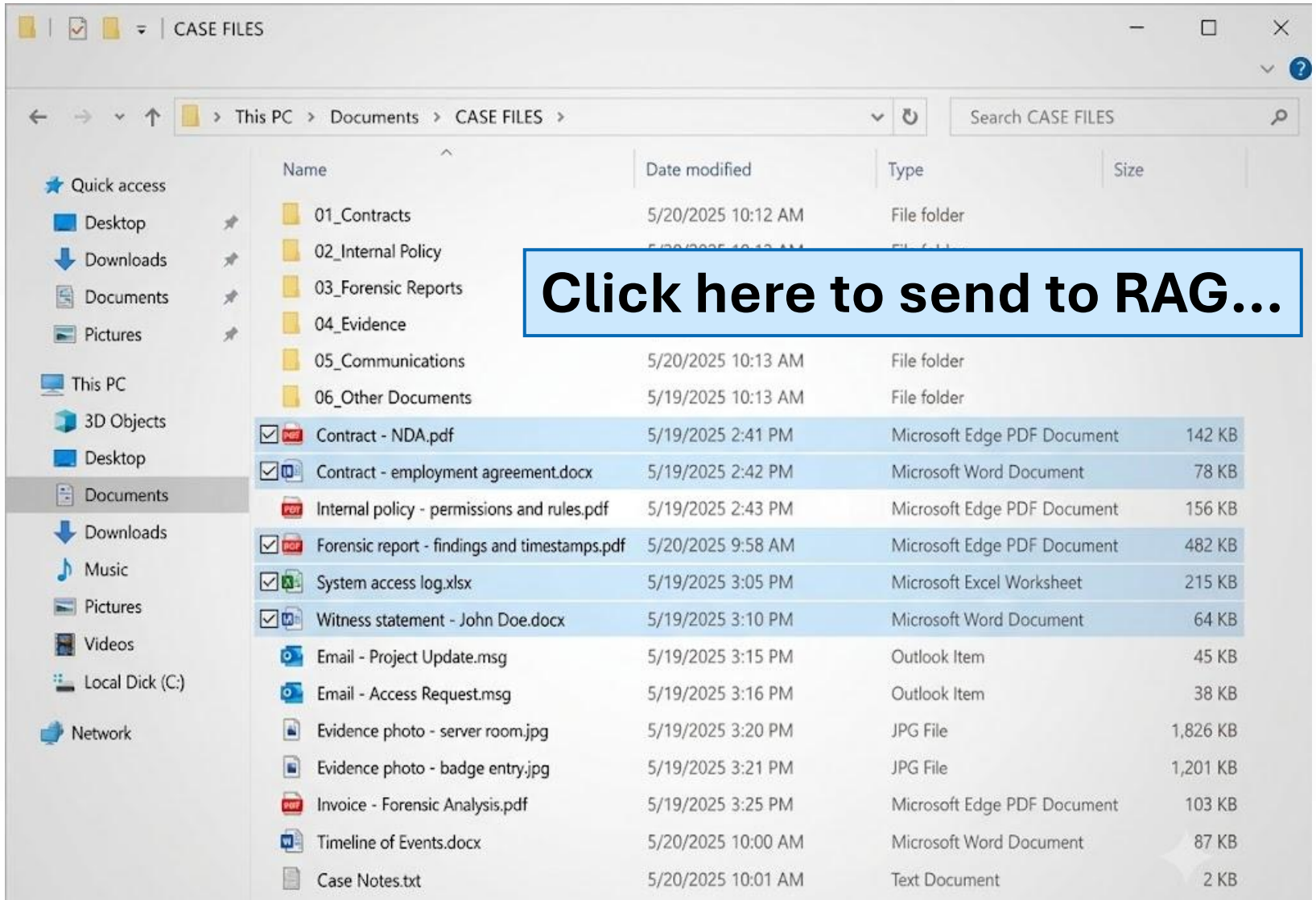
RAG = Retrieval-Augmented Generation

Scenario: Suspected internal data leak

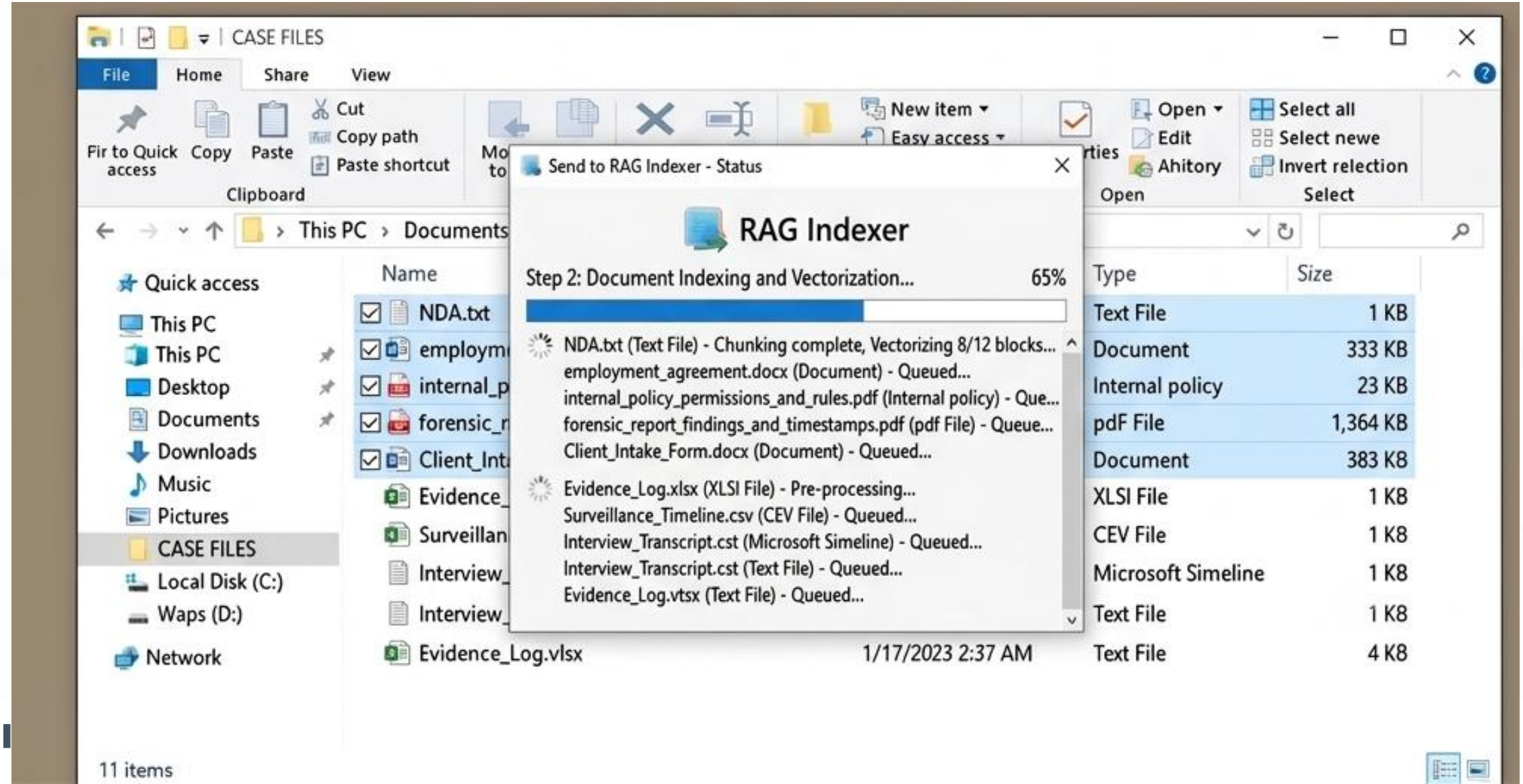
INSIG2

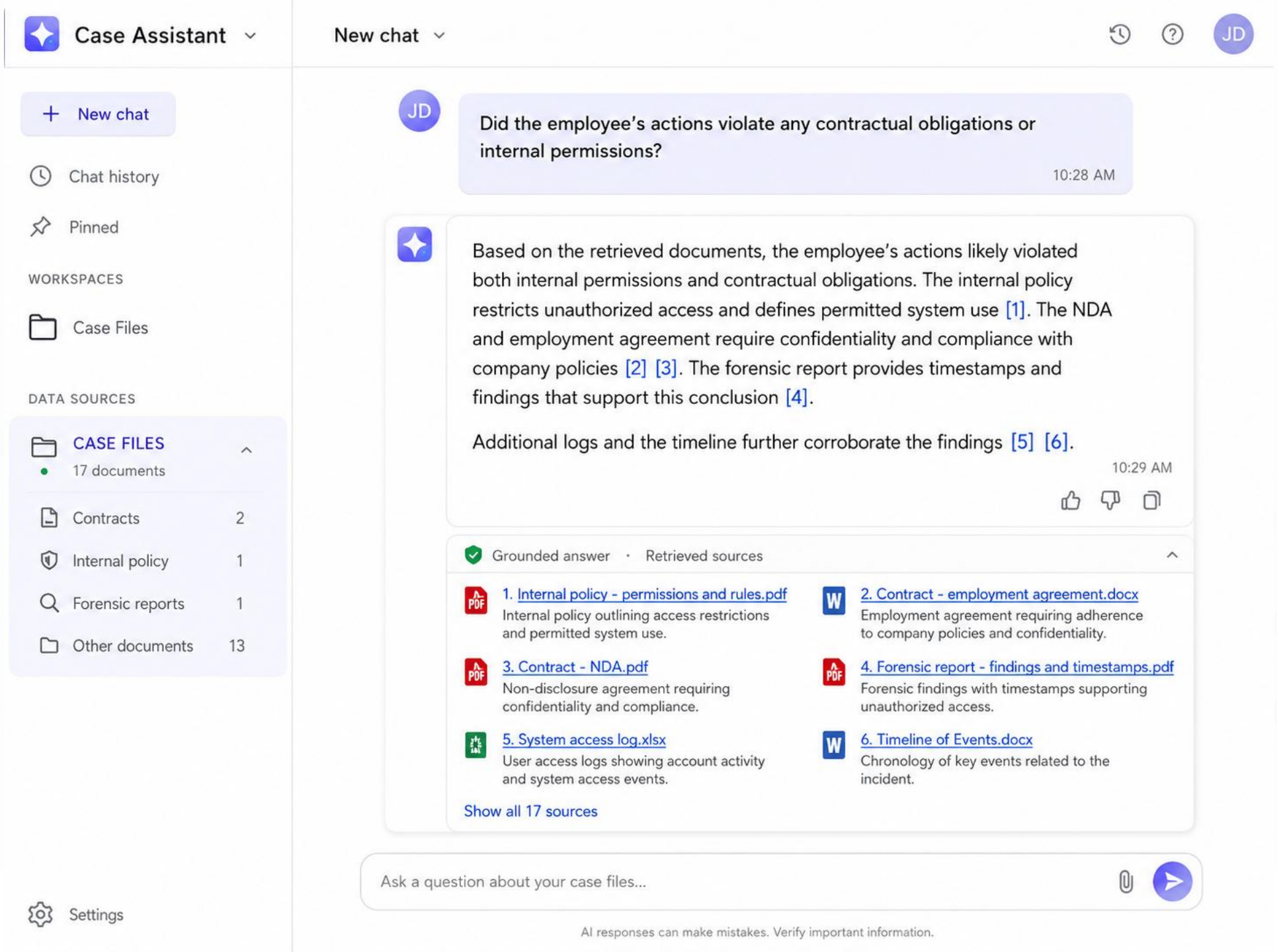
RAG = Retrieval-Augmented Generation

Scenario: Suspected internal data leak

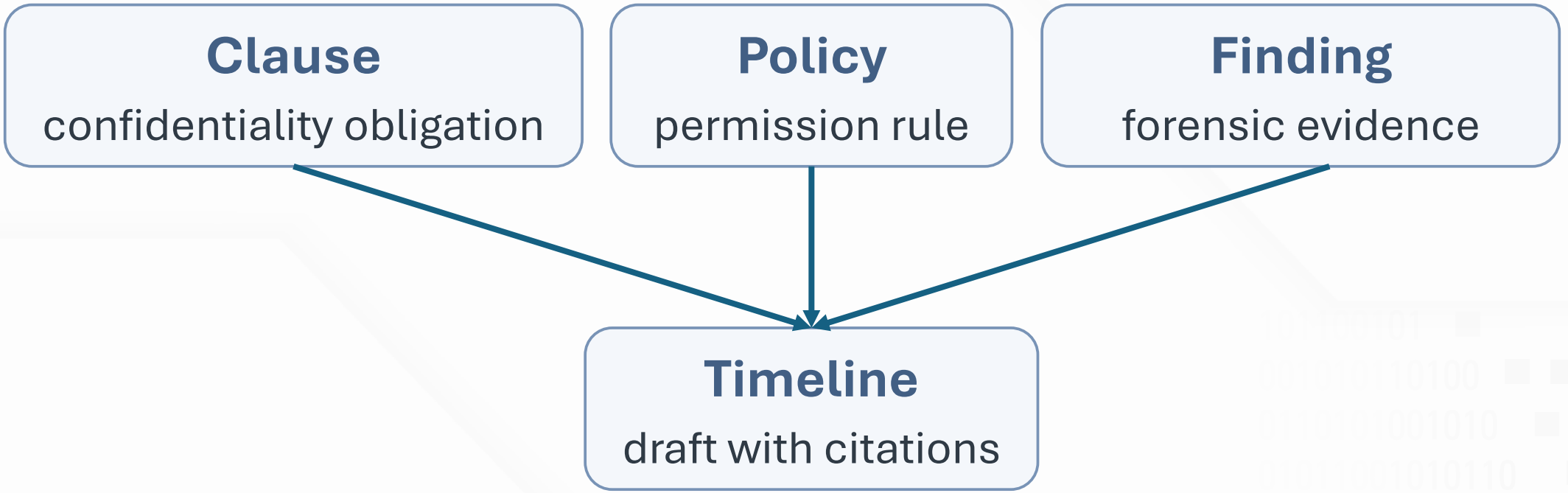


Scenario: Suspected internal data leak




Case Assistant
New chat
JD
+ New chat
Chat history
Pinned
WORKSPACES
Case Files
DATA SOURCES
CASE FILES
17 documents
Contracts 2
Internal policy 1
Forensic reports 1
Other documents 13
Settings
Did the employee's actions violate any contractual obligations or internal permissions?
10:28 AM
Based on the retrieved documents, the employee's actions likely violated both internal permissions and contractual obligations. The internal policy restricts unauthorized access and defines permitted system use [1]. The NDA and employment agreement require confidentiality and compliance with company policies [2] [3]. The forensic report provides timestamps and findings that support this conclusion [4].
Additional logs and the timeline further corroborate the findings [5] [6].
10:29 AM
Grounded answer · Retrieved sources
1. Internal policy - permissions and rules.pdf
Internal policy outlining access restrictions and permitted system use.
2. Contract - employment agreement.docx
Employment agreement requiring adherence to company policies and confidentiality.
3. Contract - NDA.pdf
Non-disclosure agreement requiring confidentiality and compliance.
4. Forensic report - findings and timestamps.pdf
Forensic findings with timestamps supporting unauthorized access.
5. System access log.xlsx
User access logs showing account activity and system access events.
6. Timeline of Events.docx
Chronology of key events related to the incident.
Show all 17 sources
Ask a question about your case files...
AI responses can make mistakes. Verify important information.

What RAG does in practice



The output is useful because each step can point back to the document

RAG = Retrieval-Augmented Generation

Navigating large files with direction

Search direction

person

date

device

event

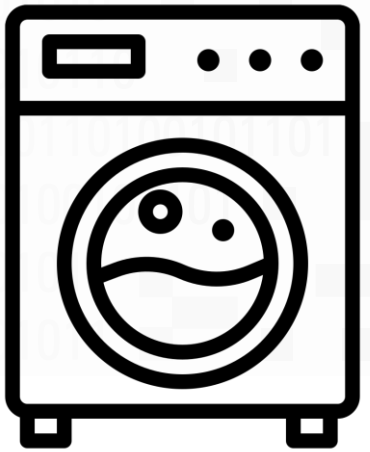
Relevant passages

faster than manual scanning

Source link

always return to the file

RAG does not read “for” the lawyer.
It helps the lawyer reach the right place faster



INSIG2

RAG = Retrieval-Augmented Generation

Smarter first-pass contract review

Locate key provisions

Compare similar contracts

Flag unusual wording

Lawyer reviews context

A first pass, not a final legal opinion

INSIG7

RAG = Retrieval-Augmented Generation

Unlocking institutional memory

Templates
starting points

Policies
current rules

Procedures
how work is done

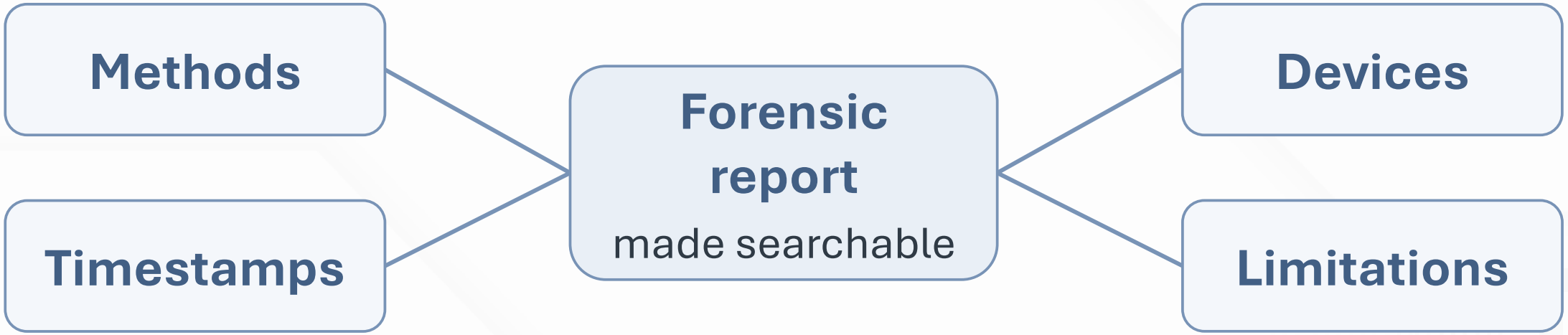
Prior work
institutional know-how

RAG makes internal knowledge searchable without turning it into uncontrolled copy-paste

INSIG2

RAG = Retrieval-Augmented Generation

Making forensic reports usable



Better preparation for expert review and cross-checking

RAG = Retrieval-Augmented Generation

Hallucinations

Hallucination
fabrication or mistake

Citation checkpoint
Does the answer point to an actual source?

Reviewable answer
lawyer can verify the passage

Hallucinations

This Government Paid Deloitte $1 Million for a Report That Included Fake AI Citations

An investigation found that Deloitte cited research that didn't exist in the 526-page report.

BY SHERIN SHIBU | EDITED BY JESSICA THOMAS | NOV 25, 2025

Hallucinations

Hallucination
fabrication or mistake

Citation checkpoint
Does the answer point to an actual source?

Reviewable answer
lawyer can verify the passage

What a *good* answer sounds like

Precise
answers the asked question

Cited
shows where it came from

Reviewable
source can be checked

Separated
facts vs. conclusions

INSIGO

RAG = Retrieval-Augmented Generation

The contract contains a **confidentiality obligation** in clause 12.
The forensic report records **USB activity** on March 14th in section 4.2.
I **did not find** a document stating that the employee had approval for that activity.
Legal significance **requires counsel review**.

What a *good* answer sounds like

Precise
answers the asked question

Cited
shows where it came from

A good legal AI answer makes verification easier, not optional

Reviewable
source can be checked

Separated
facts vs. conclusions

INSIG7

RAG = Retrieval-Augmented Generation

Start safe, then scale

Low risk
published case law
legislation

Controlled pilot
approved templates
anonymized files

Scale carefully
sensitive matters
stronger controls

Test citation quality and user behavior before moving to higher-risk documents

RAG = Retrieval-Augmented Generation

What this talk is really about

This is not "AI magic"

It is controlled, source-linked context retrieval for AI-generated drafting

- **Clauses**
- **Timestamps**
- **Policy sections**
- **Report paragraphs**

INSIG2

RAG = Retrieval-Augmented Generation

Rule that matters the most

use whichever AI tool you prefer

NOT MODEL SPECIFIC

Control first
choose the right environment

Limit access
only the right people

Require citations
make claims checkable

Verify always
counsel owns conclusions

The legal safeguard is the workflow, not the interface

INSIG7

RAG = Retrieval-Augmented Generation

Your legal AI assistant

Controlled assistant
private access
scoped content

Large-file support
search and summarize
(without losing source)

Source-linked answers
ask the file
check the source

RAG is useful when it makes verification faster and safer

INSIG2

RAG = Retrieval-Augmented Generation

Thank you for attention!

Questions are warmly welcomed

https://insig2.com/

linkedin.com/in/leonarda-stanarevic/

leonarda.stanarevic@insig2.com

Evolving Definition of Crimes

How AI transforms criminal proceedings
Cybercrimes 2.0
Pretty-Good-Privacy phones and admissibility of data

Sandor Bosch

Court of Appeal Den Bosch
The Netherlands

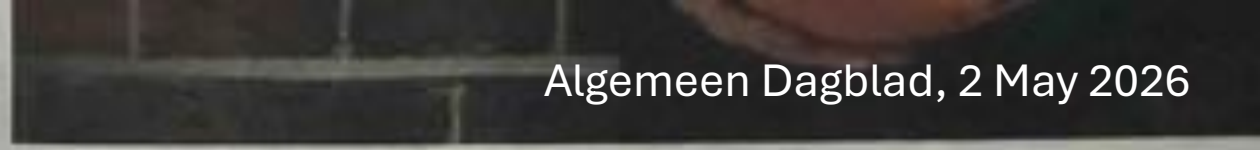
#Digitalisation and #AI in Criminal Justice
ERA seminar · Zagreb · 15-16 June 2026

Tech&Law, OSINT, AI and machine learning

Co-funded by the European Union.
Views and opinions expressed are however those of ERA only and do not necessarily reflect those of the European Union or European Commission.
Neither the European Union nor the granting authority can be held responsible for them.

Hans Spekman
groeide op in armoede

Joods zijn in steeds vijandiger klimaat



Algemeen Dagblad, 2 May 2026

'Alle 60.000 agenten moeten alert zijn op online misdaad'

Cybercriminaliteit krijgt bij politie topprioriteit

Meer dan de helft van alle criminaliteit gebeurt online. Het gaat dan om oplichting, bedreiging, fraude, diefstal en afpersing. Daarom moet iedere agent cybercriminaliteit gaan bestrijden.

Wout van Arensbergen
Henk van Gelder
Driebergen

dagelijks onderdeel worden van hun werk."

Dat inzicht zorgt voor een enorme omslag binnen de politie, die de nieuwe werkwijze de komende jaren invoert. De aanpak van online criminaliteit krijgt topprioriteit en moet volgens Duijf ook in het dagelijkse politiewerk een stevig fundament krijgen.

Samenhangend

Aangiften van online criminaliteit waarbij mensen worden opgelicht, kampen slachtoffers vaak ook met psychische schade. Ze schamen zich en durven niemand meer te vertrouwen. De totale schade van alle cyberincidenten in Nederland zou volgens een onderzoek van het ministerie van Economische Zaken jaarlijks rond de 10 miljard euro bedragen.

Duijf benadrukt dat elke aangifte van belang is. „We kijken als politie

vaak nog te enkelvoudig naar aangiften, te individueel. Vaak zijn er veel meer mensen slachtoffer geworden. De kunst wordt om naar het grotere geheel te kijken. Naar patronen, naar clusters. En dat dan aanpakken. Daarom is elke aangifte belangrijk."

De cyberspecialisten bij de landelijke en regionale teams vormen volgens Duijf het neusje van de zalm en zijn betrokken bij alle grote complexe onderzoeken naar internetcriminelen.

Ook internationaal is de samen-

Why this topic matters now

Digitalisation has moved from a specialist issue to the ordinary environment of criminal justice.

The central development is practical: evidence, communication and offending behaviour are increasingly digital, while courts remain responsible for legality, reliability and fairness.

The pressure points

AI is appearing in legal submissions, internal research tools and criminal modus operandi.

Its outputs force courts to ask who is responsible, how quality is verified, and whether the source can carry legal authority.

The courtroom reality

Cybercrime now dominates a significant part of daily practice: bank-helpdesk fraud, phishing, ransomware, doxing and unauthorised access cases require both technical literacy and classic procedural discipline.

The unresolved debate

Encrypted-phone litigation shows how national criminal procedure, cross-border cooperation and European law collide when massive datasets become central to serious organised-crime prosecutions.

Structure of the presentation

Three developments, one underlying question: how criminal justice preserves control over digital power.

AI in criminal justice

Use by courts, use by parties, and use by offenders.

Cybercrime 2.0

Dominant offence types and procedural frictions.

PGP phones

Admissibility of encrypted-communication data.

The common thread is the same throughout: digital criminal justice is becoming less about isolated computer offences and more about data environments. Courts must assess evidence that is technically complex, legally fragmented and often transnational.

The aim is a concise Dutch case study, with broader relevance for judges, prosecutors and defence lawyers working in EU criminal justice.

AI has entered Dutch criminal justice

AI appears in judicial work, legal submissions and offending methods.

01

Courts as users

Internal AI tools such as RechtspraakGPT support the court staff with non-sensitive tasks outside the judiciary domain – writing memos, policy papers, but not meant for tasks related to decision-making.

02

Parties as users

Lawyers and litigants increasingly submit AI-generated output as if it has expert value. Courts are developing a cautious response focused on verifiability, accountability and the legitimacy of the source.

03

Offenders as users

Deepfakes, automated phishing and synthetic identity fraud lower entry barriers and increase scale. AI changes the evidential landscape and the factual patterns that criminal courts must understand.

The judiciary as AI user

RechtspraakGPT and the EU AI Act make judicial AI a governance question, not merely an efficiency question.

Judiciary introduces RechtspraakGPT for its own employees

AI assistant supports employees with non-sensitive tasks outside the judicial domain

The Hague | December 10, 2025

As of today, all employees of the Judiciary can use RechtspraakGPT. This AI assistant helps with, among other things, creating, improving, and summarizing memos, policy papers, presentations, and other documents. RechtspraakGPT is expressly not intended for tasks related to judicial decisions, human resources, confidential documents, or personal data.

AI Act implications

- AI tools used to assist judicial decision-making fall within the EU AI Act's *high-risk* framework.
- For judicial users, AI literacy therefore means knowing both the tool's possibilities and its boundaries.

Source: https://www.rechtspraak.nl/organisatie-en-contact/organisatie/raad-voor-de-rechtspraak/nieuws/rechtspraak-introduceert-rechtspraakgpt-voor-eigen-medewerkers

AI output as evidence: the “synthetic expert” problem

Dutch courts are cautious when parties present AI output as if it were an authoritative source.

- AI-generated output as a claim to expertise without the institutional features that normally justify expert authority
- Courts ask whether the output is substantively reliable, whether a responsible human author can account for it, and whether the legal forum recognises the source as legitimate.
- The Dutch Bar and the CCBE have both issued guidance on responsible AI use in legal practice, stressing that AI may support lawyers but does not reduce their professional responsibility.

Tools embedded in controlled forensic or institutional workflows receive a different assessment. Hansken, ANPR systems and plagiarism tools are treated more favourably because human verification and institutional accountability surround the technology.

https://www.njb.nl/auteurs/arnoud-engelfriet/

Lesson from the prompt-and-temperature case

The procedural failure was deeper than a missing technical setting.

A lawyer submitted ChatGPT output in a dispute concerning a business plan. The court asked which prompt had been used and which **temperature setting** applied. The answers exposed that the production could not be reconstructed or verified.

What made the output fragile?

The wrong version of the document had been assessed, procedural materials had been loaded into the conversation, and the model generated legal conclusions aligned with the user's position.
The reliability problem concerned mandate, source selection and adversarial bias.

The practical lesson for courts

AI-based productions need a reproducible record: the documents used, the prompt sequence, the model context, the intended purpose and the human verification performed before submission.

Without that record, the court cannot test probative value.

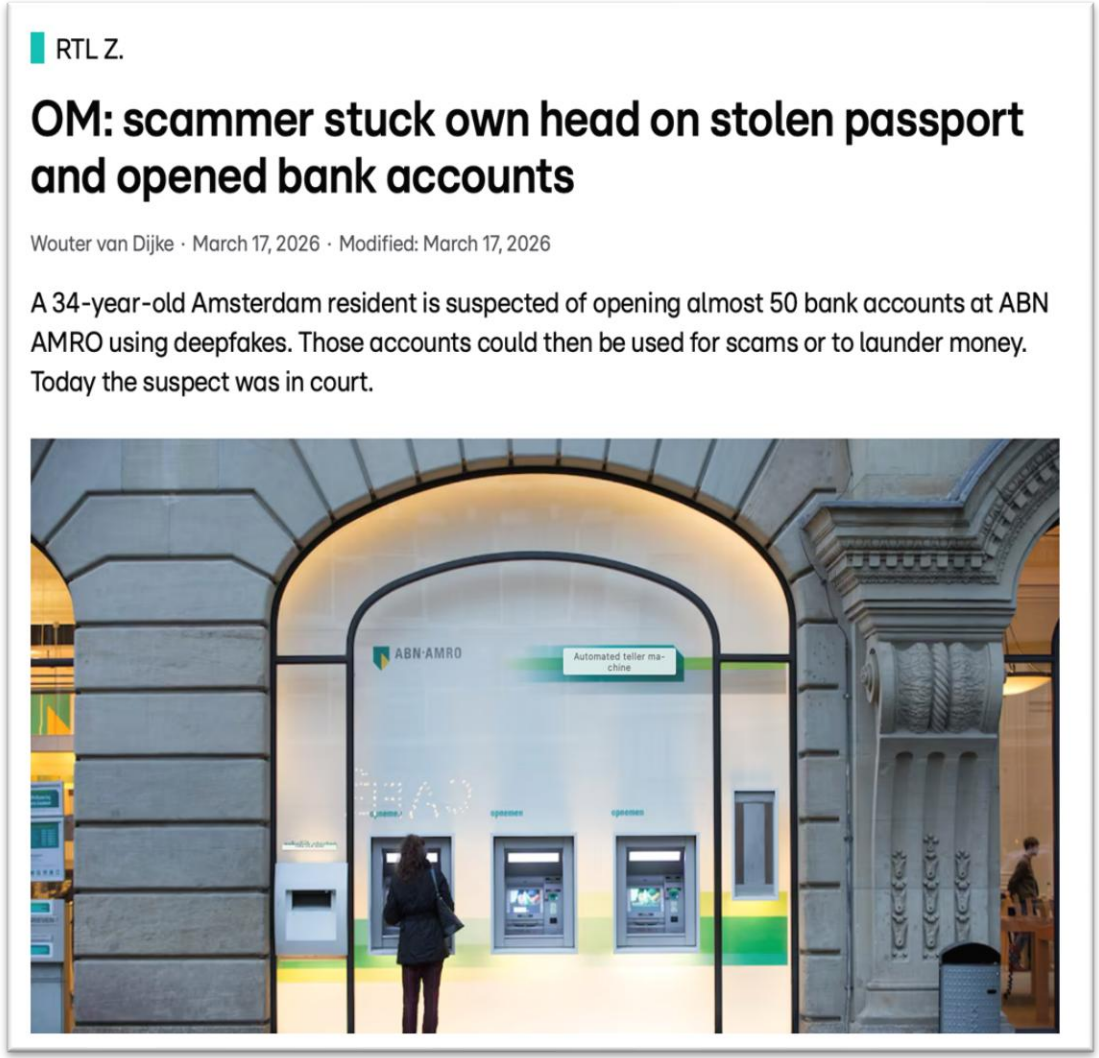
AI as an instrument of crime

The same technologies that assist legal work also expand criminal capacity.

Deepfake-enabled bank fraud

A pending Amsterdam case concerns the opening of 47 bank accounts in the Netherlands, Belgium and Italy through deepfake technology.

The significance lies in the attack on Know Your Customer controls: identity verification systems long treated as robust can be manipulated at scale when synthetic faces and documents are combined.



RTL Z.

OM: scammer stuck own head on stolen passport and opened bank accounts

Wouter van Dijke · March 17, 2026 · Modified: March 17, 2026

A 34-year-old Amsterdam resident is suspected of opening almost 50 bank accounts at ABN AMRO using deepfakes. Those accounts could then be used for scams or to launder money. Today the suspect was in court.

Press release of the court

Cybercrime is now mainstream criminal justice

Dutch data shows online criminality as a central volume problem, with a large hidden figure.

2.4m

victims of online criminality in 2024

15.7%

of the Dutch population aged 15+

16%

reported to the police

72%

faced cybercrime attempts in 2025

- Online fraud increased between 2022 and 2024, phishing remains the most visible entry point, and Dutch organisations reported a sharp rise in attacks during 2025.
- The courtroom sees only a selected part of the problem because reporting rates and attribution rates remain low.

Bank-helpdesk fraud and phishing

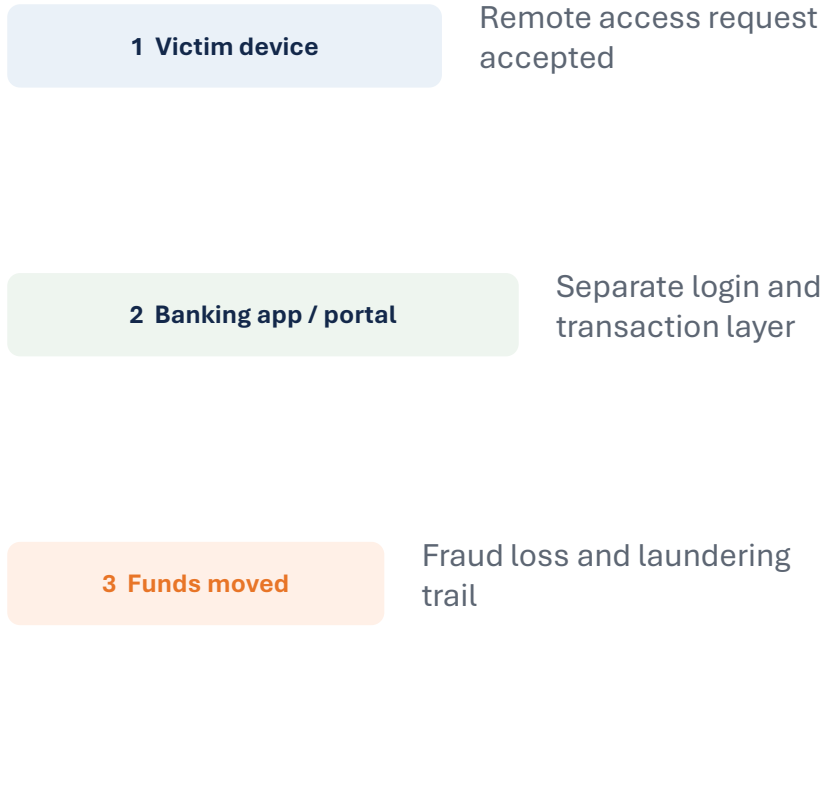
The legal analysis often turns on where access occurred and which system was actually entered.

Typical factual pattern

A victim is contacted by someone posing as a bank employee, persuaded to install remote-access software such as AnyDesk or TeamViewer, and then loses control over funds. The charges may include fraud, unauthorised access and identity-related offences.

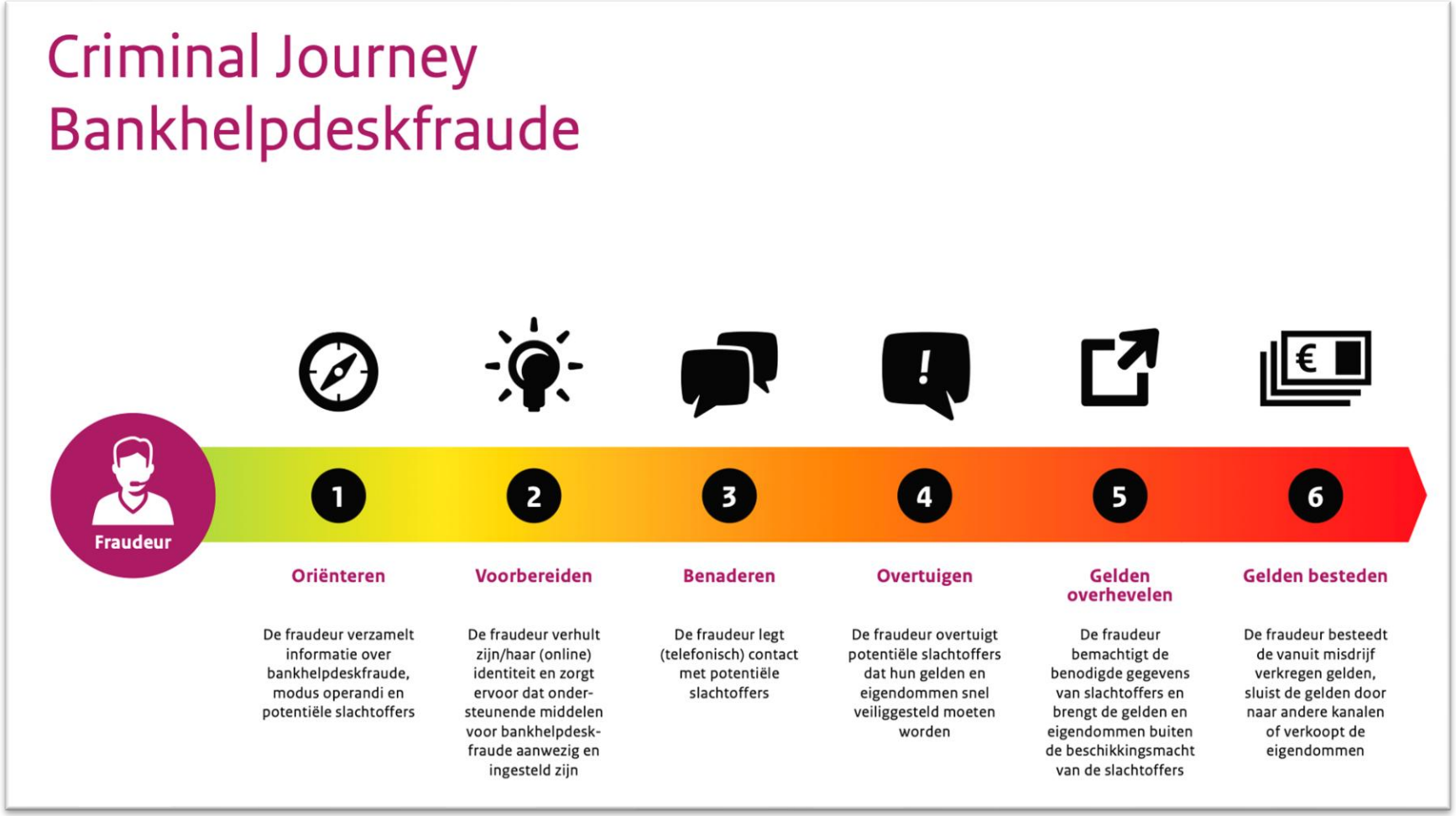
The charging problem

Dutch cybercrime case law stresses the need to distinguish access to the victim's device from access to the digital banking environment. These are separate technical events.
Installing a tool after deception does not automatically establish unauthorised entry into every later system.



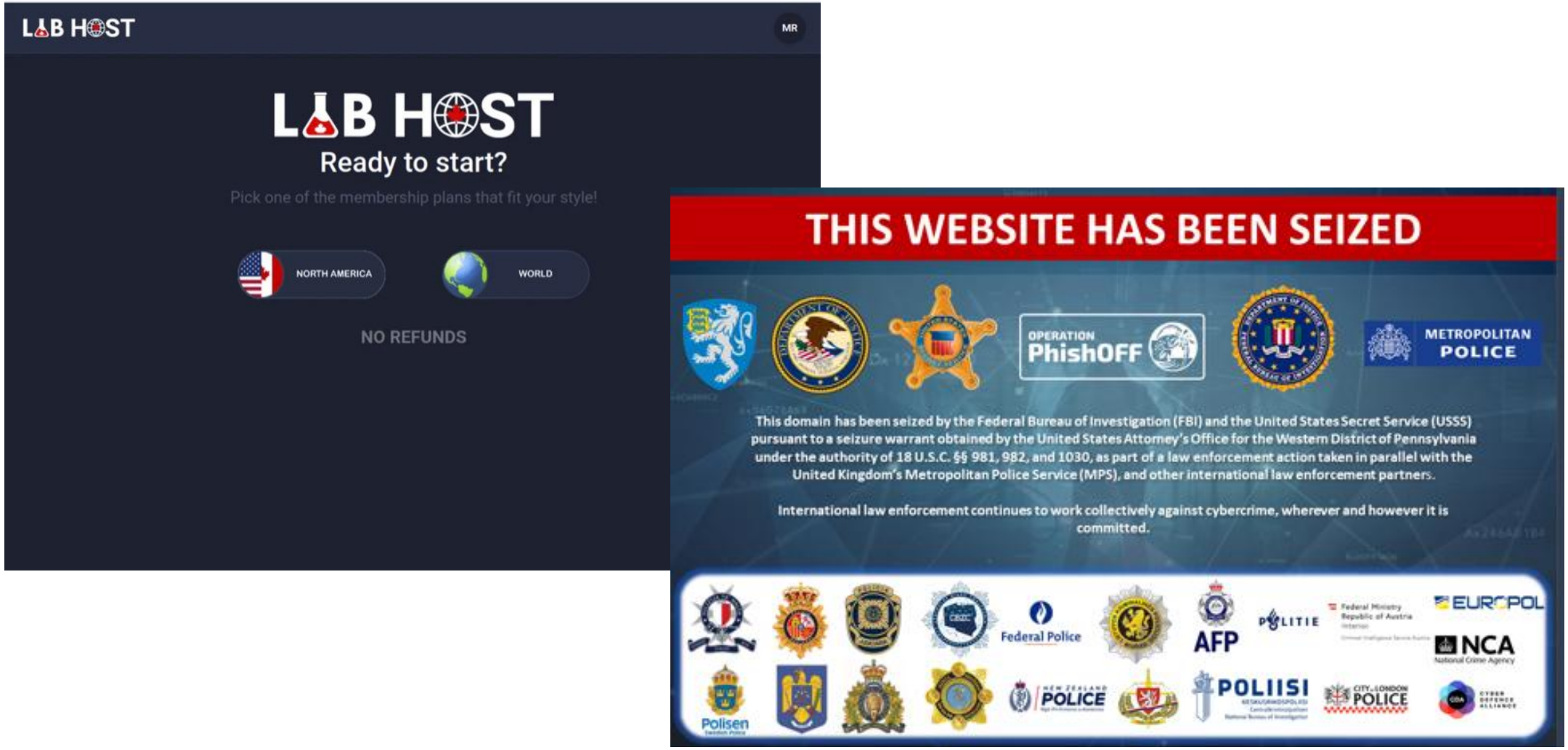
Bank-helpdesk fraud and phishing

The legal analysis often turns on where access occurred and which system was actually entered.



https://integraleaanpakonlinefraude.nl/attachment/entity/4369dac5-dff9-401b-b948-2cc7c79966e4

LabHost — Phishing-as-a-Service



LabHost — Phishing-as-a-Service

- LabHost was a global phishing-as-a-service platform offering **ready-made fake websites of banks, public bodies and platforms such as Netflix and Amazon.**
- For a monthly crypto fee, users could collect login details, bank data and credit-card information from victims.
- Operation PhishOFF dismantled the platform in April 2024 through cooperation between the UK, Europol, the FBI, the US Secret Service and 18 jurisdictions.
- The seized LabHost database allowed national authorities, including the Netherlands, to identify users and start prosecutions.
- In November 2025, the District Court of Mid-Netherlands issued the first Dutch conviction of a LabHost user, based on digital evidence linking him to phishing panels, servers, crypto payments and victim data.

ECLI:NL:RBMNE:2025:5658

Ransomware, doxing and unauthorised access

Cybercrime combines social harm, digital infrastructure and classic criminal-law concepts.

Ransomware and system disruption

Ransomware may paralyse airports, public-sector systems or prosecution services. Liability can combine unauthorised access, extortion and participation in organised criminal activity. The hardest practical issues are attribution, jurisdiction and recovery of infrastructure.

Doxing and physical risk

Article 285d of the Dutch Criminal Code covers obtaining and spreading personal data with the intent to cause fear or serious nuisance.

Online publication of photographs and address details can create immediate physical danger.

Unauthorised access as the workhorse provision

Article 138ab of the Dutch Criminal Code remains central across many cybercrime cases.
Precision in the indictment matters: what is the “automated work” for evidential purposes?
The device, application, server, cloud account, banking environment, or network infrastructure etc.

Procedural control over digital investigations

Searches of devices and datasets require judicial discipline at the front end of the investigation.

The Landeck line – C-548/21, CJEU

When the extraction or analysis of a smartphone or other digital device creates more than a limited interference with privacy, prior authorisation by an investigating judge becomes central.

In its judgment of 18 March 2025, the Dutch Supreme Court revised its case law on searches of electronic devices after **CG/Landeck**, distinguishing between *limited* and *more than limited* privacy intrusions, with prior judicial review required only for the latter.

Encrypted communication platforms

EncroChat and Sky ECC: operational context

The legal debate is inseparable from the scale of the operations.

EncroChat

A European encrypted-communication network with approximately 50,000 users in early 2020, including around 12,000 in the Netherlands. In operation 26Lemont, French and Dutch authorities used a Joint Investigation Team and a Trojan horse to intercept real-time messages over several weeks.

Estimated 115 million messages intercepted

Sky ECC

A Canadian provider of encrypted smartphones and the Sky ECC application, with about 70,000 users worldwide. Belgian and Dutch services gained live access to messages in 2021, followed by raids, arrests and the dismantling of the network.

Hundreds of arrests and major asset seizures followed

EncroChat & Sky ECC — operationele kerngetallen

Stand juni 2023 (EncroChat) en maart 2021 + 2026 (Sky ECC)

	EncroChat	Sky ECC
Operatienaam (NL)	26Lemont[1]	26Argus[2]
Operatienaam (FR/EU)	Emma 95[3]	—
Operatienaam (BE)	—	Operatie Sky[2]
Periode interceptie	1 apr — 13 jun 2020[1]	feb — mrt 2021 (3 wkn live)[4]
JIT-partners	FR, NL[1]	FR, NL, BE[2]
Aantal gebruikers	ca. 60.000 wereldwijd[3] [5] (12.000 NL)	70.000 abonnees[4] 171.000 toestellen
Onderschepte berichten	> 115 miljoen[3]	ca. 1 miljard[6] (≥ 500 mln ontsleuteld)
Aanhoudingen	6.558[3] (197 High Value Targets)	honderden NL[2] + 888 BE[4] (eerste jaar)
Inbeslagname / bevriezing	bijna € 900 miljoen[3]	€ 4,5 miljard aan drugs (BE)[4]
Veroordelingen	7.134 jaar gevangenisstraf[3]	honderden strafzaken NL[2]
Voorkomen moorden	—[3]	114 (Europol)[4]

[1] HR 14 april 2026, ECLI:NL:HR:2026:650 · [2] OM, Distributeurs cryptotelefoons Sky ECC aangehouden, 31 jan 2025 · [3] Europol & Eurojust, persconferentie Lille, 27 juni 2023 · [4] VRT Nieuws, 5 jaar na 'kraak van de eeuw', 24 feb 2026 · [5] Schermer & Oerlemans, NJB 2023/2611 · [6] D. Hiroux, VRT Nieuws, 6 april 2021

EncroChat — drie jaar na de hack

Wat is er in beslag genomen?

VERMOGEN

Cash

€ 739,7 mln

Bevroren tegoeden

€ 154,1 mln

Totaal

€ 900 mln

DRUGS

Cocaïne

103,5 ton

Cannabis

163,4 ton

Heroïne

3,3 ton

Synthetische drugs

30,5 mln pillen

WAPENS & TRANSPORT

Vuurwapens

923

Munitie

21.750 stuks

Explosieven

68

Voertuigen

971

Vaartuigen / vliegtuigen

83 / 40

Onroerend goed

271 panden

Bron: Europol & Eurojust, persconferentie Lille 27 juni 2023, 'Dismantling encrypted criminal EncroChat communications leads to over 6.500 arrests and close to EUR 900 million seized' — cumulatieve cijfers JIT-partners en deelnemende derde landen.

Encrypted communication platforms

PGP phones created a new evidential category: massive, intercepted, cross-border conversational datasets.

EncroChat and Sky ECC were designed around secrecy: encrypted messaging, modified devices, remote wiping, disabled hardware features and subscription-based access.

Why this became legally explosive

The operations did not produce a few messages from a single suspect. They generated enormous datasets across many users and jurisdictions.

That scale changed the admissibility discussion: defence lawyers requested access to underlying materials, prosecutors relied on international cooperation, and courts had to define the limits of trust in foreign investigative acts.

The core legal question

How far may a Dutch court rely on evidence obtained through foreign authorities, especially where the defence cannot examine every technical step of the interception?

The discussion involves inter-state trust principle, judicial authorization and the right to a fair trial.

The main defence challenges

The recurring arguments focus on access, legality, fair-trial rights and attribution.

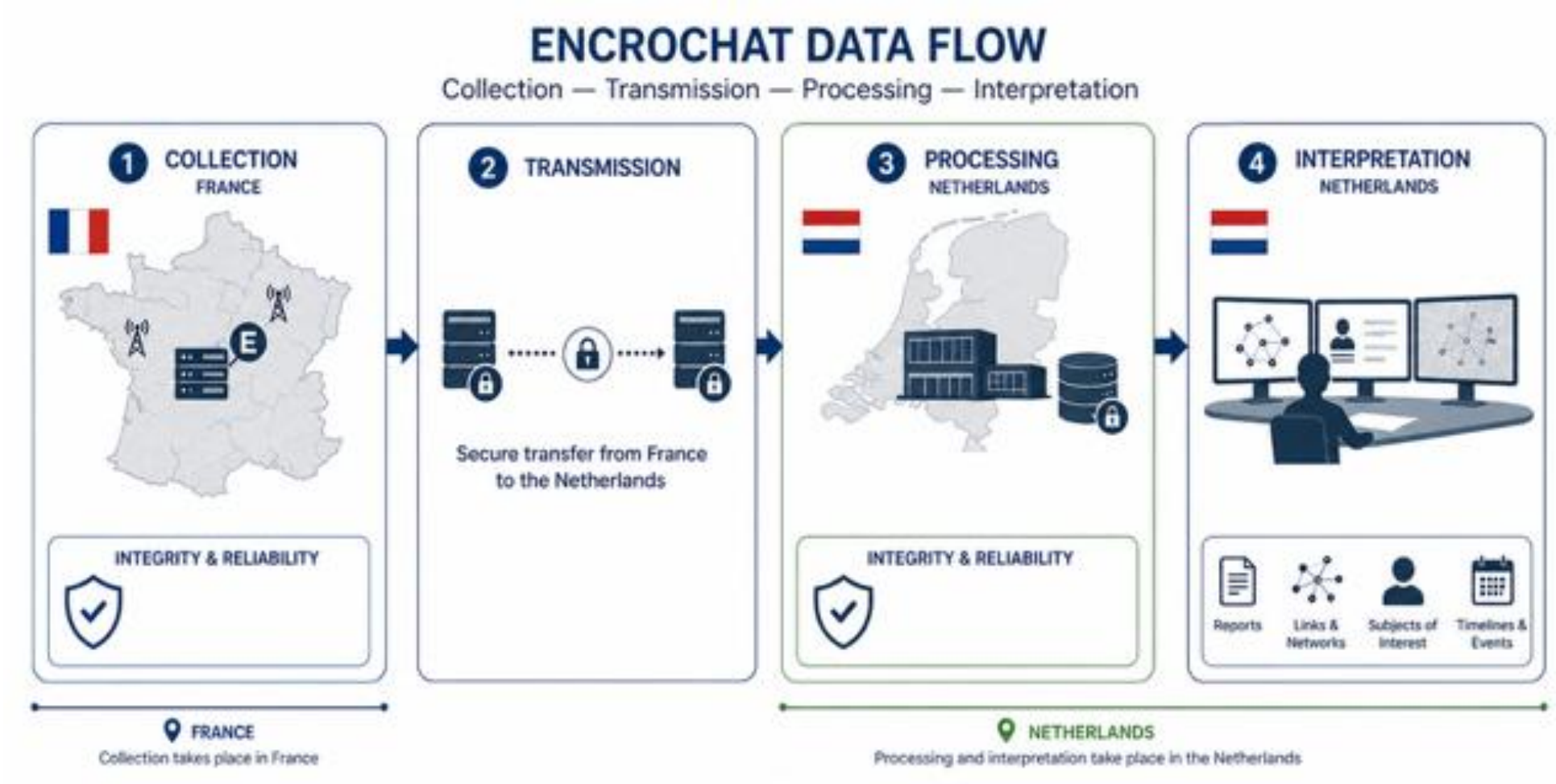
The general defence arguments that EncroChat data should be excluded:

1. it is allegedly **unlawfully obtained and processed**,
2. its **reliability can not be properly verified**, and
3. the defendant lacks **effective legal protection**.

ECLI:NL:GHSHE:2025:2301: the defence wanted the Dutch court to assess the legality and reliability of the data under Dutch law, to clarify whether the interception took place inside or outside the JIT, whether targeted interception was possible, and whether sufficient judicial oversight existed.

Joint **D**efense **T**eam – a collaborative network of experienced criminal defence lawyers from several European countries.

Admissibility challenges



Interpretation challenges

- Attribution of a specific account to an individual
- Interpretation of the content of communications
- Identification of communication counterparts and questioning as witnesses

The jurisprudential line

Dutch case law moved from inter-state trust toward a refined EU-law discussion, while preserving the JIT basis.

2022

Ennetcom

Foreign-obtained encrypted communication data may be used if the fairness of the trial is preserved.

2023

EncroChat / Sky ECC

The JIT context and the Dutch investigating judge's authorisation sustained the use of the data.

2024

CJEU C-670/22

Article 31 of the EIO Directive protects individual rights as well as state interests.

2026

HR 14 April 2026

The individual-rights reading was accepted, while Article 31 was held inapplicable to JIT exchange.

Hoge Raad 14 April 2026: the central holding

The Supreme Court adjusted the reasoning, yet preserved the admissibility framework for JIT-based EncroChat evidence.

What the defence argued

Relying on the CJEU's 2024 ruling, the defence argued that Article 31 of Directive 2014/41/EU protected individual rights and required further inquiry into the French interception. Requests included raw source data, the Dutch research file and witnesses from the French side, Europol and Eurojust.

What the Supreme Court decided

The Court accepted that Article 31 also protects individuals. It then held that the provision did not govern this evidence because the material was exchanged through a Joint Investigation Team.

Article 3 of the directive excludes JIT exchange from the directive's scope. The March 2020 authorisation by the Dutch investigating judge remained procedurally decisive.

Current position and open issues

The Dutch framework is relatively stable for JIT cases, while other routes remain legally sensitive.

For the majority of Dutch EncroChat cases, the inter-state trust principle, the JIT structure and the investigating judge's authorisation currently sustain admissibility.

Where uncertainty remains

Cases outside the JIT architecture require separate analysis. Where an European Investigation Order was used, the directive applies directly and notification questions under Article 31 may have practical consequences.

Current position and open issues

What to watch

The pending Prudniez reference from the French Cour de cassation may further develop the EU-law dimension. A future CJEU ruling could affect the relationship between notification, individual rights and evidential consequences in encrypted-phone investigations.

C-625/25, Prudniez:
French reference on effective judicial protection in cross-border digital investigations involving Sky ECC.

Pending cases:

Before the CJEU
- **C-564/25, C-565/25 and C-566/25**: Europol liability concerning Sky ECC, EncroChat and Exclu.

Before the ECtHR
- **Silgir vs Germany (no. 27618/21)**: Article 5 and Article 8 ECHR issues, concerning liberty and private life.
- **Hoeven vs Netherlands (no. 15038/24)** : Article 6 ECHR issue, concerning the right to a fair trial.

Closing synthesis

Digital criminal justice requires technical literacy, legal precision and visible human responsibility.

1	**AI changes authority**	Courts must distinguish useful technological assistance from unsupported claims of expertise. Verification and accountability determine legal value.
2	**Cybercrime changes volume**	Online offending has become a mainstream caseload, with bank fraud, phishing, ransomware, doxing and unauthorised access at the centre of practice.
3	**Encrypted-phone cases change procedure**	EncroChat and Sky ECC show that admissibility now depends on cross-border cooperation structures, judicial authorisation and control over large datasets.

Questions?

ARTIFICIAL INTELLIGENCE

Impact on Investigations and Handling in Court

Rainer Franosch - Deputy Director-General for Criminal Law

Ministry of Justice of the German Federal State of Hesse

#DIGITALISATION and #AI in Criminal Justice · ERA Conference · Zagreb · 15–16 June 2026

Funded by the European Union. Views and opinions expressed are however those of ERA only and do not necessarily reflect those of the European Union or European Commission.
Neither the European Union nor the granting authority can be held responsible for them.

HESSEN

Hessisches Ministerium der Justiz und für den Rechtsstaat

SETTING THE SCENE

Introduction to AI in Criminal Proceedings

Definition

Artificial intelligence refers to computer systems capable of performing tasks that ordinarily require human intelligence.

RELEVANCE IN CRIMINAL JUSTICE

Enhanced data analysis

Greatly enhances the capacity to analyse large and complex datasets.

Forensic & prognostic support

Assists in forensic investigations, judicial prognostic assessments in criminal law and predictive policing.

Legal assistance

Supports legal work - e.g. analysis & summarization of case law.

New legal questions

Raises questions about evidence admissibility and defendants' rights.

AI IN CRIMINAL INVESTIGATIONS AND PROCEEDINGS

Where AI Enters the Investigation

General preliminary investigations

- Threat analysis & prioritization (cybercrime, money laundering…)
- AI-generated criminal complaints (fraud prevention…)
- Situation & sentiment assessment (media analysis…)
- Data analysis & pattern recognition (serial-offence detection…)

Technical support in investigations

- Speech recognition, analysis & translation (encrypted chats…)
- Image & video analysis (facial recognition, deepfakes…)
- Social-media monitoring & OSINT analysis (web crawlers, bots…)
- Generation of images & voice imitation (undercover operations…)
- Integration of relevant data (HessenData…)
- Use of third-party AI results (e.g. Klette case…)

AI IN CRIMINAL INVESTIGATIONS AND PROCEEDINGS

Analysing Data & Assessing Risk

Analysis of large data volumes

- Detection & categorization of files (IT forensics…)
- Pre-evaluation of images and videos (child-abuse imagery, juvenile pornography…)
- Communication & network data analysis (chats, emails…)
- Financial data & transaction analysis (account data, blockchain…)

Judicial prognostic assessments

(as distinct from predictive policing)

- Risk of violence by individuals & overall threat assessment (police…)
- Criminal liability of statements & preliminary evaluation (hate speech…)
- Risk of flight & reoffending (grounds for detention…)
- Risk of recidivism (probation, preventive detention…)

AI IN CRIMINAL INVESTIGATIONS AND PROCEEDINGS

AI as Legal Assistance

Speech recognition & translation

Legal assistance and complaint chatbots.

Analysis & summarization of case law

Research support such as Beck-chat.

Document analysis & information integration

Form-filling and “robo-judge” drafting support.

Deadline tracking & statistics

Automated reminders and case statistics.

CASE STUDY

Predictive Policing in Germany

Implementation

Deployed across various German federal states.

Challenges

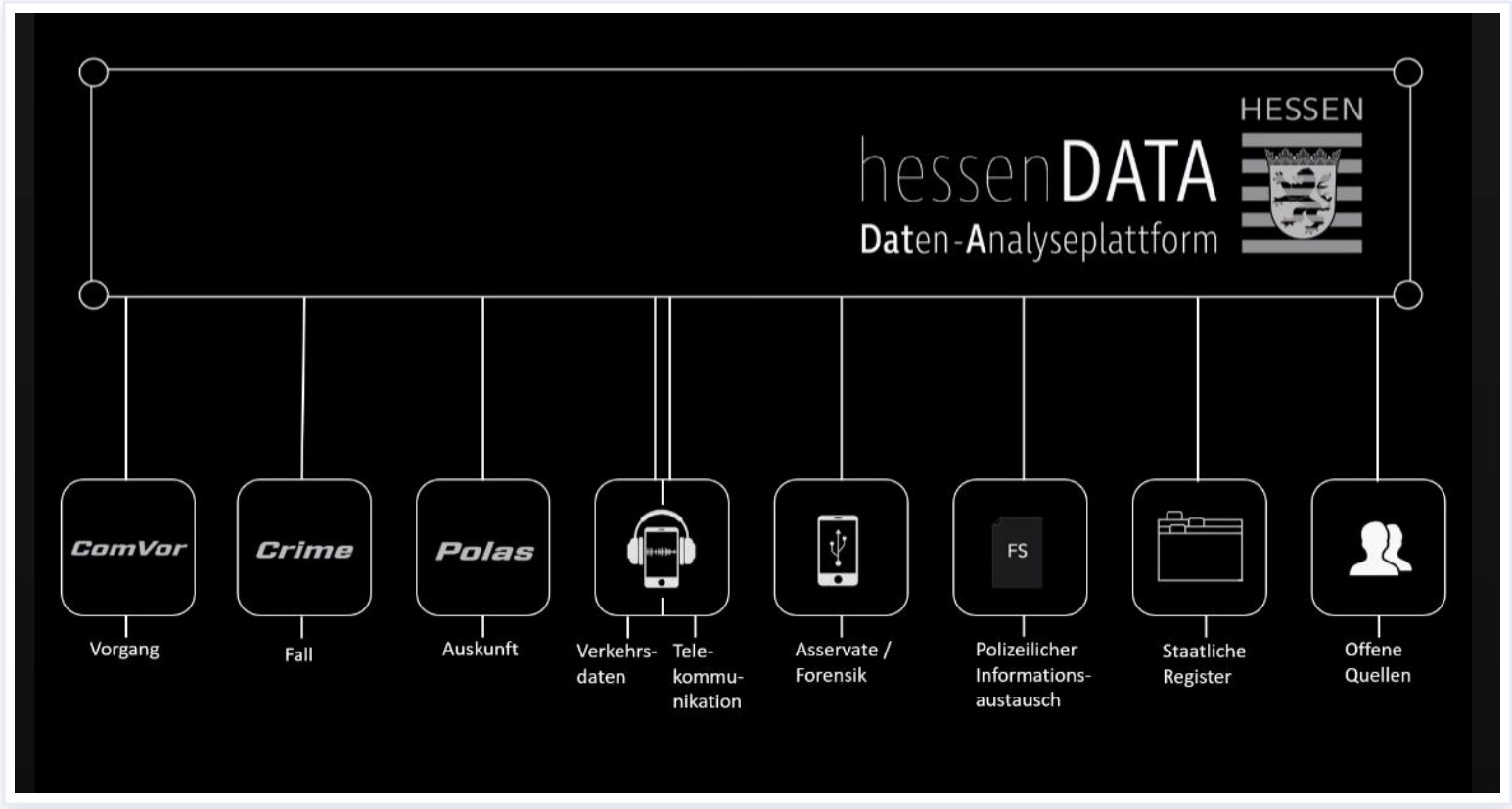
Data-protection compliance and concerns about algorithmic bias.

Open debate

Effectiveness and legality remain actively contested.

CASE STUDY · HESSENDATA (PALANTIR) - 1 / 7

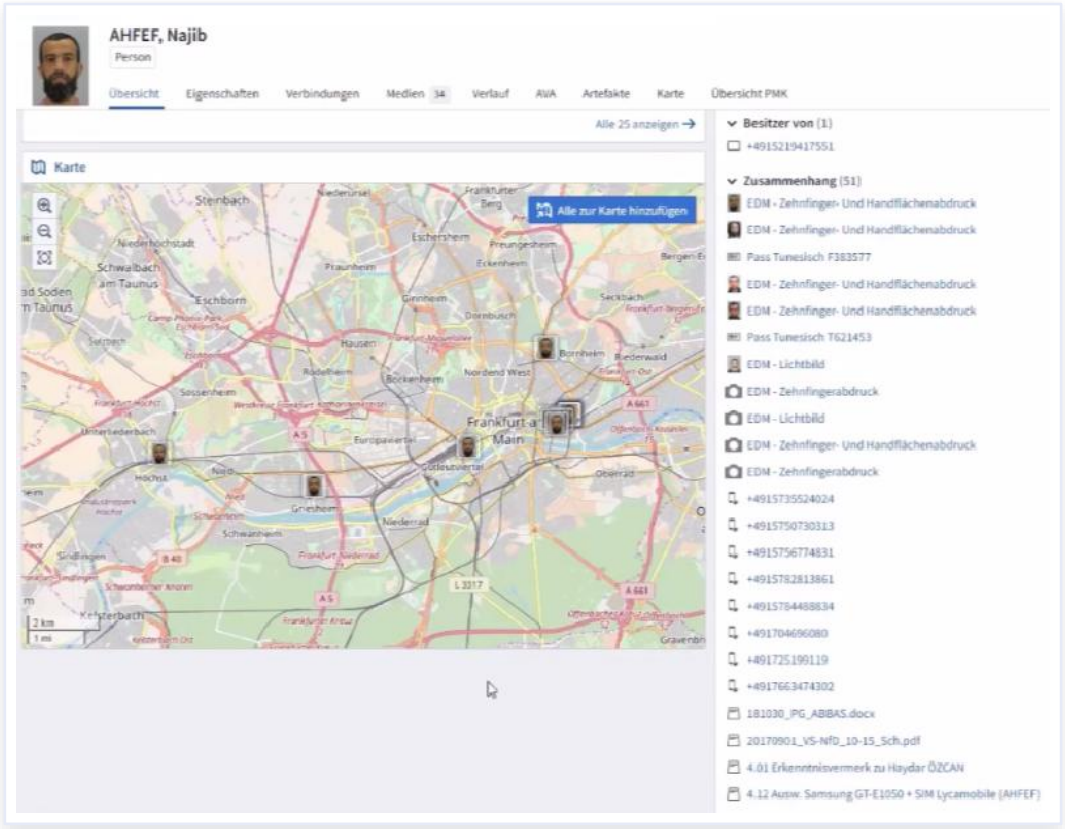
Cross-Database Analysis in Practice



Central analysis dashboard - the HessenDATA platform (built on Palantir).

CASE STUDY · HESSENDATA (PALANTIR) - 2 / 7

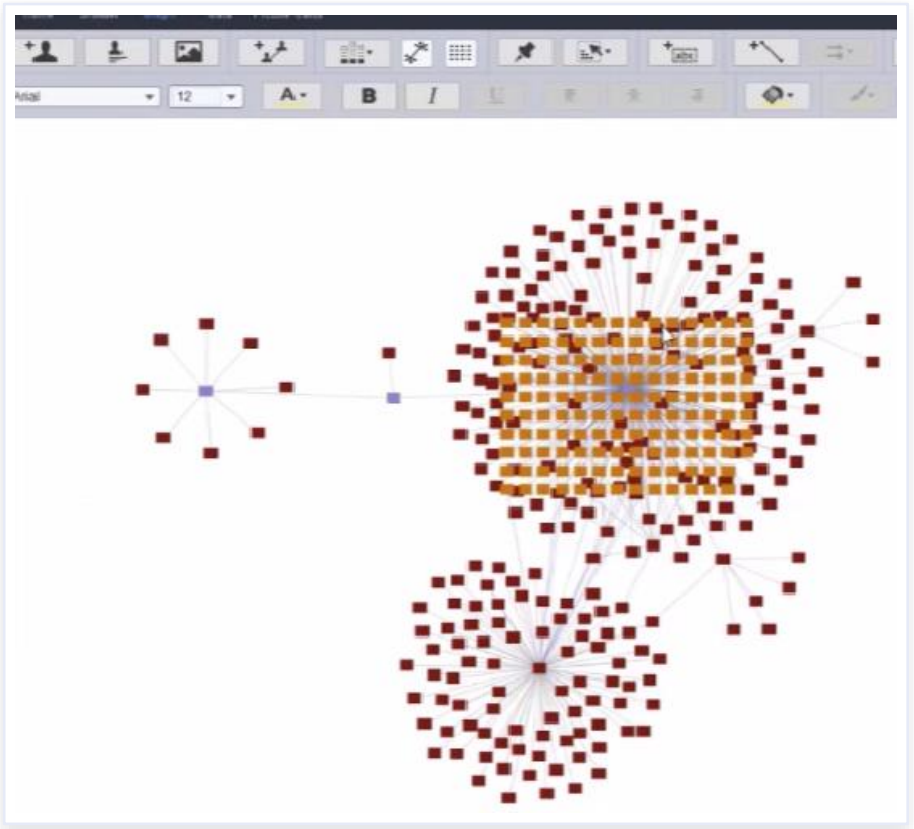
Cross-Database Analysis in Practice



Geospatial view: case locations linked on an interactive map.

CASE STUDY · HESSENDATA (PALANTIR) - 3 / 7

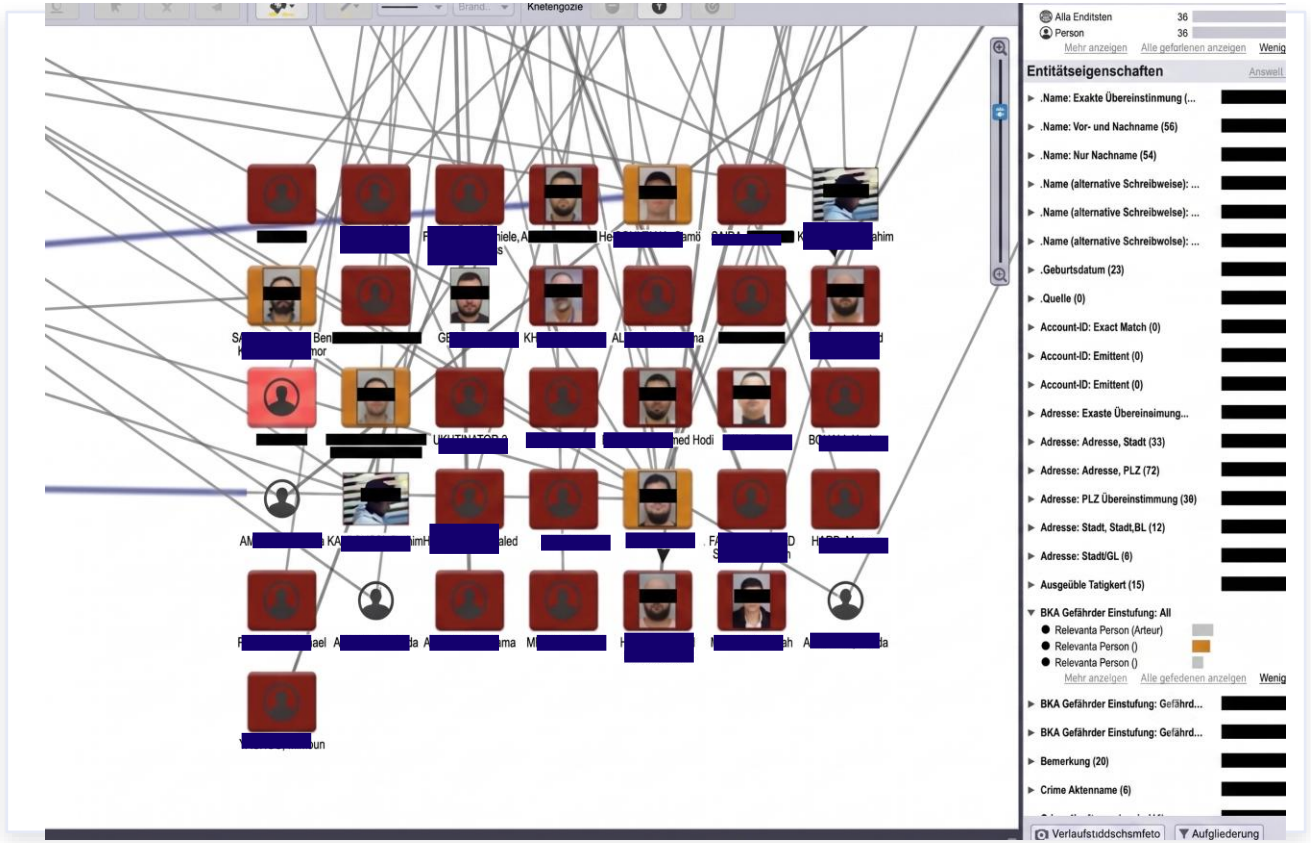
Cross-Database Analysis in Practice



Link analysis: entity-relationship network across data sources.

CASE STUDY · HESSENDATA (PALANTIR) - 4 / 7

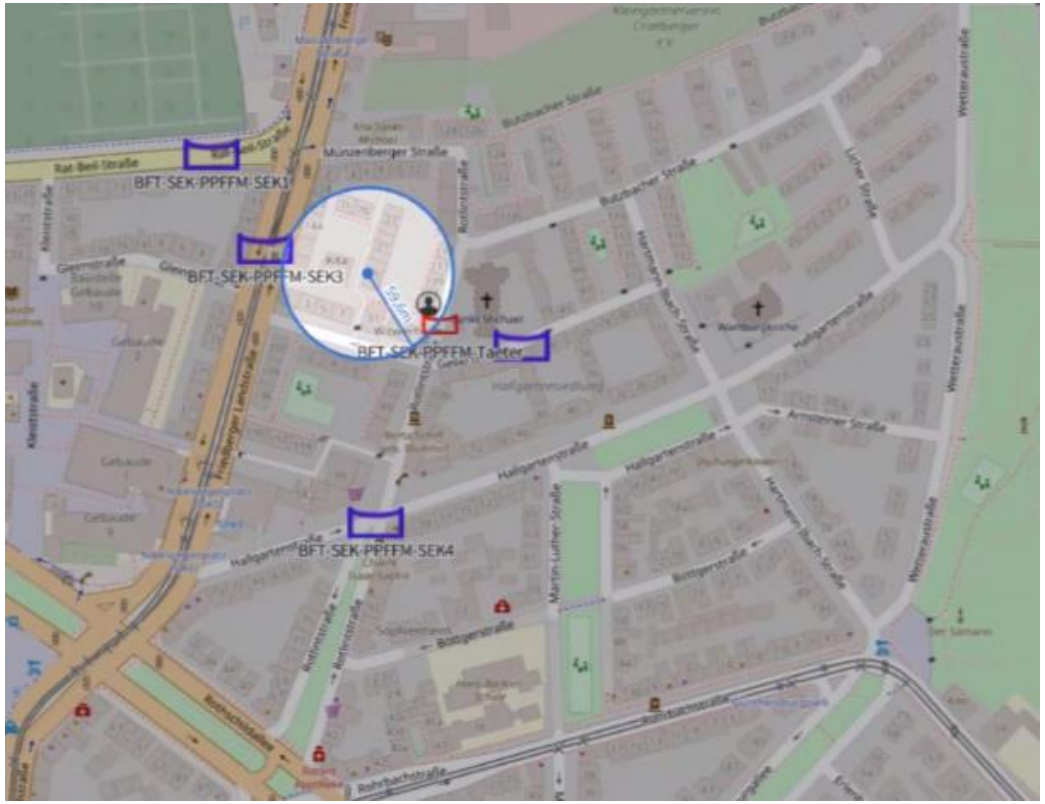
Cross-Database Analysis in Practice



Combined media grid and relationship analysis.

CASE STUDY · HESSENDATA (PALANTIR) - 5 / 7

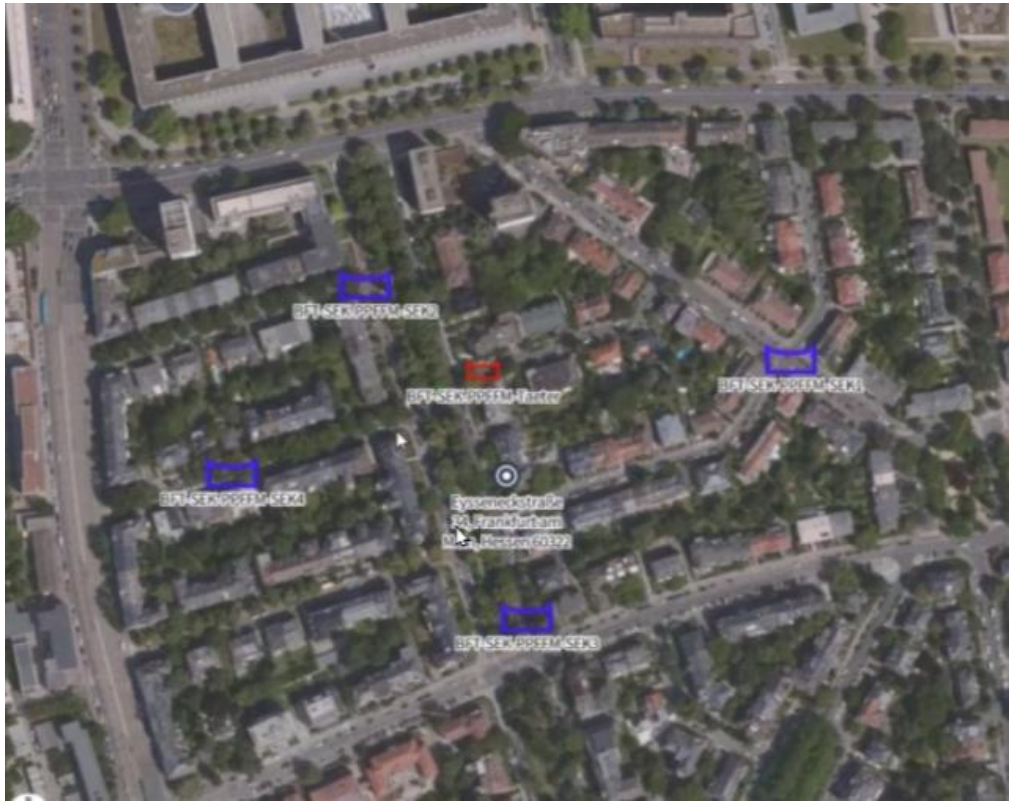
Cross-Database Analysis in Practice



Location radius and geofencing around points of interest.

CASE STUDY · HESSENDATA (PALANTIR) - 6 / 7

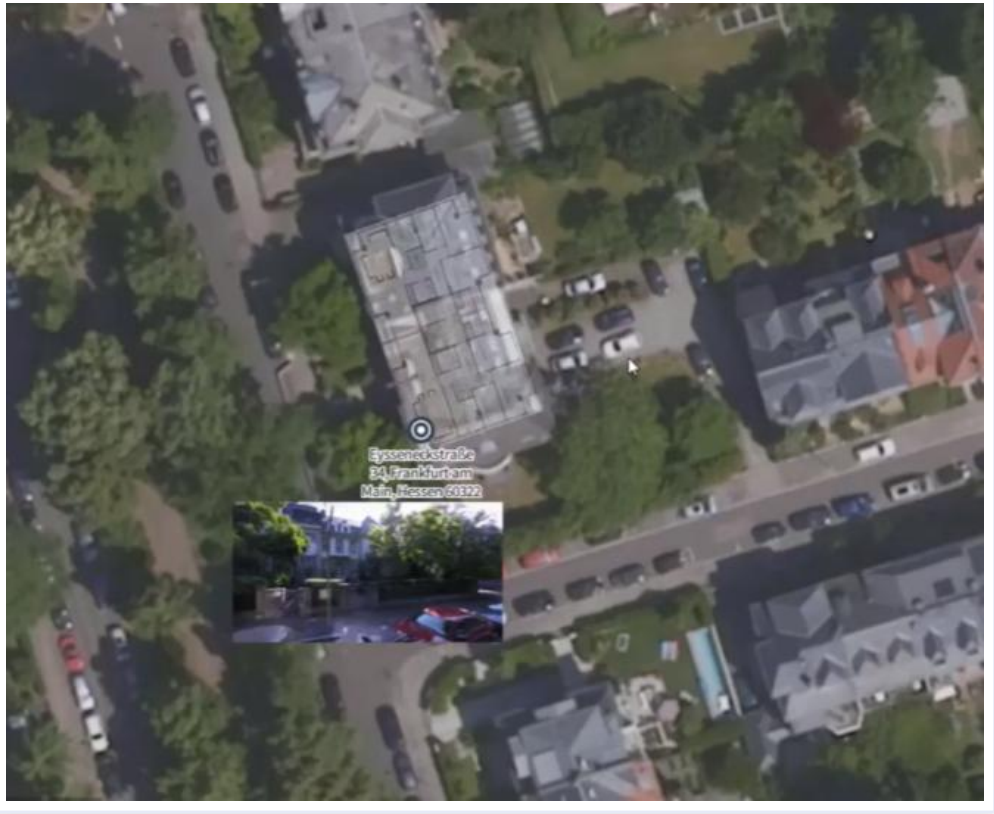
Cross-Database Analysis in Practice



Connected locations plotted across the city.

CASE STUDY · HESSENDATA (PALANTIR) - 7 / 7

Cross-Database Analysis in Practice



Aerial / satellite view of a location of interest.

CASE STUDY - WIESBADEN RECKLESS-DRIVING CASE

VR and AI Used in a Murder Trial

SPIEGEL Panorama

Prozess in Wiesbaden

Tödlicher Unfall – Raser zu lebenslanger Haft verurteilt

Er raste mit Tempo 130 durch die Innenstadt: Ein 25-Jähriger ist in Hessen des Mordes schuldig gesprochen worden. Vor Gericht hatte der Mann Reue gezeigt.

29.11.2023, 20.22 Uhr

Scene of the fatal collision, Wiesbaden

WIESBADEN RECKLESS-DRIVING CASE

VR and AI Used in a Murder Trial

The facts of the case

- October 2022: a 24-year-old drove at 120 km/h in a 50 km/h zone in Wiesbaden.
- He ignored a red light and fatally crashed into another vehicle.
- The victim was a 55-year-old woman.
- The driver had a prior history of traffic violations.
- Trial held in 2023 at Wiesbaden Regional Court.
- Charged with murder under **§ 211 StGB**.
- The court found he acted with conditional intent (bedingter Vorsatz).

120 / 50

km/h driven in a 50 km/h zone

§ 211

Murder - German Criminal Code

Life

Outcome: life imprisonment

WIESBADEN RECKLESS-DRIVING CASE

How VR and AI Shaped the Verdict

AI-assisted VR reconstruction

The court rebuilt the crime scene in 3D, enabling an immersive view of:

- Driving path and speed
- Visibility and timing
- The possibility to prevent the crash

Assessing intent

AI-assisted VR helped the court weigh intent and foreseeability.

A German first

Pioneering use of VR in German criminal justice.

Evidentiary clarity

Enhanced spatial understanding and clarity of the evidence.

Legal classification

Reinforced classifying extreme speeding as murder.

Precedent

Sentencing set a strong precedent for reckless-driving cases.

WIESBADEN CASE - FROM THE WRITTEN JUDGMENT

“Getting into the Car”: VR in the Verdict

> In the second step, according to witness “police officer 6 (PHK 6)”, it was necessary to select the correct technology to capture the images so that a realistic rendering of the perspectives could be achieved. A problem was that ordinary cameras have a **static viewing angle**, which cannot be changed afterward and thus only allows a limited representation of the actual perspective. It was crucial to create the possibility of virtually "getting into the car" and seeing the actual positions. The solution was the use of **"virtual reality" (VR)**, which here essentially meant recording with **360° cameras**, so that one could subsequently select the respective viewing angle oneself. (…) To obtain an even more realistic impression of the visibility conditions, the court could follow in real time on a screen what witness PHK 6 saw in the VR headset he was wearing. First, the view from the perspective of the Mercedes driver was shown - initially at **70 km/h** (original speed), and then at **140 km/h** (double playback speed), viewed multiple times. Witness PHK 6 moved his gaze on the court's instructions and at the request of other parties, thereby steering the perspective displayed on the screen. This confirmed the impression already gained from the VLC version, while conveying a more realistic perception.
>
> *- Excerpt from the court's written judgment*

CASE STUDY · AI IN THE COURTROOM

“Im Namen des Volkes” - The Written Judgment

Landgericht Darmstadt

Geschäftsnummer

3 KLs 200 Js 2761/24
(2/24)

Zur Geschäftsstelle
gekommen am: 23. Jan. 2025

IM NAMEN DES VOLKES
URTEIL

In der Strafsache

g e g e n [redacted]

zuletzt ohne festen Wohnsitz,
z. Zt. JVA Weiterstadt,
ledig (verlobt), deutscher Staatsangehöriger

w e g e n sexuellen Missbrauchs von Kindern

Excerpt from the court's written judgment (“In the name of the people - Judgment”).

CASE STUDY · AI IN THE COURTROOM

Forensic & Investigative Documentation

Bundeskriminalamt

Bundeskriminalamt (Federal Criminal Police Office)

BETREFF Ermittlungen wegen schweren sexuellen Missbrauchs von Kindern
Hier: Authentifizierung von Bild- und Videodaten

BEZUG Untersuchungsanträge des PP Darmstadt vom 02.04.2024 und 26.04.2024, Az. ST/0044172/2024

Tabelle 8: Liste der relevanten Metadaten der eingereichten Bilddateien Nr. 4-7, sowie für ein Referenzbild (IMG_20240429_110034.jpg), welches mit dem eingereichten Mobiltelefon A aufgenommen wurde.

Beschreibung	IMG_20220618_215537_291.jpg	IMG_20220618_215537_404.jpg	IMG_20220618_215537_573.jpg	IMG_20220618_215537_751.jpg	IMG_20240429_110034.jpg
ImageWidth	6560				
ImageHeight	3028				
EncodingProcess	Baseline DCT, Huffman coding				
BitsPerSample	8				
ColorComponents	3				
YCbCrSubSampling	YCbCr4:2:0 (2 2)				
Model	Mi Note 10 Pro				
Orientation: Rotate	180	180	270 CW	90 CW	Horizontal
ModifyDate [MESZ]	2022:06:18 21:44:26	2022:06:18 21:49:27	2022:06:18 21:45:51	2022:06:18 21:40:00	2024:04:29 11:00:37
YCbCrPositioning	Centered				
ISO	2458	2642	2382	2385	148
ExposureProgram	Program AE				
Fnumber	2.0				
ExposureTime	1/11	1/10	1/10	1/13	1/60
Exif_0x9999	"mirror":true,"sensor_type":"front","Hdr":"off"				
SensingMethod	Not defined				
SubSecTime	266879	480441	272532	804955	833845

CASE STUDY · AUTHENTIC EVIDENCE CHALLENGED

“The Video Was AI-Generated” - A Defendant's Claim

The case

Criminal proceedings concerning the sexual abuse of a child.

THE DEFENDANT'S CLAIM

An incriminating video - found on his mobile phone and showing him engaging in sexual acts with his three-year-old biological daughter - had, he claimed, been **artificially generated using AI**.

He asserted that the video did not depict a real event.

CHILD-ABUSE CASE - FROM THE WRITTEN JUDGMENT

Why the Court Rejected the “Deepfake” Claim

> The fact that video file no. 1 was **not artificially generated using AI** follows, in the court's view, from **expert witness K's convincing statements**, according to which the **metadata of video file no. 1 rules out artificial generation**. Furthermore, the recording position of the video - and the fact that it was recorded only **47 minutes** before video files no. 2 and no. 3, likewise found on the defendant's mobile phone - indicate that this video must also have been recorded by the defendant.
>
> *- Excerpt from the court's written judgment*

CHILD-ABUSE CASE - THE SENTENCE

The Outcome

7 years

Total term of imprisonment

Convictions

The defendant was sentenced to a total term of imprisonment of seven years for aggravated sexual abuse of children with child-pornography intent in two cases - each in conjunction with sexual abuse of wards and with the production of child-pornography content - and, in one further case each, for third-party possession of child-pornography content and possession of child-pornography content.

CHILD-ABUSE CASE - THE EXPERT'S REASONING

Why the Video Could Not Have Been AI-Generated

> When asked whether it would theoretically be possible to create the videos using AI, the expert explained that, in theory, it is possible to generate a video synthetically - but this would require **suitable training material: images of a person with a similar appearance**. Here, a particularly notable feature is the penis shown in the videos, due to implants located beneath the glans; this **distinctive feature makes synthetic generation even harder without corresponding original image material**. The real crux, however, is that the AI-generated video would have needed to be compressed into the file format of the device - specifically the **Xiaomi Mi Note 10 Pro** - which would require an extremely high level of IT expertise; the expert stated that even he himself would not be capable of doing this. Moreover, an AI-generated video would only produce **random noise, not the systematic noise** present in the examined files. The expert therefore concluded that the videos **could not have been generated using AI**.
>
> *- Expert witness, as recorded in the judgment*

LESSONS LEARNED

The “Liar's Dividend”

The liar's dividend

Casting doubt on authentic evidence is as serious a courtroom threat as fabrication itself.

Authentic, dismissed as fake

Defendants increasingly try to dismiss authentic recordings as possible deepfakes.

Demand a factual foundation

Courts should require a factual basis before entertaining such challenges - yet in this case questioning was allowed though the defence offered no support for its AI-manipulation theory.

Detection is contested

Expert evidence is the pivot point, but deepfake detection is genuinely unreliable - with documented performance collapse on unseen, real-world fakes.

WHEN GENUINE EVIDENCE IS CALLED A “DEEPFAKE”

United States v. Reffitt

D.D.C., No. 21-cr-00032 - the first January 6 trial and an early appearance of the deepfake defense

WHAT HAPPENED AT TRIAL

1. A genuine 360° helmet-camera video of the defendant at the Capitol was admitted on direct examination - with no defence objection.
2. On cross-examination, defence counsel asked the FBI analyst about deepfakes and suggested the footage could have been AI-manipulated.
3. The prosecution objected; the court asked for a good-faith basis. Counsel offered none beyond an intention to ask whether exhibits were altered - and was allowed to continue.
4. The analyst confirmed no reason to think the video was fake. Defence argued “deepfake” at closing anyway. The jury convicted on all five counts.

THE CAUTIONARY POINT

0

items of evidence ever offered to support the AI-manipulation theory

5 / 5

counts of conviction

Real evidence was put in doubt at no cost - the essence of the “liar's dividend.”

Source: A. Mitchell, “Deepfaked Evidence,” Berkeley Technology Law Journal (2025); trial transcript, U.S. v. Reffitt, No. 21-cr-00032 (D.D.C.).

FROM AN EARLY DEEPFAKE-DEFENSE CASE TO COURTROOM PRACTICE

Five Takeaways for Bench and Prosecution

1 Low bar, big gap

Sufficiency-level authentication lets manipulation be raised without any showing that it occurred.

2 Good faith needs teeth

Requiring a basis helps only if a bare intention to ask is not treated as enough to proceed.

3 Ready the examiner

Forensic witnesses should affirm that media shows no indicia of synthesis - not merely describe it.

4 A graduated burden

Proposed U.S. FRE 901(c): an objection needs a plausible basis; then authenticity is proven to a higher bar.

5 AI literacy first

No rule works unless judges and counsel grasp what generative AI can and cannot do.

⚠ The bottom line

As fakes grow familiar, the guilty can discredit real evidence by merely invoking the possibility.

Sources: Berkeley Technology Law Journal (2025); R. Chesney & D. Citron, 107 Calif. L. Rev. 1753 (2019); U.S. FRE Advisory Committee (proposed Rule 901(c)).

EUROPOL IOCTA 2026

The Rise of Synthetic CSAM

Für das Bild *ph_02054_.png* wurden folgende Prompts eingesetzt:

POSITIVE PROMPT	pre teen child girl walking up a beach carrying a surfboard under her arm, long wavy brunette hair blows in the wind, wearing a wetsuit unzipped and showing a bit of cleavage, long sleeves, morning sunlight reflects off the water, heavy surf
NEGATIVE PROMPT	((censored)), ((Asian)), ((bad anatomy)), bad hands, three hands, three legs, bad arms, missing legs, missing arms, poorly drawn face, bad face, fused face, cloned face, worst face, three crus, extra crus, fused crus, worst feet, three feet, fused feet, fused thigh, three thigh, fused thigh, extra thigh, worst thigh, missing fingers, extra fingers, ugly fingers, long fingers, horn, extra eyes, huge eyes, amputation, disconnected limbs, cartoon, cg, 3d, unreal, animate bad anatomy, bad hands, breasts, three hands, three legs, bad arms, missing legs, missing arms, poorly drawn face, bad face, fused face, cloned face, worst face, three crus, extra crus, fused crus, worst feet, three feet, fused feet, fused thigh, three thighs, fused thigh, extra thigh, worst thigh, missing fingers, extra fingers, ugly fingers, long fingers, horn, extra

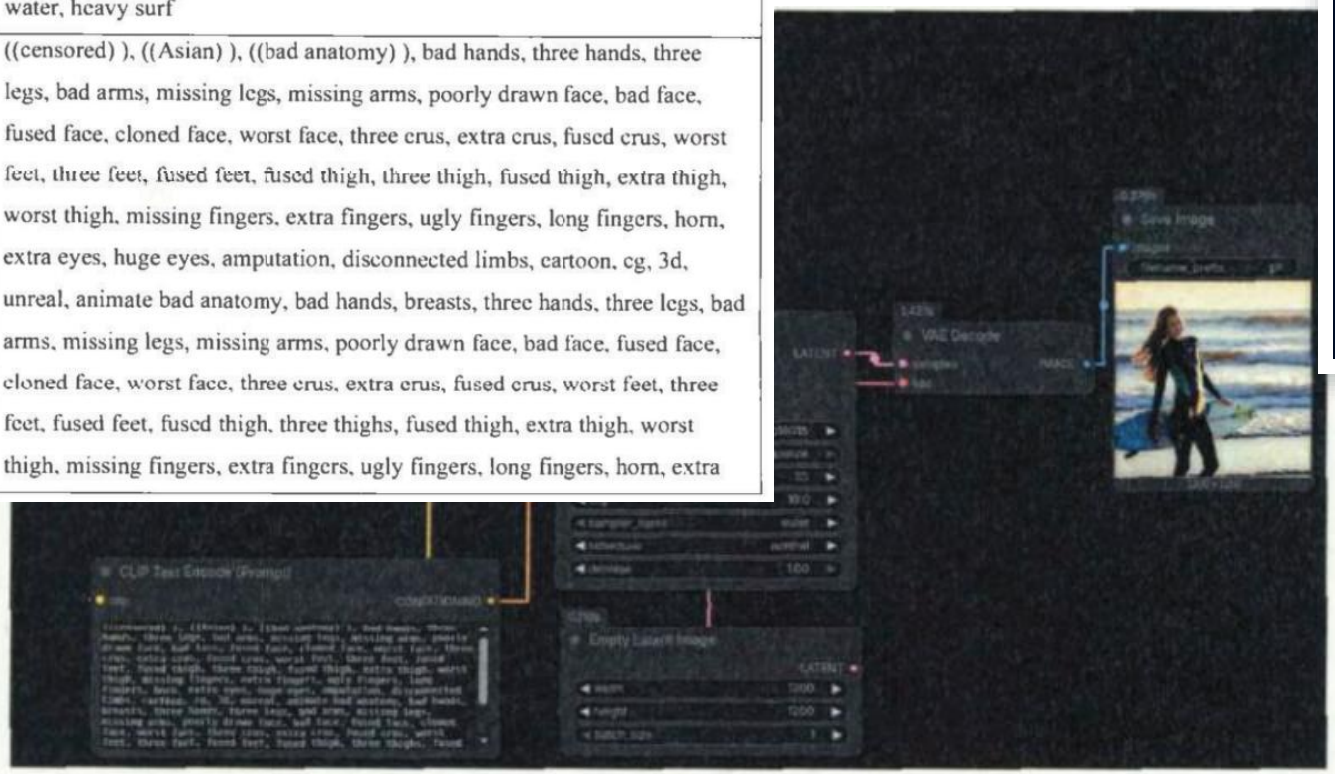


Abbildung 3 – Workflow aus Abb. 2 nach Verarbeitung durch ComfyUI

EUROPOL IOCTA 2026

The Rise of Synthetic CSAM

Production at scale

The rapid evolution and accessibility of AI tools have drastically scaled up the production of Child Sexual Abuse Material (CSAM) and sophisticated offender grooming techniques.

Organised exchange

Investigations reveal international platforms where offenders exchange technical skills, ready-made prompts, and OPSEC tips to refine synthetic production.

Unprecedented challenge

This multiplied volume of highly realistic AI-generated material poses severe, unprecedented challenges for imagery analysis and the identification of offenders.

EUROPOL IOCTA 2026

AI Generation & Evasion Tactics

Fully vs. partially synthetic

Image-to-image models alter existing photos to create partially synthetic CSAM. In parallel, advancing text-to-image and text-to-video models generate entirely new, fully synthetic material from offender prompts alone.

Offline models

To bypass online content moderation and safety guardrails, offenders use offline AI models - deliberately trained on authentic abuse material for accurate, unmoderated generation.

Bots in E2EE groups

Automated generation bots operate within encrypted communications. Bots capable of editing images to produce synthetic CSAM on demand have been detected inside end-to-end-encrypted groups.

CASE STUDY

AI in Investigative Journalism

Tracking a fugitive

Used to help track fugitive terrorist Daniela Klette.

Facial recognition

Journalists applied facial-recognition tools to public images.

Public vs. private

Raised questions about AI's role in private versus public investigation.

DANIELA KLETTE CASE

How Facial Recognition Reopened the Hunt

- **Daniela Klette**: former RAF (Red Army Faction) member.
- Suspected of involvement in serious crimes from the 1980s and 1990s.
- Went underground in 1993 and lived undetected for **over 30 years**.
- One of Germany's most-wanted fugitives.
- In 2024, investigative journalists used the facial-recognition tool **PimEyes**.
- PimEyes compared public images to online sources using AI algorithms.
- A match was found between old RAF photos and a woman in Berlin.
- This led to a reactivation of law-enforcement efforts.

DANIELA KLETTE CASE - THE VERDICT

Sentenced in Verden, May 2026

13 years

Prison sentence (Verden court, 27 May 2026)

- Arrested in early 2024 in Berlin after the renewed investigation.
- Convicted of **aggravated armed robbery, attempted kidnapping, and possession of military weapons**.
- The ruling rested on a series of heists on supermarkets and cash-transport vehicles between 1999 and 2016, committed to finance her life underground after the RAF disbanded.
- The verdict focused strictly on these criminal acts - separate from any politically motivated terrorism charges from her earlier RAF years.
- Alleged accomplices Burkhard Garweg and Ernst-Volker Staub, both ex-RAF members, **remain at large**.

LEGAL PERSPECTIVES ON BIOMETRIC SCRAPING & DIGITAL IDENTIFICATION

AI Biometrics in Criminal Procedure

Legality of biometric scraping

GDPR Article 9 constraints and the impact of the EU AI Act on mass-scale facial harvesting.

Private vs. public surveillance

A shift of investigative tasks to private-sector databases - and the resulting challenges for public oversight.

Evidentiary value & standards

The weight of AI-generated matches in court, and the procedural fairness of algorithmic evidence.

LEGAL FRAMEWORK

The European Union's Rules

EU Artificial Intelligence Act

Regulation (EU) 2024/1689 classifies AI by risk - unacceptable, high, limited, minimal. High-risk systems (e.g. biometric ID) face strict requirements.

Charter of Fundamental Rights

Guarantees the rights to privacy, data protection, and a fair trial.

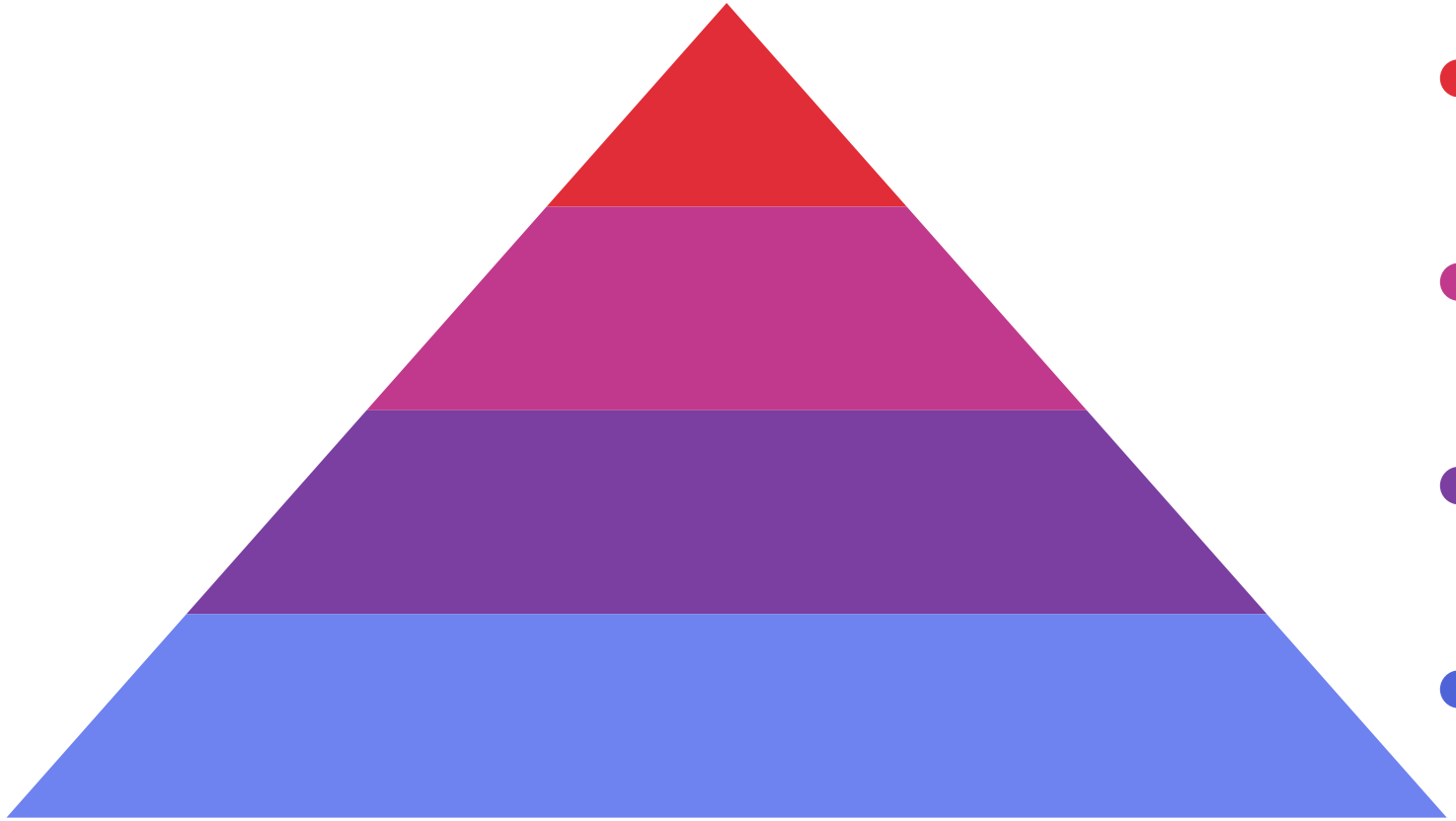
e-Evidence Regulation

Cross-border access to electronic evidence - directly affecting AI-generated data.

EU ARTIFICIAL INTELLIGENCE ACT

A Risk-Based Approach

The AI Act defines four levels of risk for AI systems:



Unacceptable risk

Prohibited AI practices

High risk

Strict requirements (e.g. biometric ID)

Limited risk

Specific transparency obligations

Minimal risk

Most AI - no specific obligations

PROHIBITED AI SYSTEMS · CHAPTER II, ART. 5

Real-Time Biometric ID: Banned - Except…

Real-time remote biometric identification (RBI) in publicly accessible spaces for law enforcement is **prohibited** - except in three situations:

Finding victims

Searching for missing persons, abduction victims, and people who have been human-trafficked or sexually exploited.

Preventing grave threats

Preventing a substantial and imminent threat to life, or a foreseeable terrorist attack.

Serious-crime suspects

Identifying suspects in serious crimes - e.g. murder, rape, armed robbery, drug and illegal-weapons trafficking, organised crime, environmental crime, etc.

PROHIBITED AI SYSTEMS · CHAPTER II, ART. 5

The Safeguards on Real-Time RBI

1

Strict necessity

Permitted only where not using the tool would cause considerable harm - and always weighing the rights and freedoms of affected persons.

2

Assessment & registration

Before deployment: a fundamental-rights impact assessment and registration in the EU database. In duly justified urgency, deployment may start before registration, provided it is registered later without undue delay.

3

Judicial authorisation

Prior authorisation from a judicial or independent administrative authority. In urgency it may begin first, but authorisation must be requested within 24 hours - and if refused, deployment must cease immediately, deleting all data, results and outputs.

EUROPEAN COMMISSION

Guidelines on Prohibited AI Practices

European Commission

Brussels, 4.2.2025 - C(2025) 884 final

Annex: Guidelines on prohibited AI practices established by the AI Act.

ANNEX

to the

Communication to the Commission

Approval of the content of the draft Communication from the Commission - Commission Guidelines on prohibited artificial intelligence practices established by Regulation (EU) 2024/1689 (AI Act)

PROHIBITED AI SYSTEMS · ART. 5 - EXAMPLE 1

Festival: Untargeted Facial Recognition

> During a busy festival, police deploy live facial recognition to monitor the area and identify wanted individuals with outstanding arrest warrants for illegal drug trafficking and sexual offences. At the entrances, live video of passers-by is compared against a watchlist. **Concerning the offence types, RBI can be used for illegal drug trafficking. However, sexual offences are not on the list** - unless they relate to the sexual exploitation of children, child sexual abuse material, or rape. The police are **not allowed** to deploy real-time facial recognition in a broad, untargeted manner, in the hope of finding wanted criminals and taking them off the streets.
>
> *- European Commission, Guidelines on prohibited AI practices*

ASSESSMENT

Not permitted

Broad, untargeted use - and most of the cited offences fall outside Art. 5.

PROHIBITED AI SYSTEMS · ART. 5 - EXAMPLE 2

Festival: A Targeted Search

> The case is different if the police have received a **physical description with a photograph** of a wanted individual who is subject to a **European Arrest Warrant for drug trafficking**, and they have reason to believe he will be present at the festival. In those circumstances, deploying real-time facial recognition to identify a **targeted individual** may be covered by Article 5(1)(h)(iii) AI Act.
>
> *- European Commission, Guidelines on prohibited AI practices*

ASSESSMENT

May be permitted

A targeted search for one identified person, on a qualifying offence.

PROHIBITED AI SYSTEMS · ART. 5 - EXAMPLE 3

After a Terror Attack

> After a serious terror attack at a Christmas market with **12 deaths**, the police use real-time facial recognition to identify the offender and track where he is escaping. They also use the real-time facial recognition of the nearby train station and at the destination stations of trains leaving shortly after the attack. In the case of a **terror attack**, such use can be permitted under Article 5(1)(h)(iii) AI Act.
>
> *- European Commission, Guidelines on prohibited AI practices*

ASSESSMENT

Can be permitted

A foreseeable / actual terrorist attack is an express exception.

CONSIDERATIONS AND DISCUSSION

Concerns and Counterpoints

COMMON CONCERNS

- Bias and discrimination.
- Transparency and accountability - the difficulty of explaining AI decisions.
- Legal uncertainty - the lack of clear AI rules in criminal law.

COUNTERPOINTS

- **Human expert witnesses are themselves biased and inconsistent** - why should AI be regulated more than fallible human judgment, despite offering more transparency?
- **AI is not the decision-maker** - criminal procedure already has oversight (e.g. judicial review), so extra regulation is redundant and burdensome.
- **Regulatory burden hampers law enforcement** - while AI offers superior traceability.

CONSIDERATIONS AND DISCUSSION

A Call for Proportionality

THESIS

The EU AI Act overregulates AI tools in criminal justice - placing an undue burden on investigations without equivalent scrutiny of human actors.

Regulate by function

Regulate based on function and context - not on AI status alone.

Safeguard, don't stifle

Ensure safeguards without stifling innovation.

Hold everyone to account

Focus on accountability across both human and artificial contributors.

THANK YOU FOR YOUR ATTENTION!

Questions? Remarks?

HESSEN

Is Mandatory Disclosure of digital access fair? Evaluating e-evidence, pins and passwords

Muthupandi Ganesan
Barrister & Partner
Aliant Law

15 June 2026

Zagreb

Co-funded by the European Union.
Views and opinions expressed are however those of ERA only and do not necessarily reflect those of the European Union or European Commission.
Neither the European Union nor the granting authority can be held responsible for them.

ALIANT®
Powered by *Human* Intelligence

This Presentation will cover

- Mandatory Disclosure under UK regime
- Notice under section 49 RIPA
- Trial procedure & Expert Evidence
- Fairness – Human Rights – Remedy?

ALIANT®
Powered by *Human* Intelligence

Mandatory Disclosure of Pins and Passwords

- **What type of material can be subject of mandatory disclosure?**
  - **Protection Information**
  - **Comes in to possession of the Police lawfully**

- **Appropriate Persons – on reasonable grounds believes that:**

(a)that a key to the protected information is in the **possession of any person**,
(b)that the imposition of a disclosure requirement in respect of the protected information is—
(i)necessary on grounds falling within subsection (3), or
(ii)necessary for the purpose of securing the effective exercise or proper performance by any public authority of any statutory power or statutory duty,
(c)that the imposition of such a **requirement is proportionate** to what is sought to be achieved by its imposition, and
(d)that it is not reasonably practicable for the person with the appropriate permission to obtain possession of the protected information in an intelligible form without the giving of a notice under this section,
the person with that permission may, by notice to the person whom he believes to have possession of the key, impose a disclosure requirement in respect of the protected information.

ALIANT®
Powered by *Human* Intelligence

Criteria for disclosure?

- A disclosure requirement in respect of any protected information is necessary on grounds falling within this subsection if it is necessary—
  - (a) in the interests of national security;
  - (b) for the purpose of preventing or detecting crime; or
  - (c) in the interests of the economic well-being of the United Kingdom. (section 49 (3)

- Notice to be given under section 49(4)

ALIANT®
Powered by *Human* Intelligence

Notice requirement

must be given in writing or (if not in writing) must be given in a manner that produces a record of its having been given;

(b) **must describe the protected information** to which the notice relates;

(c) must specify the matters falling within subsection (2)(b)(i) or (ii) by reference to which the notice is given;

(d) must specify the office, rank or position held by the person giving it;

(e) must specify the office, rank or position of the person who **for the purposes** of Schedule 2 granted permission for the giving of the notice or (if the person giving the notice was entitled to give it without another person's permission) must set out the circumstances in which that entitlement arose;

(f) must specify the time by which the notice is to be complied with; and

(g) must set out the disclosure that is required by the notice and the form and manner in which it is to be made;

and the time specified for the purposes of paragraph (f) **must allow a period for compliance which is reasonable in all the circumstances.**

ALIANT®
Powered by *Human* Intelligence

Refusal to provide Pins and Passwords (1) - Terrorism

- Rex v Jonathan Nuttall – Central Criminal Court – 2023
- 5 months trial with 6 Defendant trial
- Allegations of bomb hoax, money laundering and failure to provide pins and passwords
- Chronology
  - March 2022: Arrest and seizure of electronic devices (30 items)
  - April 2022: Charged with bomb hoax and money laundering.
  - July 2022: Request for disclosure of pins and passwords
  - August 2022: Response by the Defendant – cannot recall the passwords and pins.
  - January 2023: Further charges of failure to give pins and passwords.

ALIANT®
Powered by *Human* Intelligence

Notice under section 49

- The protected information to which the Section 49 Notice relates to are as follows:

1. RJB/33 - iPhone 11 Pro A2160 – requires alphanumeric PIN
2. RJB/81 - iPhone 12 Pro Max A2342 – requires alphanumeric PIN
3. RJB/47 - Integral Courier USB Stick – encrypted USB
4. RJB/75 - Integral Courier USB Stick – encrypted USB
5. AAW/20 – IronKey USB in box – requires password

- 6. AAW/3 – MacBook Pro in case – requires password

Defendant Response

1. The Devices have a long and complex password as advised to the public by the National Crime Agency.
2. The Defendant did not write it down or make a note of it and as such cannot recall.
3. The Defendant did not use the same password for different digital devices.
4. The passage of time of nearly 5 months by the time of the NOTICE meant that he cannot recall.

ALIANT®
Powered by *Human* Intelligence

Expert Evidence

- Examined only after Defendant gave evidence.
- 2 x Devices - did not have passwords
- 1 x Device – on factory settings
- 1 x Device – cant be sure, if password was set up.

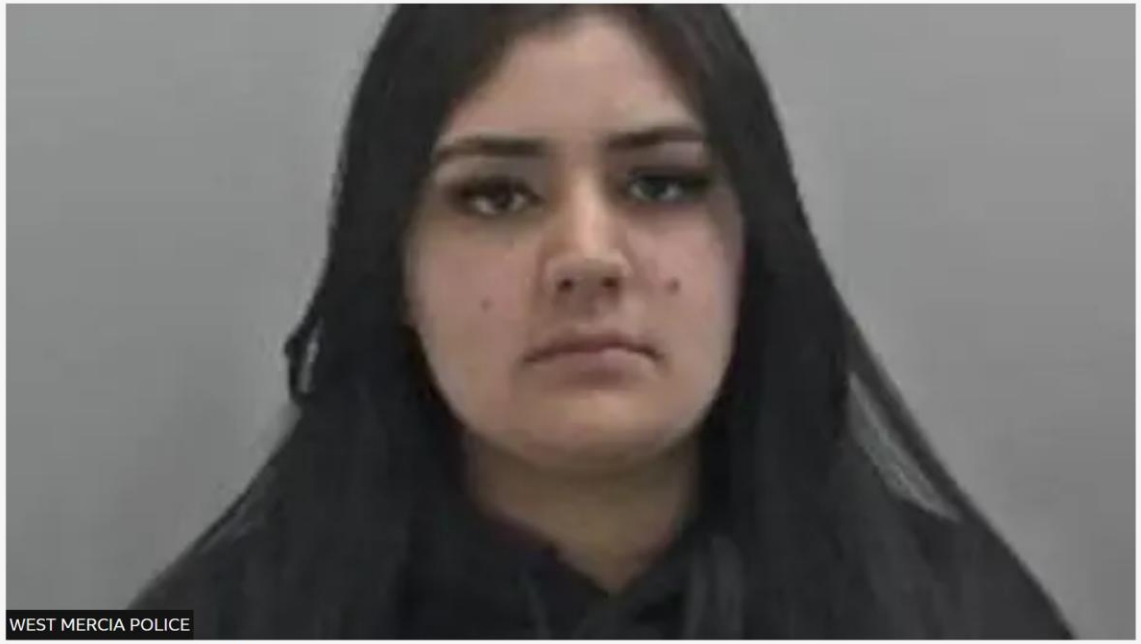
Sentence:

<u>Count 5 and 6:</u> Failure to provide pins and passwords to two telephones seized by the Police. The Defendant was sentenced to 6 months imprisonment concurrent for both Counts 5 and 6 but consecutive to other sentences for counts 1, 3 and 4.

ALIANT®
Powered by *Human* Intelligence

Refusal to provide Pins and Passwords (2)

Woman jailed for refusing to reveal phone password



Sanaa Shahzad is thought to be the first woman in the West Mercia Police area to be jailed for refusing to give police her phone password

Shahzad "deliberately obstructed" the inquiry by "refusing us the password to her phone", police said after her three-month term for failure to disclose the key to protected information.

The three months are to run concurrently to Shahzad's 12-month sentence for dangerous driving - an offence unrelated to the fatal Redditch crash but recorded on the same day.

ALIANT®
Powered by *Human* Intelligence

Refusal to provide Pins and Passwords (3)

Police suspected Tommy Robinson had information relevant to acts of terrorism on phone, court told

Activist refused to give police his phone pin when stopped at Channel tunnel in July 2024

Tommy Robinson, attending Westminster magistrates court on Monday, says his phone had 'journalistic material on it'.

Tommy Robinson cleared of terror offence after not giving police access to his phone

ALIANT®
Powered by *Human* Intelligence

Refusal to provide Pins and Passwords (4) (Live Case)

In this matter, Mr Father Christmas ("the defendant") faces one allegation in Count 3 as follows:

Count 3:

STATEMENT OF OFFENCE

FAILURE TO COMPLY WITH A NOTICE, contrary to Section 53 of the Regulation of Investigatory Powers Act 2000.

PARTICULARS OF OFFENCE

Mr Father Christmas between the 19th day of July 2021 and the 29th day of November 2024, being a person to whom a section 49 notice had been given, he did knowingly fail, in accordance with the notice, to make the disclosure required by virtue of the giving of the notice, namely he did fail to provide the PIN number for an iPhone that was required of him.

ALIANT®
Powered by *Human* Intelligence

Fairness?

- Case specific: Victim v Defendants Rights
- Nature of criminal investigation (child abuse/ child sex images v economic crime or other forms serious organised crime)
- Timing of criminal investigation
- Evidential basis – Political motivation (Tommy Robinson)
- Trustworthiness of decision making? - fairness
- Sentence: up to 2 years.
- Remedy? -

ALIANT®
Powered by *Human* Intelligence

Any questions?

Muthupandi Ganesan
Barrister & Partner
E-mail: mganesan@aliantlaw.com

20 – 21 November 2025

Bavarian State Ministry of Justice

#DIGITALISATION AND #ARTIFICIALINTELLIGENCE IN CRIMINAL JUSTICE

Zagreb 16 June 2026

Data retention

data protection

vs.

the risk of systemic impunity

Co-funded by the European Union.
Views and opinions expressed are however those of ERA only and do not necessarily reflect those of the European Union or European Commission.
Neither the European Union nor the granting authority can be held responsible for them.

Data protection vs. the risk of systemic impunity

EDRi
The CJEU jeopardises essential privacy protections to accommodate false law enforcement claims

BBC Sign in
NEWS
Top EU court rejects EU-wide data retention law
8 April 2014

Structure of presentation

- **Introduction**
  - Definition
  - State of play of legislation
  - Significance for the investigation and prosecution of crimes
- **Case law of the Court of Justice of the EU**
  - Basic considerations of the CJEU
  - State of play
  - Resulting framework for national legislation
- **Current legislative developments**

What does „data retention“ mean?

Obligation for **providers of electronic communications services** to

- **store traffic/location data** (not subscriber/content data) for a certain period of time and to
- **provide access** to authorities under certain conditions

Current legal framework

EU-level:

None (Data Retention Directive 2006/24/EC declared invalid by CJEU decision of 08.04.2014 (C-293/12, C-594/12 Digital Rights Ireland)

Member States:

EUROJUST
European Union Agency for Criminal Justice Cooperation

Fragmentation (Eurojust/EJCN overview of 11/2024 https://www.eurojust.europa.eu/publication/effect-court-justice-european-union-case-law-national-data-retention-regimes-judicial-cooperation): most MSs have law in place, but no recognisable common pattern

Significance for the investigation of crimes

Identification of perpetrators through **subscriber data allocated to dynamic IP-address** (+port number/time stamp), e.g. based on NCMEC (National Center for Missing and Exploited Children)-notifications

BKA- position paper of July 2023:
https://www.bka.de/SharedDocs/Kurzmeldungen/DE/Kurzmeldungen/230623_Mindestspeicherfristen_IP-Adressen.html

success rate for the allocation of IP-addresses to concrete subscribers in NCMEC-cases:

- currently (without any data retention): 41%
- with a hypothetical data retention period of two weeks: 84,5 %

Case law of the CJEU – procedural setting

- **Preliminary rulings on** national data retention law in Member States

- Questions referred to CJEU by national courts concern
  - **interpretation of Article 15(1) of Directive 2002/58/EC** (e-privacy Directive)
  - read in the light of **Charter of fundamental rights**
    - Art. 7 (Respect for private life)
    - Art. 8 (Protection of personal data)
    - Art.11 (Freedom of expression and information)

Case law of the CJEU – procedural setting

Article 15(1) of Directive 2002/58/EC

"Member States may adopt legislative measures to restrict the scope of the rights and obligations provided for in (...) this Directive when such restriction constitutes a **necessary, appropriate and proportionate measure** within a democratic society to safeguard **national security** (i.e. State security), **defence, public security, and the prevention, investigation, detection and prosecution of criminal offences** (...). To this end, Member States may, inter alia, adopt legislative measures providing for the retention of data for a limited period justified on the grounds laid down in this paragraph. (...)"

Case law of the CJEU – Milestone decisions

- **Digital Rights Ireland** (C-293/12 and C-594/12) 08.04.2014: Data retention Directive is disproportionate and invalid

- **Tele 2 Watson** (C-203/15 and C-698/15) 21.12.2016: general and indiscriminate retention of all traffic and location data for the purpose of fighting serious crime violates EU-law

- **Quadrature du Net** (C-511/18 and C-512/18) 06.10.2020 exception for IP-addresses

- **Hadopi** (C-470/21) 30.04.2024 expansion/clarification of the exception for IP addresses

Case law of the CJEU – Basic considerations

Balance between the various interests and rights at issue:

Rights/interests interfered with by data retention	Rights/interests protected by data retention
Respect for private life	Efficiency of combating crime
Protection of personal data	Obligation to protect (the rights of minors)
Freedom of expression and information	

Case law of the CJEU – Basic considerations

General and indiscriminate retention of all traffic and location data for the purpose of fighting crime

is NOT in line with EU-law

Case law of the CJEU – Key arguments

- As an exception Article 15(1) of Directive 2002/58/EC has to be interpreted narrowly; **the exception mustn´t become the rule**

- **Storage is an interference by itself**, independently of a possible later use of/access to the data

- **Traffic/location data no less sensitive than content** regardless of retention period (provides means to establish profiles of individuals)

Case law of the CJEU – Key arguments

- **Proportionality** requires:
  - Precise rules on **scope of interference and safeguards**
  - **Connection** between the data to be retained and the objective of the legislation

Resulting limits for legislation

Objective of prosecuting serious crime does not justify indiscriminate general data retention; **exceptions:**

- General and indiscriminate retention of **data relating to the civil identity of users**
- **Quick freeze**
- **Targeted retention of traffic and location data** which is limited according to the categories of persons or using a geographical criterion
- General and indiscriminate **retention of IP addresses** assigned to the source of an internet connection

Retention of IP adresses - Hadopi decision

- Retention of (source) IP addresses also for the purpose of combating **general crime (not only serious crime)**

  Precondition: "watertight" separation from other stored data

- **Access by administrative authority** for the sole purpose of identifying perpetrators without prior judicial review

CJEU (C-470/21, par. 119) **"…not to allow such access would carry a real risk of systemic impunity…"**

Current legislative developments

Impact assessment by the European Commission

(https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/14680-Data-retention-by-service-providers-for-criminal-proceedings-impact-assessment_en)

Objective:

„(…) ensure the availability of certain categories of non-content data for the purpose of carrying out successful criminal investigations and prosecutions (…)"

Policy options:

- soft law measures
- legislative measures

Thank you for the attention!

Michael Rothärmel
Email: michael.rothaermel@stmj.bayern.de

#DIGITALISATION and #AI in Criminal Justice

Technical insights for the preparation, identification and preservation phase

David Silva Ramalho

Lawyer | University of Lisbon's School of Law

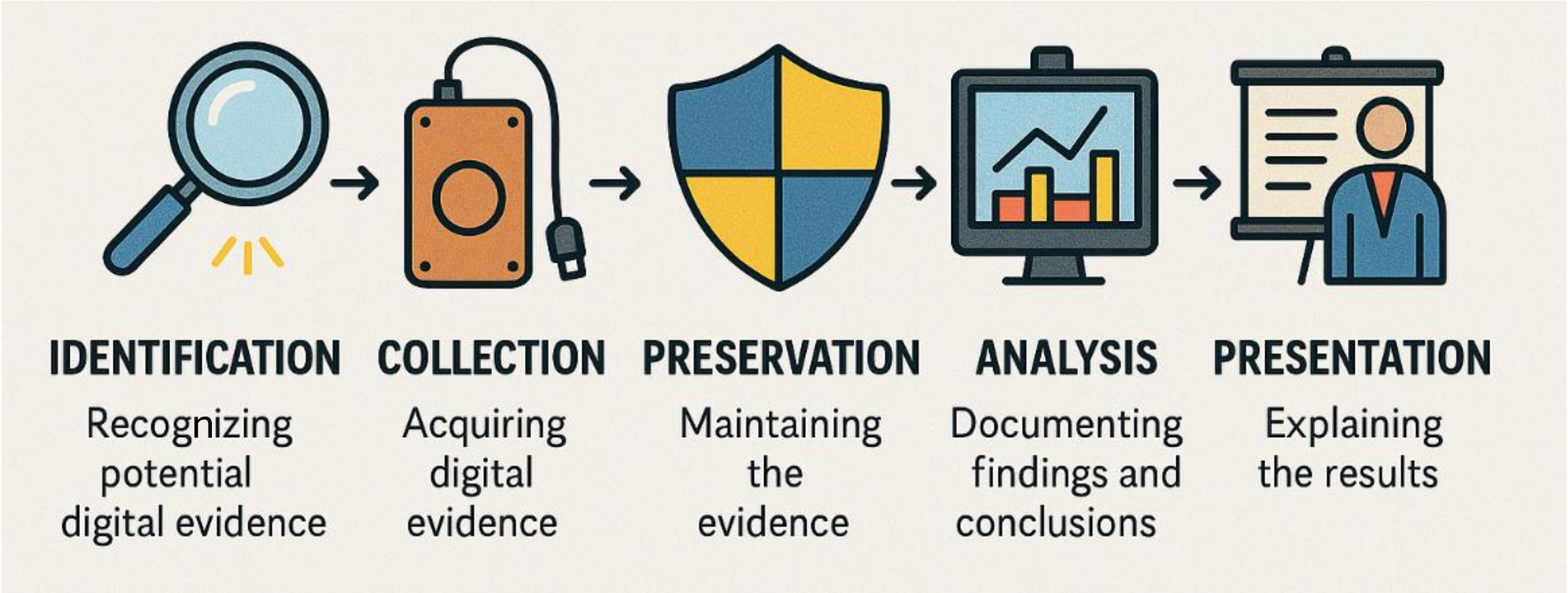
Co-funded by the European Union.
Views and opinions expressed are however those of ERA only and do not necessarily reflect those of the European Union or European Commission. Neither the European Union nor the granting authority can be held responsible for them.


Starting from the top

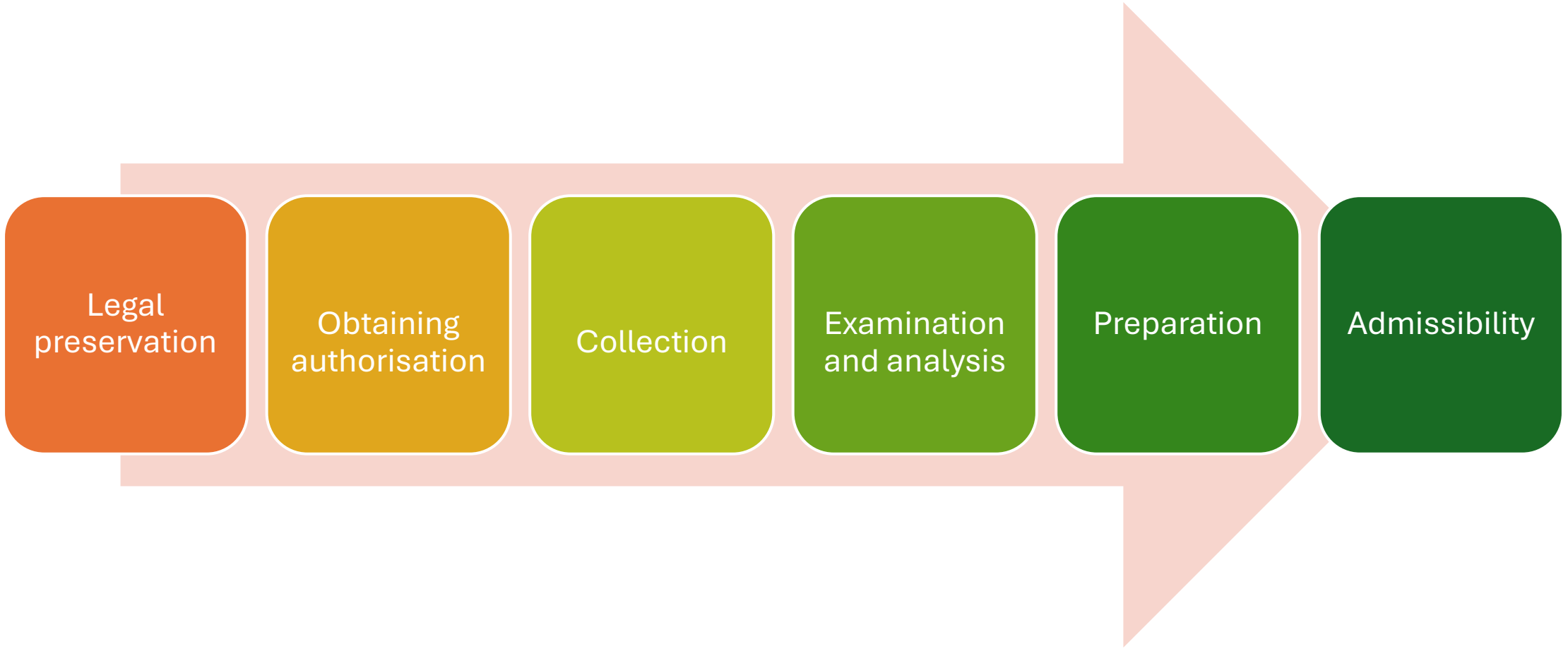
COMPUTER FORENSICS

Computer forensics is a branch of digital forensics that involves the methodical **identification, collection,** , **preservation**, **analysis**, and **presentation** of computer-related evidence to investigate and prevent cybercrimes or other digital incidents”

COMPUTER FORENSICS PROCEDURES



COMPUTER FORENSICS AND E-EVIDENCE



Preservation

- The first goal of computer forensics is to preserve the integrity of digital evidence.
- This means ensuring that the data is not tampered with, altered, or destroyed during the investigation. Proper **chain of custody** procedures must be followed.

Capture volatile data

- Digital evidence is frequently volatile, which means that it can change or disappear quickly.

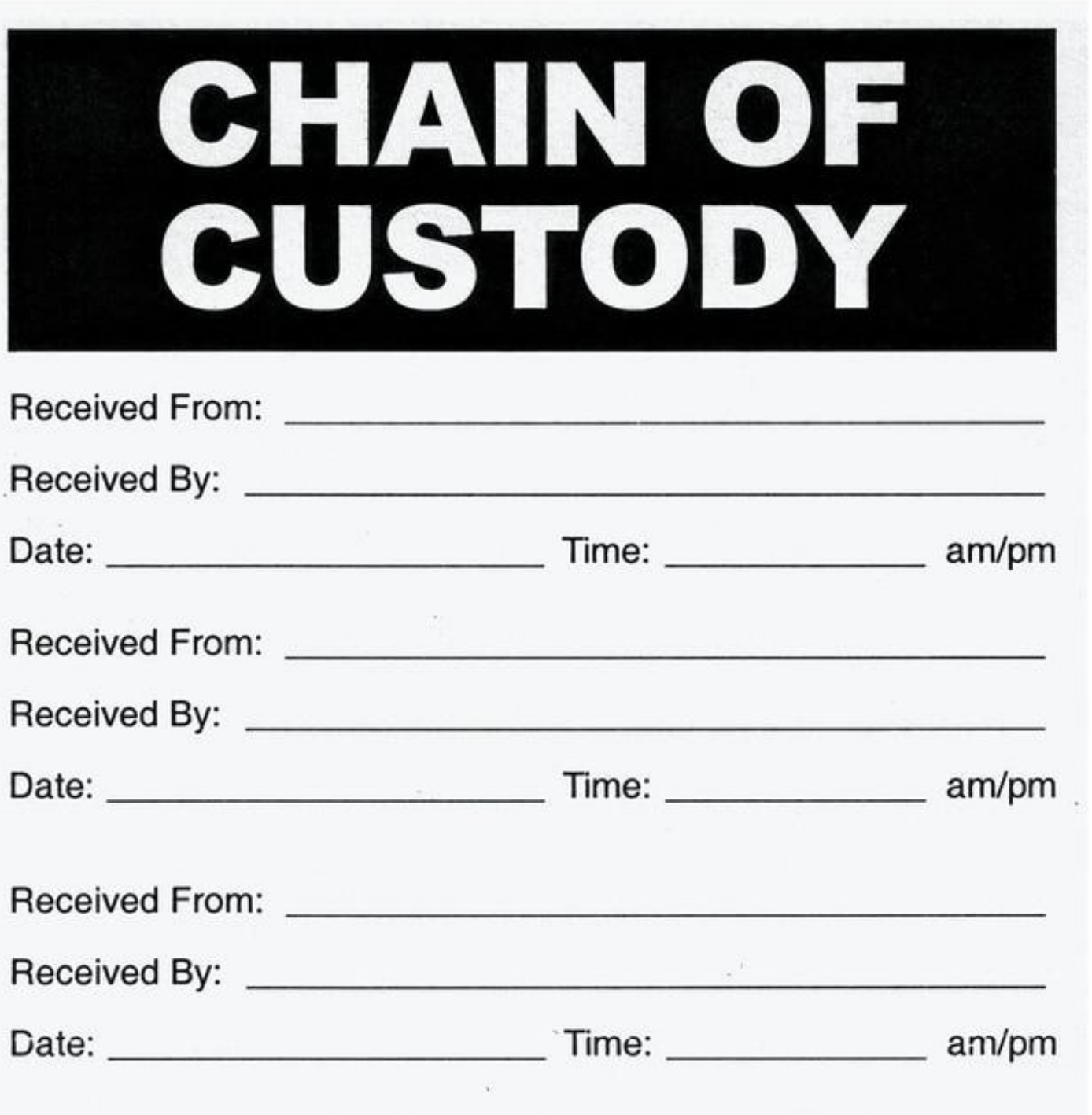
- Investigators must act swiftly to capture and preserve volatile data, which includes running processes, open network connections, RAM contents, etc.

Documentation and logging

- All procedures and actions taken during the investigation must be documented.
- This documentation should include, among others, the date and time of each action, the investigators involved, as well as the tools and methods used.

Legality of the investigation

- All necessary authorisations must be in place for the evidence to be collected and the forensic analyst to act.
- This includes different authorisations for different data (e.g. emails, messages, intimate files, etc.).



Chain of custody

- **Definition**: The chain of custody is a documented record of the possession, control, transfer, and analysis of digital evidence.
- **What for?** It guarantees that the evidence is admissible in court by demonstrating how it was handled and preserved from day 1 until it reaches the court.
- **Unbroken Chain:** Every transfer, person, and location is logged (date, time, what was done)
- **Admissibility Link:** Courts require showing that evidence is in *substantially same condition* as original

"Your Honour, I call Nigel From The Pub .. witness on whatever you like."

Impartial analysis, reporting and expert testimony

- The data should be thoroughly analysed, whether to confirm or refute the accusation's narrative.
- It should be conducted by an independent analyst.
- If possible, the suspect should be involved.
- A report must be then drafted.
- The expert must present itself before court to have its methods analysed and challenged.

OSINT

What we should have

Identify and preserve

1. Identification of Relevant Data

First, one needs to determine what OSINT content is relevant (e.g. posts, comments, private messages, likes, media uploads, timelines, followers).

Then we identify user accounts involved (which may be public, private, anonymous, or impersonating).

Identify and preserve

2. Preservation in a Forensically Sound Manner

Social media evidence can **change or be deleted quickly**, so forensic preservation is relevant.

Tools or experts preserve the evidence exactly as it was at the time of collection, including:

- **Metadata** (timestamps, account IDs, geo-tags)
- **Original URLs** and unique post IDs
- **Cryptographic hashes** (to prove later that the data hasn't changed)

Tools and capture

3. Use of Forensic Tools

Digital forensics specialists use certified tools that ensure data is collected without alteration and is well-documented:

These tools often create an **audit trail** and generate reports that include screenshots, metadata, and hash values for admissibility.

Tools and capture

4. Capture Methods

Depending on the platform and access level (public or private), forensic practitioners may use:

- **API access** (when legal and available) to download structured data
- **Account owner downloads** (e.g. “Download Your Info” from Facebook)
- **Authenticated screenshots or screen recordings** (sometimes with timestamp overlays and hash verification)
- **Manual browsing with logging tools** to document navigation and context

Wayback machine?

Notary?

Chain of custody and preparation

5. Chain of Custody Documentation

Every step is logged: who collected the data, when, how, and where it's stored.

Hashes are computed and used to **verify evidence integrity** over time.

This audit trail is critical in court to show the evidence hasn't been altered.

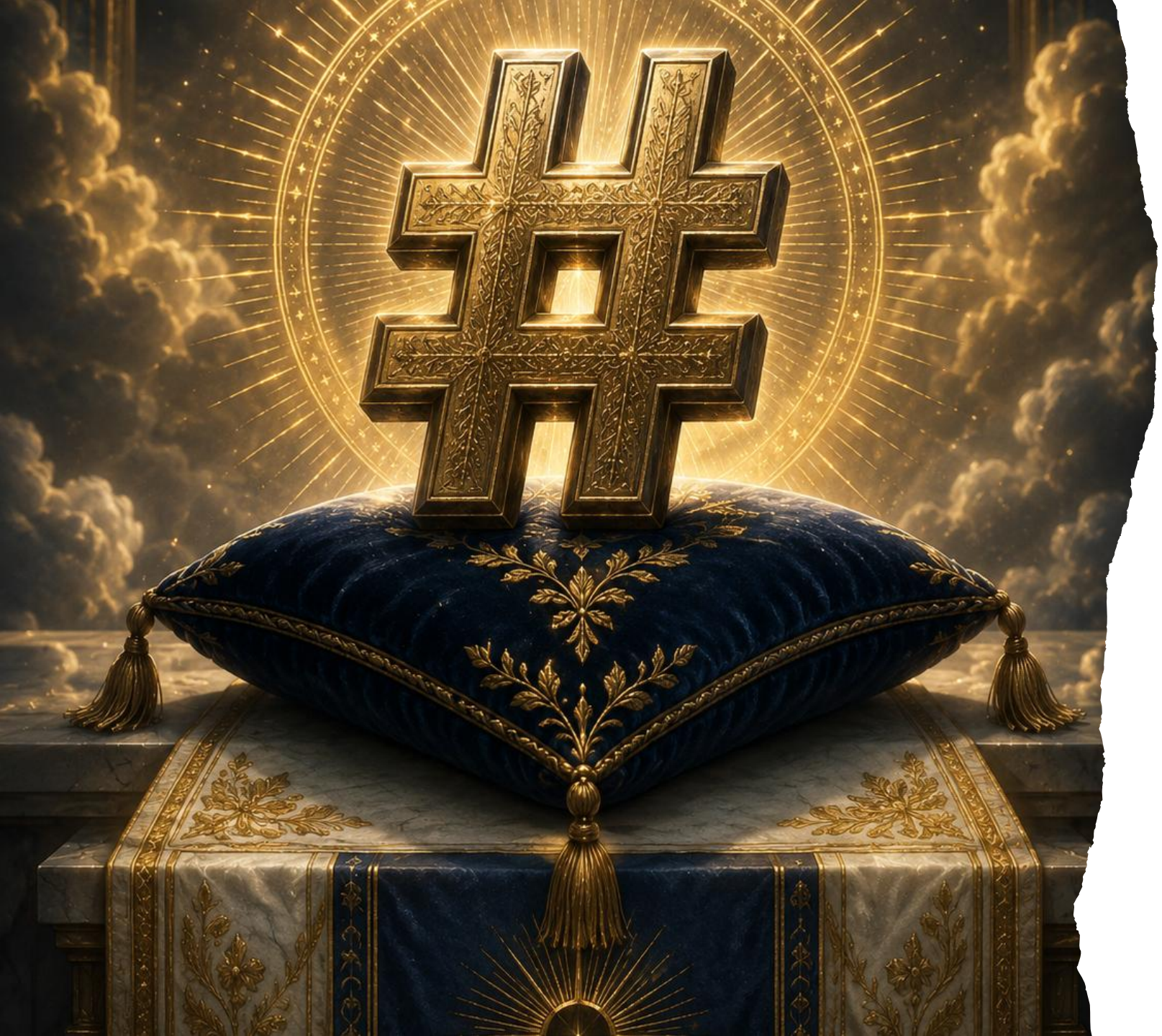
6. Preparation for Courtroom Admissibility

Evidence should be authenticated under applicable national rules, if they exist, or according to best practices.

Metadata, witness testimony, or platform records may be used to show:

- The content is what it claims to be
- It came from a particular account
- It hasn't been altered since collection

What we actually have



The holy hash

COMMONWEALTH

v.

Bryon L. BANAS

No. 13–P–597

Appeals Court of Massachusetts

March 21, 2014

Discussion. Admission of Facebook picture. The defendant argues that it was error to admit a picture of shoes from the defendant's Facebook page because it was not properly authenticated as being posted by the defendant. **We agree it was error but conclude it was not prejudicial.**

Authentication is a "condition precedent to admissibility" that requires that the proponent provide "evidence sufficient, if believed, to convince the jury by a preponderance of the evidence that the item in question is what the proponent claims it to be." Commonwealth v. Purdy, 459 Mass. 442, 447 (2011). In Commonwealth v. Williams, 456 Mass. 857, 869 (2010), the Court held that evidence that a message was from an individual's Web page was not sufficient to authenticate that the individual wrote the message. **Evidence of additional confirming circumstances is needed to authenticate the message, which could include "how secure such a Web page is, who can access a Myspace Web page, whether codes are needed for such access, etc**." *Ibid.* See also Commonwealth v. Purdy, 459 Mass. at 450.[1]Here, Nalepinski testified that **he was Facebook friends with the defendant, logged onto defendant's page, saw the picture, and printed it. This was not sufficient to authenticate that the post was made by the defendant**. It was error to admit the picture.


Evidence from physical searches

Computers

ISO 27037 and the ACPO/College of Policing standards

1. Connect the device via write blocker
2. Create a forensic bit-for-bit image (full sector copy, including unallocated space, deleted files, slack space)
3. Calculate the SHA-256 hash of both original and image immediately after acquisition
4. Record both values in the chain of custody documentation
5. Seal and store the original — label, photograph, controlled conditions
6. All subsequent analysis conducted on the image, never the original
7. Periodic hash verification to confirm the image has not been altered

Important: live box or dead box?

If the computer is on, live forensics should be done.

Smartphones

Different challenges and different scenarios:

1. Is it encrypted?
2. Is it online (Faraday it)?
3. Is there cloud synchronization?
4. What information does one wish to collect (app data, location data, messages, contacts, call logs)?

Large organizations

1. Identify systems, custodians, data categories and date ranges
2. Preserve logs and suspend deletion policies where lawful
3. Use company technical staff under supervision
4. Record extraction queries and hash exports
5. Preserve audit logs.

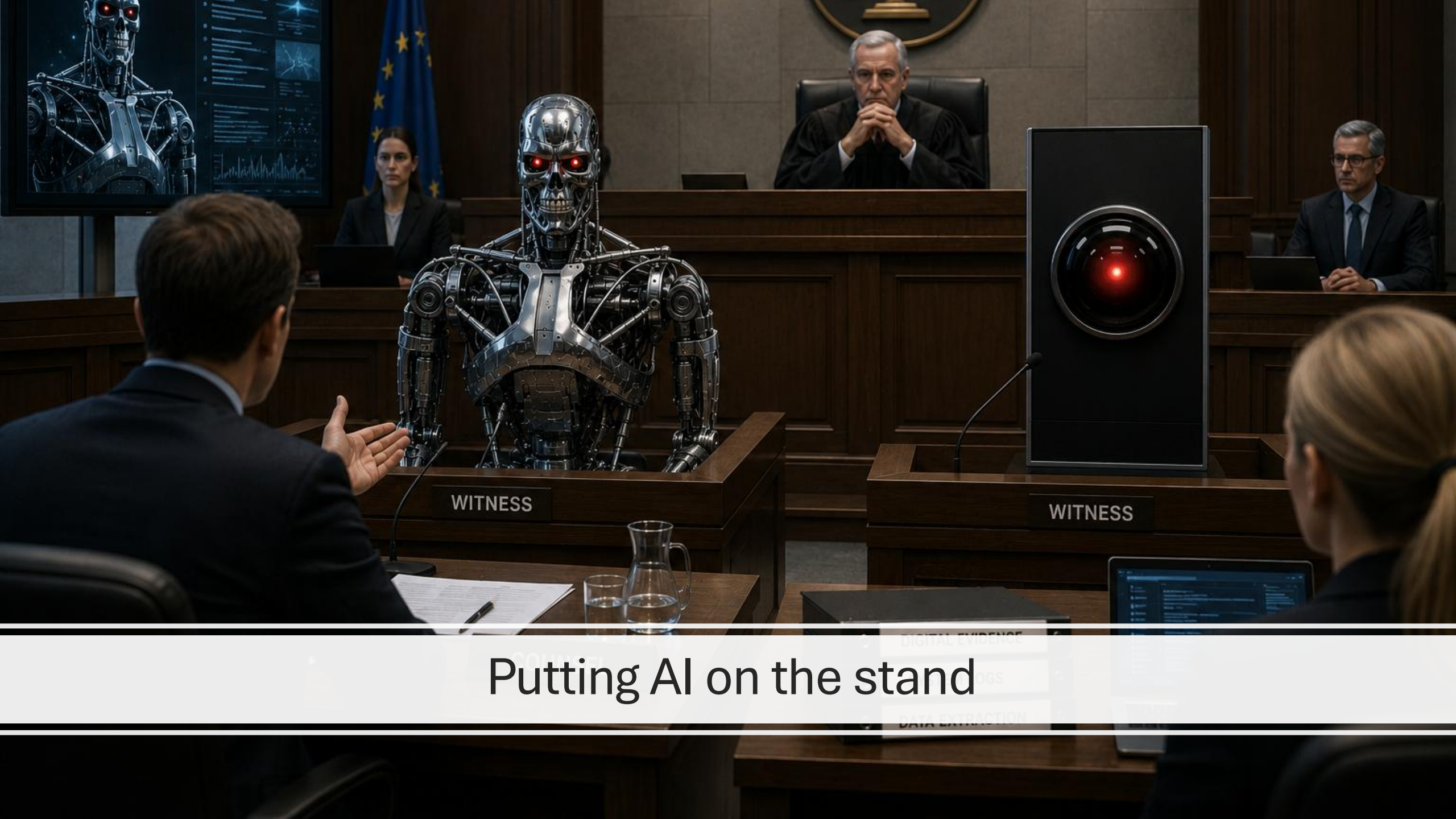
Important

Seizure should target specific data, not bulk data or full servers

Collection of evidence with AI

AI for evidence collection and analysis

1. New requisites
2. New challenges to the defense
    1. The black box problem
    2. Hidden filtering of evidence
    3. Automation bias
    4. Lack of disclosure
    5. Reproducibility problems
    6. Ai-Generated investigative leads
    7. Resource asymmetry



Putting AI on the stand

US • 8 MIN READ

How ChatGPT conversations became ‘a treasure trove’ of evidence in criminal investigations

MAY 2, 2026

By  Eric Levenson

Last October, federal prosecutors charged **Jonathan Rinderknecht with arson** for allegedly starting a fire that later developed into the destructive Palisades Fire in California. Part of the evidence included his requests to ChatGPT. He asked the app to produce an image of people running from a fire, and he said that he once burned a Bible and “felt so liberated,” according to an affidavit in support of a criminal complaint.

Closing remarks

Thank you!
Obrigado!

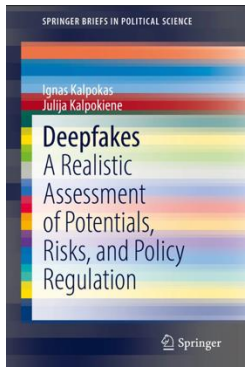
David Silva Ramalho
dsramalho@mlgts.pt

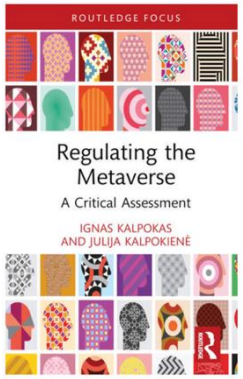
FROM IDENTITY TO CONTENT TO EVIDENCE: IS OUR (MIS)TRUST MISPLACED IN THE AGE OF DEEPFAKES AND AGENTIC AI?

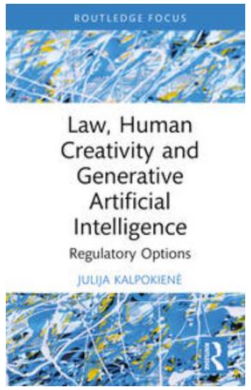
dr. Julija Kalpokienė, LL.M
15-16 June 2026 Zagreb
ERA: #DIGITALISATION and #AI in Criminal Justice

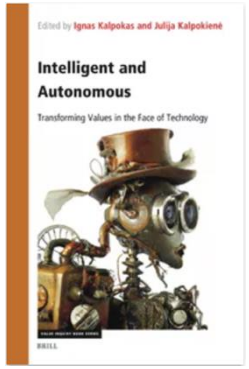
Co-funded by the European Union.
Views and opinions expressed are however those of ERA only and do not necessarily reflect those of the European Union or European Commission.
Neither the European Union nor the granting authority can be held responsible for them.

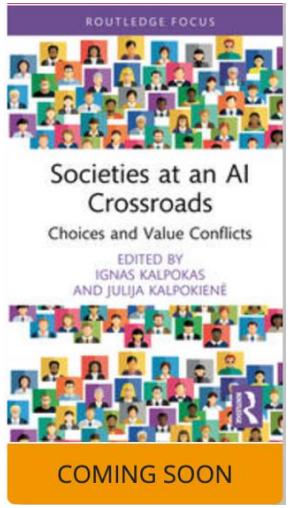
DALL-E "Lawyers having fun in Zagreb"











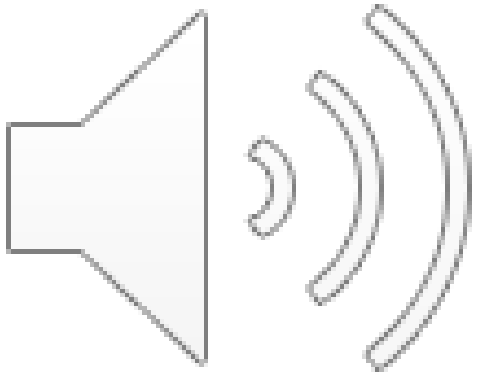
ABOUT ME

www.linkedin.com/in/techlawexpert

- Practicing lawyer - advokatas (Lithuania & Germany)
  kalpokiene@rickert.law | www.rickert.law
- Assoc. Prof. & Researcher at Vytautas Magnus University
- Postdoc Fellow at Vilnius University

LET'S LISTEN…

Canva generated image



Voice generated with Luvvoice

OUTLINE

- Deepfakes and generative AI: the expanding spectrum of synthetic outputs
- Automation and agentic AI: scaling content creation and deception
- Digital crime: a few examples
- Risks and opportunities of automation

Jon Stone

Deepfakes Surge in 2025, Raising Alarms for Financial Institutions

BBC

Home News Sport Business Innovation Culture Arts Travel Earth Audio Video Live

Deepfakes

19 Sep 2025

Friend stole my face for deepfake nudes – now I want tougher laws

The victim of one of the first deepfake prosecutions in Scotland says the law needs to change to protect victims.

19 Aug 2025

Man sent friends nude deepfakes of woman from high school

Callum Brooks was fined for altering the pictures of the woman and sharing them with his friends without her consent.

9 Aug 2025

Elon Musk's AI accused of making explicit AI Taylor Swift videos

Grok Imagine's "spicy" mode made explicit videos of Taylor Swift, according to The Verge and Gizm

Screenshot

AI · ARTIFICIAL INTELLIGENCE

Asia

Finance companies fight back against AI deepfakes, with over 70% of new enrollment attempts to some firms being fake

BY **LIONEL LIM**
ASIA REPORTER

August 13, 2025 at 3:05 AM EDT

CFO

Opinion Library Events Press Releases Topics

92% of companies have experienced financial loss due to a deepfake

Deepfake fraud attempts have taken form in both audio and video format at an increasing rate, according to new data from Regula.

Published Nov. 6, 2024

SCRIPPS NEWS

Viral celebrity deepfake ad warns of AI being used 'trick you into not voting'

A video with more than 6 million views on YouTube is warning voters to pay closer attention to what they see and hear online.

Forbes

The Dark Side Of AI: How Deepfakes And Disinformation Are Becoming A Billion-Dollar Business Risk

Bernard Marr Contributor

Follow

Nov 6, 2024, 01:43am EST

abc NEWS Video Live Shows Elections 538 Shop

2024 Election Dashboard Results Map State Results Exit Polls

AI deepfakes a top concern for election officials with voting underway

Artificial intelligence could be weaponized on voters, feds warn

How deepfakes, nudes and teen misogyny have changed growing up

Gendered misconduct on the rise, female teachers scared of being “deepfaked” and parents protecting badly behaved boys: this is high school in 2024.

By Bri Lee for ABC’s Long Read

Teenagers

Sat 2 Nov

Live Shows ••• CBS NEWS

FBI warns of deepfake videos ahead of Election Day

The Federal Bureau of Investigation is warning the public about two videos falsely claiming to be from the FBI on election security. One mentions the apprehension of groups committing ballot fraud and the other has to do with second gentleman Doug Emhoff. The bureau stresses that the videos are not authentic, are not from the FBI and the content they depict is false. CBS News Homeland Security and Justice reporter Nicole Sganga has more.

NOV 4, 2024

Legal Cheek

NEWS MOST LISTS RESOURCES JOURNAL EVENTS FAIRS VAC SCHEME

NEWS

US judge stops case after lawyers on both sides cite AI-hallucinated cases

By Legal Cheek on Jun 11 2026 8:45am

BBC

Home News Football 2026 Sport Business Technology Health Culture Arts Travel Earth Audio Video Live

Police officer accused of creating AI evidence

2 days ago

Share Save Add as preferred on Google

Samantha Noble

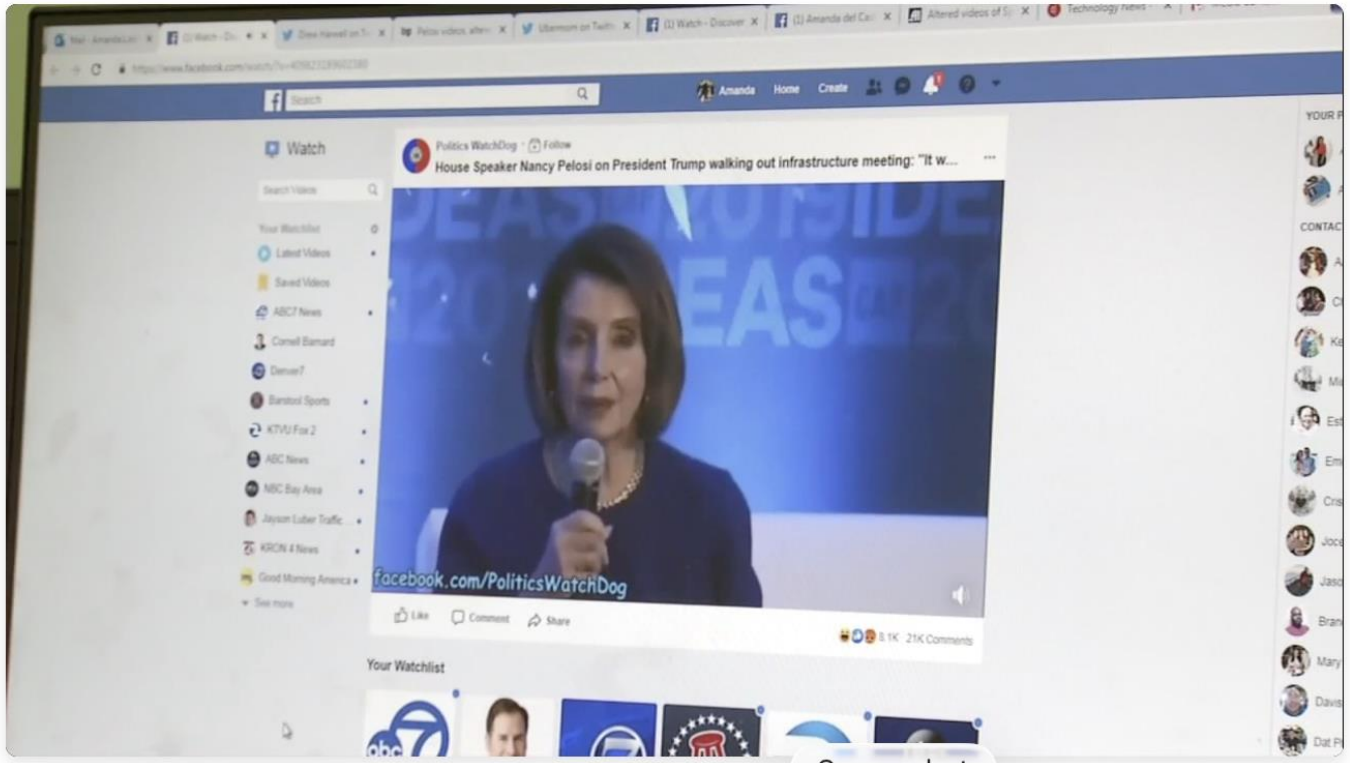
East Midlands

RISKS ALL AROUND US?

- Shallow fakes
- OSINT
  - Data shared by us
  - Data leaked and/or sold online
- Generative AI
- Deepfakes
  - Risks
  - Opportunities
  - A constant race?

Facebook says doctored Nancy Pelosi video does not violate its policy

Saturday, May 25, 2019



Screenshot

Facebook says it's not planning to take down the doctored video of House [redacted] elosi that's going viral.

SHALLOW FAKE

May 2019:
Nancy Pelosi
(House
speaker, the
Democrats)

DEEPFAKES – HOW SCARY ARE THEY?

- Media (image, video, sound):
  - Either created by AI or
  - Manipulated by AI
  - E.g.: face swapping or facial manipulation
- What is required to create a deepfake?
  - Photos / videos (publicly available images may suffices)
  - Text / sound
- Increasingly a mobile device suffices to generate relatively good quality deepfakes:
  - Cheap,
  - Quick to generate,
  - Undetectable without special tools.

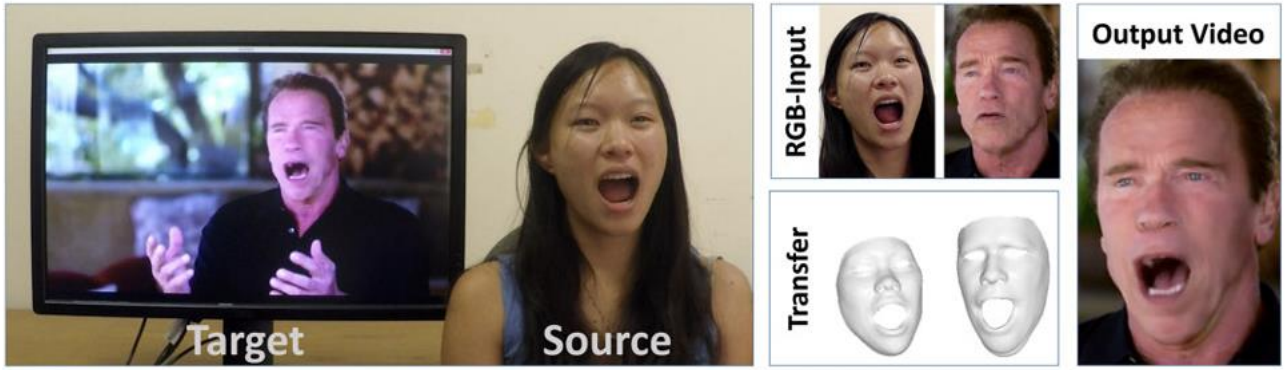
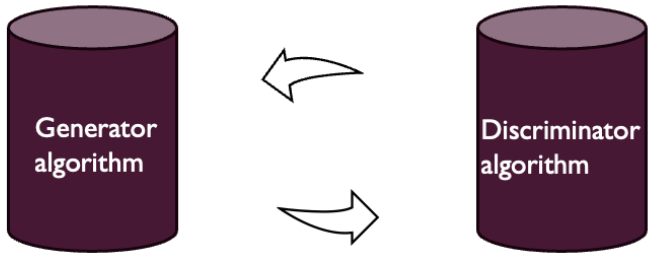


Figure 1. Illustration of Face2Face method. Image credits: Thies and Others.

Edvinas Meskys, Aidas Liaudanskas, Julija Kalpokiene and Paulius Jurcys. "Regulating deep fakes: legal and ethical considerations" Journal of Intellectual Property Law & Practice, 2020, Vol. 15, No. 1



trained using samples (images, audio, and/or video) & tasked to create a new piece of media or manipulate an existing one

trained to recognise certain features & points out where the "generator" missed something and has to go back and correct any inconsistencies

WHAT'S AVAILABLE?

- Text in any language
- Image / Face / Video
- Voice: realistic or even real (generated)
- Email spoofing
- Phone spoofing
- Real time generation

LOW ENTRY – CHEAP & READILY AVAILABLE

- Various types of generation: text, voice, video
- Caters to different regions, language, etc.

WHO ARE YOU?







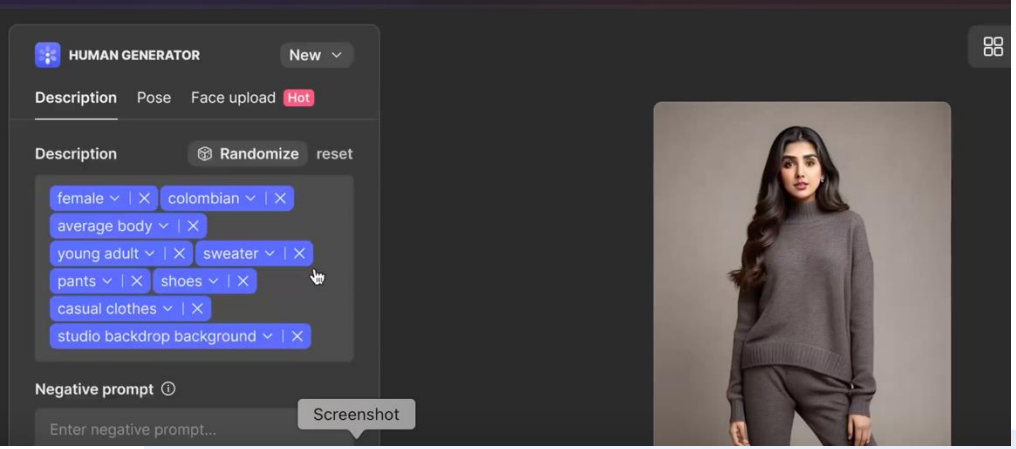


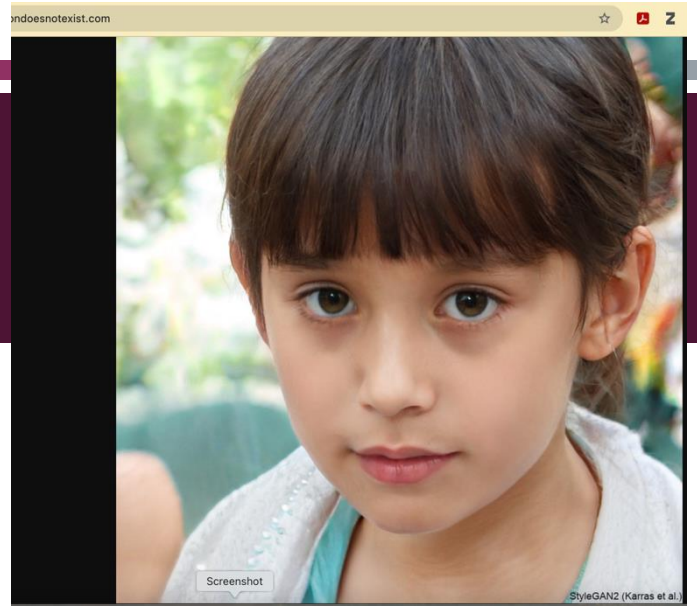

https://thispersondoesnotexist.com/

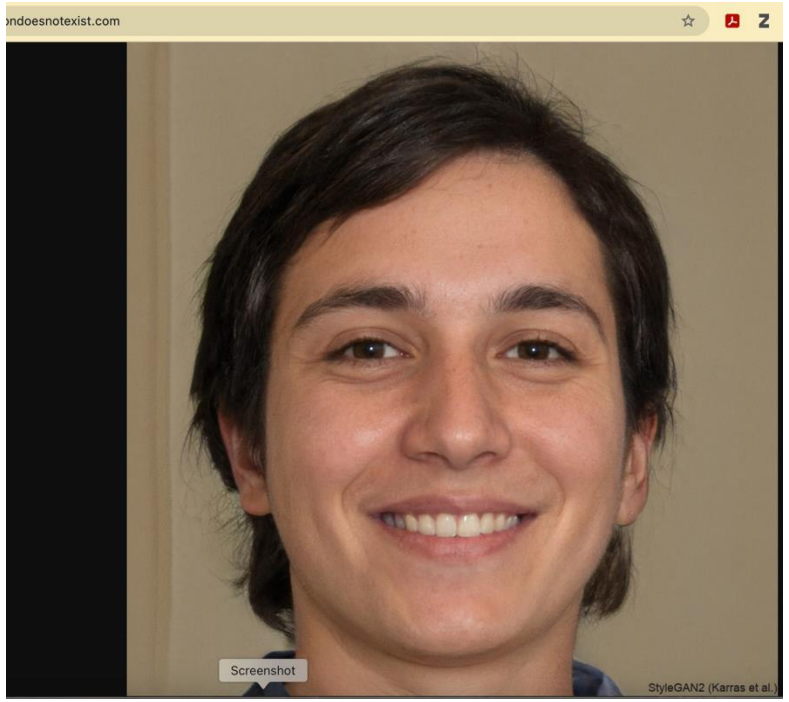
Turn God Mode on. Meet Human Generator

Create hyperrealistic full-body photos of people in real time

Create human Free



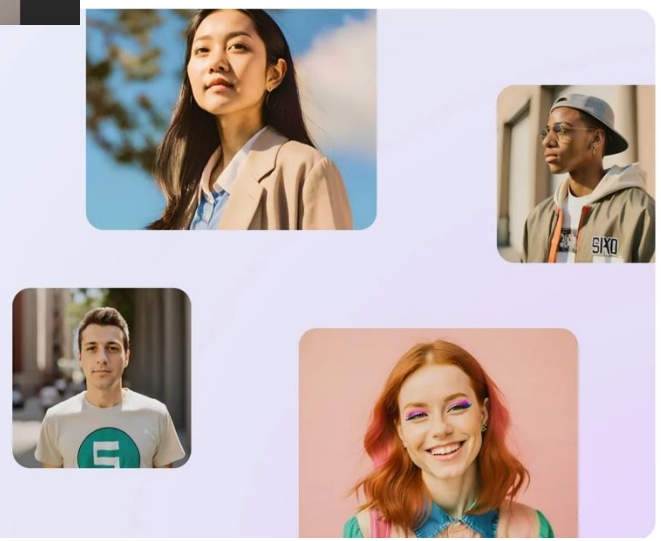




Create custom faces with the best AI face generator

Worry no more about finding the perfect stock photo with Text to Image on Canva. With the AI person generator, you can make custom, photorealistic faces for your pitch decks, websites, product demos, and more.

Create a face with AI



FACE GENERATOR

Faces

Sign in

Sex

- Male
- Female

Headpose

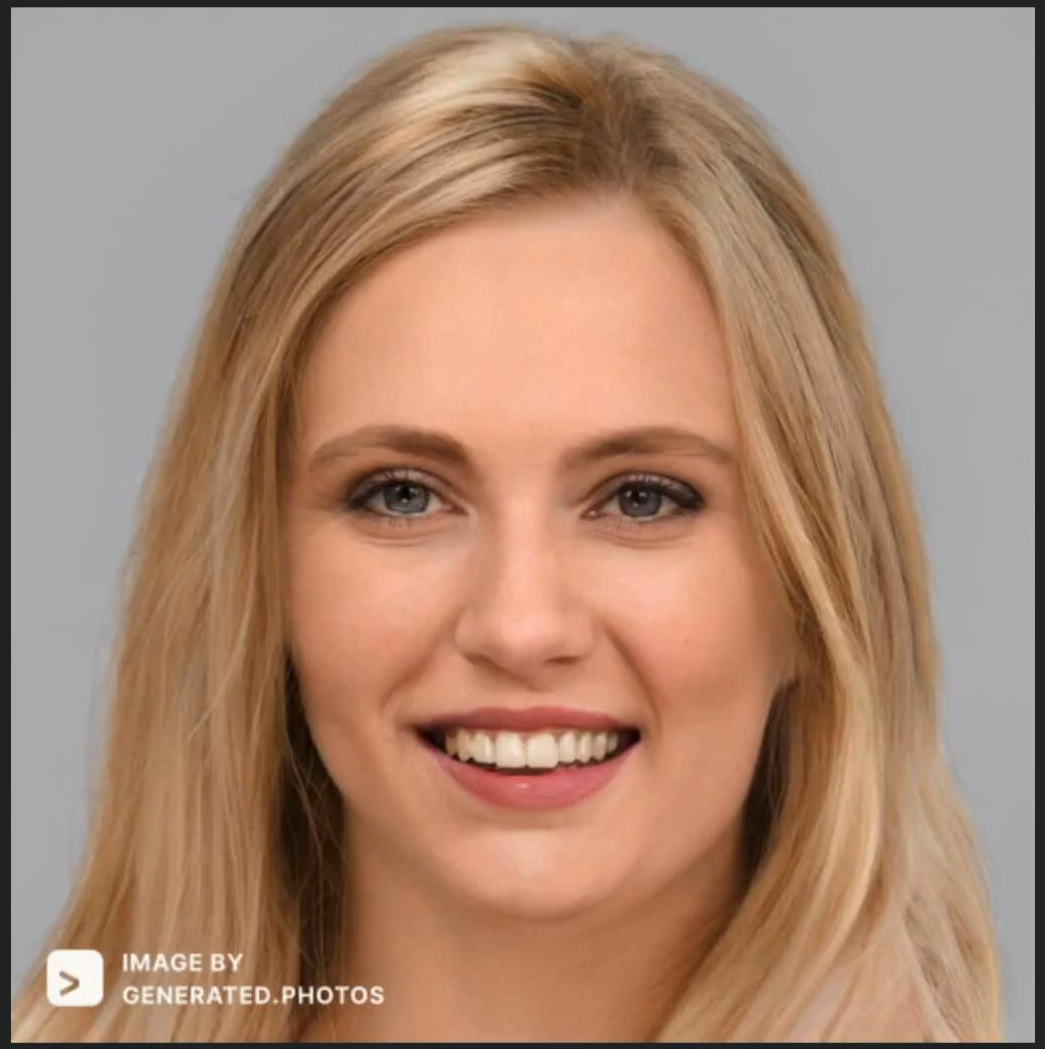
Age

Younger Older

Emotion

- Neutral
- Happy
- Surprised
- Angry
- Contemptuous
- Disgusted
- Frightened
- Sad

Skin Tone Very Fair



Download

Add to cart

Share

GENERATIVE AI & DEEPFAKES

E. g.: McDonald's commercial in Japan

SHOW ME YOUR ID // ONLINE VERIFICATION

RZECZPOSPOLITA POLSKA / REPUBLIC OF POLAND / RÉPUBLIQUE DE

PASZPORT
PASSPORT
PASSEPORT

TYPE P
IPYSTYC/CODE POL
N"CATY/PEPRONYSISI-IDE INDŻINAN'E EM 9638245

1. NAZWNO-IM I WIZMENY
MUSIELAK

2. PRITY / NAME / JCRIT / ANNAMES
BORYS ANDRZEJ

3. CI'ZONBSTWFOCTE D²BIRTH / PEBSONALAS
23 APR/AVR 1984

N JEDVOZJ NET. ID PAR EU PAN IDENTITE
60053482714

5. SEX / PLACE
M/M

AUTHORITKA / MATURTY SIGNATURE
MAZOWIECKI
WOJ. MAZOWECKIE
VOIED.

2. DATA I USZOCU / DATE DESPII / DEEXPIRY
25 STY/JAN 2023

3. DATE D EXPIRY / DATE D EXPIRY / OSSUE
25 STY/JAN 2033

P<POLMUSIELAK<<<BORYS<ANDRZEJ<<<<<<<<<<<<
EM9638245<POL8404238M3301256754<<<<<<<02

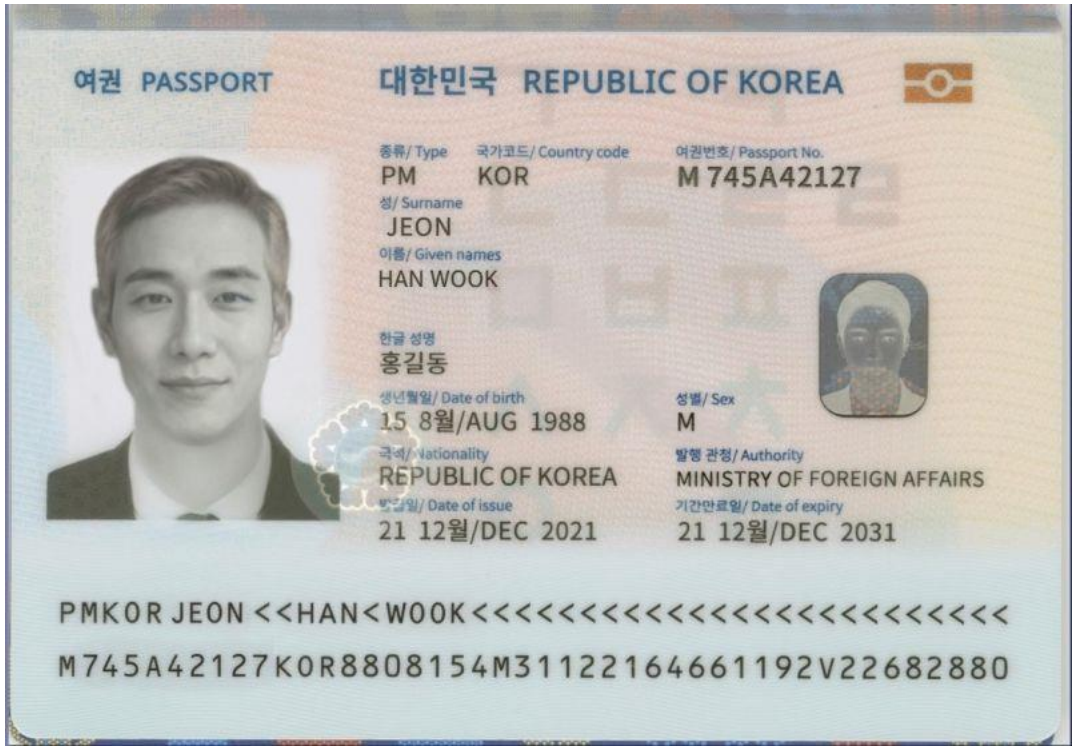
WHAT ARE THE DANGERS? HOW MUCH DO WE RELY ON VERIFICATION?

North Korean hackers use ChatGPT to forge a South Korean military ID

14 Sept. 2025, Bloomberg

How are ID documents used?
What are the verification procedures?
How much do we trust when we see an ID? E.g. a copy of it?

Other use cases: phishing, gaining trust, etc.



WHAT USE IS A DOMAIN?

- Internet Corporation for Assigned Names and Numbers (ICANN)
- Registries & Registrars
- www.is-it-fraud.org
- www.winter-fuel.is-it-fraud.org/get-scammed

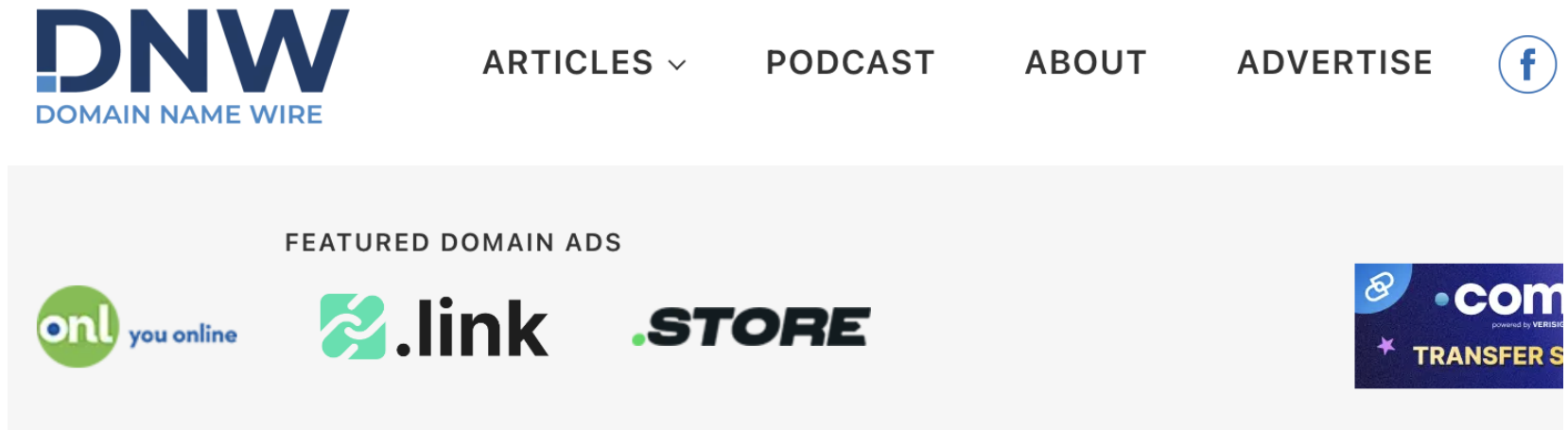
WHAT IS NEEDED?

- Register a domain (Registries & Registrars)
- Hosting a website
- May other things, such as email, SMS, etc. + payment providers
- AI + phish kits

EXAMPLES FOR DISCUSSION

- What if an ID needs to be produced?

FAKE OFFICIAL-LOOKING DOCUMENTS

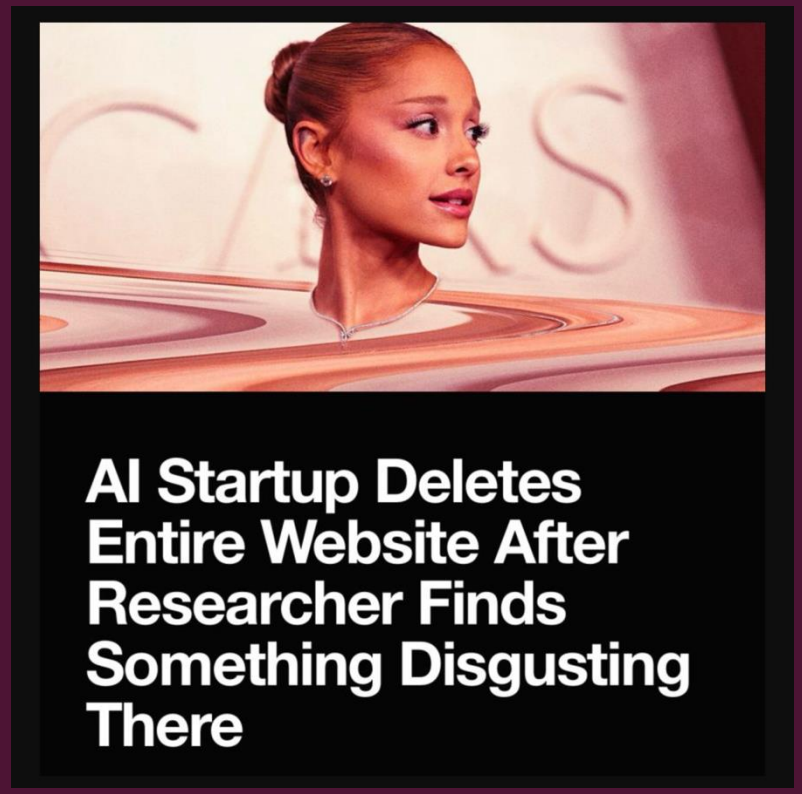


WHERE ARE WE HEADING TO?

- Black Mirror: the almond milk and nut allergy scene.
- Who drank the milk? Was it Maria?
- How far off are we?

DOES IT ALSO IMPACT THE LEGAL JUSTICE SYSTEM?

AI as a tool to perpetrate crime
AI as a tool to overwhelm and distract
AI as a tool to help prevent, detect crime



INNOVATING

- Legitimate sounding calls to get samples of your voice. -> Then a scam call in your voice to those associated with you.
- Does not need to be so sophisticated.
- Do we help with data? (e.g. LIEPA-3)

DETECTION

- May not be visible without employing detection tools
- For example, CCTV footage and Zoom calls tend to be low quality, similar as Deepfakes
- Detection tools need to be constantly improved & developed

VIDEO AS A PIECE OF EVIDENCE

- Whose responsibility is it, anyway?
- Education / training – why is it important?
- Detection: how to evaluate? Expertise?
- Expert evidence:
  - Who covers the costs?
  - Who requests?
  - How to ensure that it is detected? Technology, expert knowledge, etc.

DISCUSSION & QUESTIONS

- Let‘s keep in touch
- advokate@kalpokiene.lt | kalpokiene@Rickert.law
- LinkedIn: www.linkedin.com/in/techlawexpert

TABLE OF CONTENTS

Co-financed by the European Union

This publication has been produced with the financial support of the Justice Programme of the European Union. The content of this publication reflects only the ERA's view and the Commission is not responsible for any use that may be made of the information it contains.

BACKGROUND DOCUMENTATION

*** *All documents are hyperlinked* ***

Recent work carried out by the European Union on AI and Digitalisation

1	**The European AI ACT** Regulation (EU) 2024/1689 of the European Parliament and of the Council 13 June 2024 laying down harmonised rules on artificial intelligence and amending Regulations (EC) No 300/2008, (EU) No 167/2013, (EU) No 168/2013, (EU) 2018/858, (EU) 2018/1139 and (EU) 2019/2144 and Directives 2014/90/EU, (EU) 2016/797 and (EU) 2020/1828 (Artificial Intelligence Act)	
2	Council Decision (EU) 2023/436 of 14 February 2023 authorising Member States to ratify, in the interest of the European Union, the Second Additional Protocol to the Convention on Cybercrime on enhanced cooperation and disclosure of electronic evidence	
3	Regulation (EU) 2023/1543 of the European Parliament and of the Council of 12 July 2023 **on European Production Orders and European Preservation Orders for electronic evidence in criminal proceedings** and for the execution of custodial sentences following criminal proceedings	
4	Directive (EU) 2023/1544 of the European Parliament and of the Council of 12 July 2023 laying down harmonised rules on the designation of designated establishments and the **appointment of legal representatives for the purpose of gathering electronic evidence in criminal proceedings**	
5	Regulation (EU) 2023/2844 of the European Parliament and of the Council of 13 December 2023 on the **digitalisation of judicial cooperation and access to justice in cross-border civil, commercial and criminal matters**, and amending certain acts in the field of judicial cooperation	
6	Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market For Digital Services and amending Directive 2000/31/EC **(Digital Services Act)**	
7	Decision (EU) 2022/2481 of the European Parliament and of the Council of 14 December 2022 establishing the Digital Decade Policy Programme 2030	
8	Regulation (EU) 2021/694 of the European Parliament and of the Council of 29 April 2021 establishing the Digital Europe Programme and repealing Decision (EU) 2015/2240, OJ L 166, 11.5.2021.	

9	Regulation (EU) 2024/1183 of the European Parliament and of the Council of 11 April 2024 amending Regulation (EU) No 910/2014 as regards establishing the European Digital Identity Framework (eIDAS 2.0), OJ L 30.4.2024.	
10	European e-Justice Strategy 2024–2028, OJ C/2025/437, 16.1.2025 (ELI: C/2025/437)	

Other EU criminal justice documents

A) The institutional framework for criminal justice in the EU

A1) Main treaties and conventions

A1-01	Protocol (No 36) on Transitional Provisions
A1-02	Statewatch Analysis, "The Third Pillar acquis" after the Treaty of Lisbon enters into force, Professor Steve Peers, University of Essex, Second Version, 1 December 2009
A1-03	Consolidated version of the Treaty on the functioning of the European Union, art. 82-86 *(OJ C 326/47; 26.10.2012)*
A1-04	Consolidated Version of the Treaty on the European Union, art. 9-20 *(OJ C326/13;, 26.10.2012)*
A1-05	Charter of fundamental rights of the European Union *(OJ. C 364/1; 18.12.2000)*
A1-06	Explanations relating to the Charter of Fundamental Rights *(2007/C 303/02)*
A1-07	Convention implementing the Schengen Agreement of 14 June 1985 *(OJ L 239; 22.9.2000, P. 19)*

A2) Court of Justice of the European Union

A2-01	Court of Justice of the European Union: Presentation of the Court
A2-02	European Parliament Fact Sheets on the European Union: Competences of the Court of Justice of the European Union, April 2023
A2-03	Regulation (EU, Euratom) 2019/629 of the European Parliament and of the Council of 17 April 2019 amending Protocol No 3 on the Statute of the Court of Justice of the European Union, OJ L 111, 17 April 2019
A2-04	Consolidated Version of the Statute of the Court of Justice of the European Union (01 August 2016)
A2-05	Consolidated version of the Rules of Procedure of the Court of Justice (25 September 2012)

A3) European Convention on Human Rights (ECHR)

A3-01	Convention for the Protection of Human Rights and Fundamental Freedoms as amended by Protocols No. 11 and No. 14 together with additional protocols No. 4, 6, 7, 12 and 13, Council of Europe Convention for the Protection of Human Rights and Fundamental Freedoms as amended by Protocols Nos. 11, 14 and 15, supplemented by Protocols Nos. 1, 4, 6, 7, 12, 13 and 16, Council of Europe

A3-02	Guide on the case-law of the European Convention on Human Rights: European Union law in the Court's case-law, Council of Europe, updated on 31 August 2022
A3-03	Case of Grzeda v. Poland (Application no. 43572/18), Strasbourg, 15 March 2022
A3-04	Case of Mihalache v. Romania [GC] (Application no. 54012/10), Strasbourg, 08 July 2019
A3-05	Case of Altay v. Turkey (no. 2) (Application no. 11236/09), Strasbourg, 09 April 2019
A3-06	Case Beuze v. Belgium (Application no. 71409/10), Strasbourg, 09 November 2018
A3-07	Case of Vizgirda v. Slovenia (Application no. 59868/08), Strasbourg, 28 August 2018
A3-08	Case of Şahin Alpay v. Turkey (Application no. 16538/17), Strasbourg, 20 March 2018
A3-09	Grand Chamber Hearing, Beuze v. Belgium [GC] (Application no. 71409/10), Strasbourg, 20 December 2017
A3-10	Case of Blokhin v. Russia (Application no. 47152/06), Judgment European Court of Human Rights, Strasbourg, 23 March 2016
A3-11	Case of A.T. v. Luxembourg (Application no. 30460/13), Judgment European Court of Human Rights, Strasbourg, 09 April 2015
A3-12	Case of Blaj v. Romania (Application no. 36259/04), Judgment European Court of Human Rights, Strasbourg, 08 April 2014
A3-13	Case of Boz v. Turkey (Application no. 7906/05), Judgment European Court of Human Rights, Strasbourg, 01 October 2013 (FR)
A3-14	Case of Pishchalnikov v. Russia (Application no. 7025/04), Judgment European Court of Human Rights, Strasbourg, 24 October 2009
A3-15	Case of Salduz v. Turkey (Application no. 36391/02), Judgment, European Court of Human Rights, Strasbourg, 27 November 2008

A4) Brexit

A4-01	Trade and Cooperation Agreement between the European Union and the European Atomic Energy Community, of the one part, and the United Kingdom of Great Britain and Northern Ireland, of the other part *(OJ L 149, 30.4.2021)*
A4-02	Eurojust: Judicial cooperation in criminal matters between the European Union and the United Kingdom from 1 January 2021, 1 January 2021
A4-03	Draft text of the Agreement on the New Partnership between the European Union and the United Kingdom (UKTF 2020-14), 18 March 2020
A4-04	Draft Working Text for an Agreement on Law enforcement and Judicial Cooperation in Criminal Matters
A4-05	The Law Enforcement and Security (Amendment) (EU Exit) Regulations 2019 (2019/742), 28th March 2019
A4-06	Brexit next steps: The European Arrest Warrant, House of Commons, 20 February 2020
A4-07	Brexit next steps: The Court of Justice of the EU and the UK, House of Commons, 7 February 2020
A4-08	The Law Society, "Brexit no deal: Criminal Justice Cooperation", London, September 2019
A4-09	European Commission, Factsheet, „A „No-deal"-Brexit: Police and judicial cooperation", April 2019

A4-10	CEPS: Criminal Justice and Police Cooperation between the EU and the UK after Brexit: Towards a principled and trust-based partnership, 29 August 2018
A4-11	Policy paper: The future relationship between the United Kingdom and the European Union, 12 July 2018
A4-12	House of Lords, Library Briefing, Proposed UK-EU Security Treaty, London, 23 May 2018
A4-13	HM Government, Technical Note: Security, Law Enforcement and Criminal Justice, May 2018
A4-14	LSE-Blog, Why Britain´s habit of cherry-picking criminal justice policy cannot survive Brexit, Auke Williams, London School of Economics and Political Science, 29 March 2018
A4-15	House of Commons, Home Affairs Committee, UK-EU Security Cooperation after Brexit, Fourth Report of Session 2017-19, London, 21 March 2018
A4-16	HM Government, Security, Law Enforcement and Criminal Justice, A future partnership paper
A4-17	European Criminal Law after Brexit, Queen Mary University London, Valsamis Mitsilegas, 2017
A4-18	House of Lords, European Union Committee, Brexit: Judicial oversight of the European Arrest Warrant, 6th Report of Session 2017-19, London, 27 July 2017
A4-19	House of Commons, Brexit: implications for policing and criminal justice cooperation (24 February 2017)
A4-20	Scottish Parliament Information Centre, Briefing, Brexit: Impact on the Justice System in Scotland, Edinburgh, 27 October 2016

B) Mutual legal assistance

B1) Legal framework

B1-01	Council Act of 16 October 2001 establishing in accordance with Article 34 of the Treaty on European Union, the Protocol to the Convention on Mutual Assistance in Criminal Matters between the Member States of the European Union *(2001/C 326/01), (OJ C 326/01; 21.11.2001,P. 1)*
B1-02	Council Act of 29 May 2000 establishing in accordance with Article 34 of the Treaty on European Union the Convention on Mutual Assistance in Criminal Matters between the Member States of the European Union *(OJ C 197/1; 12.7.2000, P. 1)*
B1-03	Agreement between the European Union and the Republic of Iceland and the Kingdom of Norway on the surrender procedure between the Member States of the European Union and Iceland and Norway (OJ L 292, 21.10.2006, p. 2–19)
B1-04	Second Additional Protocol to the European Convention on Mutual Assistance in Criminal Matters *(Strasbourg, 8.XI.2001*)
B1-05	Additional Protocol to the European Convention on Mutual Assistance in Criminal Matters *(Strasbourg, 17.III.1978*)
B1-06	European Convention on Mutual Assistance in Criminal Matters *(Strasbourg, 20.IV.195*9)
B1-07	Third Additional Protocol to the European Convention on Extradition (*Strasbourg, 10.XI.2010*)
B1-08	Second Additional Protocol to the European Convention on Extradition *(Strasbourg, 17.III.1978)*
B1-09	Additional Protocol to the European Convention on Extradition (*Strasbourg, 15.X.1975*)

B1-10	European Convention on Extradition (*Strasbourg, 13.XII.1957*)

B2) Mutual recognition: the European Arrest Warrant

B2-01	Proposal for a Regulation of the European Parliament and of the Council on the transfer of proceedings in criminal matters, COM/2023/185 final, 5 April 2023
B2-02	European Parliament resolution of 20 January 2021 on the implementation of the European Arrest Warrant and the surrender procedures between Member States (2019/2207(INI)), *(OJ C 456, 10.11.2021)*
B2-03	Council Framework Decision 2009/299/JHA of 26 February 2009 amending Framework Decisions 2002/584/JHA, 2005/214/JHA, 2006/783/JHA, 2008/909/JHA and 2008/947/JHA, thereby enhancing the procedural rights of persons and fostering the application of the principle of mutual recognition to decisions rendered in the absence of the person concerned at the trial *(OJ L 81/24; 27.3.2009)*
B2-04	Council Framework Decision of 13 June 2002 on the European arrest warrant and the surrender procedures between Member States *(OJ L 190/1; 18.7.2002, P. 1)*
B2-05	Case law by the Court of Justice of the European Union on the European Arrest Warrant – Overview, Eurojust, 15 March 2020
B2-06	Case C-142/22, OE, Judgment of the Court (Second Chamber), 6 July 2023
B2-07	Case C-699/21, E.D.L, Judgment of the Court (Grand Chamber), 18 April 2023
B2-08	Joined Cases C-514/21 and C-515/21, LU and PH, Judgment of the Court (Fourth Chamber), 23 March 2023
B2-09	Case C-158/21, Puig Gordi and Others, Judgment of the Court (Grand Chamber), 31 January 2023
B2-10	Case C-168/21, Procureur général près la cour d'appel d'Angers, Judgment of the Court (Third Chamber), 14 July 2022
B2-11	Joined Cases C-562/21 PPU and C-563/21 PPU, Openbaar Ministerie (Tribunal établi par la loi dans l'État membre d'émission), Judgment of the Court (Grand Chamber), 22 February 2022
B2-12	Case C-649/19, Spetsializirana prokuratura (Déclaration des droits), Judgement of the Court (Fifth Chamber), 28 January 2021
B2-13	Case C-414/20 PPU, MM, Judgment of the Court (Third Chamber), 13 January 2021
B2-14	Joined Cases C-354/20 PPU and C-412/20 PPU, Openbaar Ministerie (Indépendance de l'autorité judiciaire d'émission), Judgement of the Court (Grand Chamber), 17 December 2020
B2-15	Case C-416/20 PPU, Generalstaatsanwaltschaft Hamburg, Judgement of the Court (Fourth Chamber), 17 December 2020
B2-16	Case C-584/19, A and Others, Judgement of the Court (Grand Chamber), 8 December 2020
B2-17	Case C-510/19, AZ, Judgement of the Court (Grand Chamber), 24 November 2020
B2-18	Case C-717/18, X (European arrest warrant – Double criminality) Judgement of the Court of 3 March 2020
B2-19	Case C-314/18, SF Judgement of the Court of 1 March 2020
B2-20	Joined Cases C-566/19 PPU (JR) and C-626/19 PPU (YC), Opinion of AG Campos Sánchez-Bordona, 26 November 2019
B2-21	Case C-489/19 PPU (NJ), Judgement of the Court (Second Chamber) of 09 October 2019

B2-22	Case 509/18 (PF), Judgement of the Court (Grand Chamber), 27 May 2019
B2-23	Joined Cases C-508/18 (OG) and C-82/19 PPU (PI), Judgement of the Court (Grand Chamber), 24 May 2019
B2-24	The Guardian Press Release: Dutch court blocks extradition of man to 'inhumane' UK prisons, 10 May 2019
B2-25	Case 551/18, IK, Judgement of the Court of 06 December 2018 (First Chamber)
B2-26	CJEU Press Release No 141/18, Judgement in Case C-207/16, Ministerio Fiscal, 2 October 2018
B2-27	CJEU Press Release No 135/18, Judgement in Case C-327/18 PPU RO, 19 September 2019
B2-28	Case C-268/17, AY, Judgement of the Court of 25 July 2018 (Fifth Chamber)
B2-29	Case C-220/18 PPU, ML, Judgement of the Court of 25 July 2018 (First Chamber)
B2-30	Case C-216/18 PPU, LM, Judgement of the Court of 25 July 2018 (Grand Chamber)
B2-31	InAbsentiEAW, Background Report on the European Arrest Warrant - The Republic of Poland, Magdalena Jacyna, 01 July 2018
B2-32	Case C-571/17 PPU, Samet Ardic, Judgment of the court of 22 December 2017
B2-33	C-270/17 PPU, Tupikas, Judgment of the Court of 10 August 2017 (Fifth Chamber)
B2-34	Case C-271/17 PPU, Zdziaszek, Judgment of the Court of 10 August 2017 (Fifth Chamber)
B2-35	Case C-579/15, Popławski, Judgement of the Court (Fifth Chamber), 29 June 2017
B2-36	Case C-640/15, Vilkas, Judgement of the Court (Third Chamber), 25 January 2017
B2-37	Case C-477/16 PPU, Kovalkovas, Judgement of the Court (Fourth Chamber), 10 November 2016
B2-38	Case C-452/16 PPU, Poltorak, Judgement of the Court (Fourth chamber), 10 November 2016
B2-39	Case C-453/16 PPU, Özçelik, Judgement of the Court (Fourth Chamber), 10 November 2016
B2-40	Case C-294/16 PPU, JZ v Śródmieście, Judgement of the Court (Fourth Chamber), 28 July 2016
B2-41	Case C241/15 Bob-Dogi, Judgment of the Court (Second Chamber) of 1 June 2016
B2-42	C-108/16 PPU Paweł Dworzecki, Judgment of the Court (Fourth Chamber) of 24 May 2016
B2-43	Cases C-404/15 Pál Aranyosi and C-659/15 PPU Robert Căldăraru, Judgment of 5 April 2016
B2-44	Case C-237/15 PPU Lanigan, Judgment of 16 July 2015 (Grand Chamber)
B2-45	Case C-168/13 PPU *Jeremy F / Premier ministre*, Judgement of the court (Second Chamber), 30 May 2013
B2-46	Case C-399/11 *Stefano Melloni v Ministerio Fiscal*, Judgment of of 26 February 2013
B2-47	Case C-396/11 Ciprian Vasile Radu, Judgment of 29 January 2013
B2-48	C-261/09 Mantello, Judgement of 16 November 2010
B2-49	C-123/08 Wolzenburg, Judgement of 6 October 2009
B2-50	C-388/08 Leymann and Pustovarov, Judgement of 1 December 2008
B2-51	C-296/08 Goicoechea, Judgement of 12 August 2008
B2-52	C-66/08 Szymon Kozlowski, Judgement of 17 July 2008

B3) Mutual recognition: freezing and confiscation and asset recovery

B3-01	European Judicial Network (for information on mutual recognition of freezing and confiscation orders, including on competent authorities), 14 December 2020, last reviewed on 24 July 2023
B3-02	Moneyval 64th Plenary Meeting report, Strasbourg, 5 January 2023
B3-03	Proposal for a Directive of the European Parliament and of the Council on asset recovery and confiscation *(Brussels, 25.5.2022, COM (2022) 245 final)*
B3-04	Proposal for a Regulation of the European Parliament and of the Council establishing the Authority for Anti-Money Laundering and Countering the Financing of Terrorism and amending Regulations (EU) No 1093/2010, (EU) 1094/2010, (EU) 1095/2010, *(Brussels, 20.7.2021 COM(2021) 421 final)*
B3-05	FATF, COVID-19-related Money Laundering and Terrorist Financing Risk and Policy Responses, Paris, 4 May 2020
B3-06	Money-Laundering and COVID-19: Profit and Loss, Vienna, 14 April 2020
B3-07	FATF President Statement – COVID-19 and measures to combat illicit financing, Paris 1 April 2020
B3-08	Moneyval Plenary Meeting report, Strasbourg, 31 January 2020
B3-09	Directive (EU) 2019/1153 of the European Parliament and of the Council of 20 June 2019, laying down rules facilitating the use of financial and other information for the prevention, detection, investigation or prosecution of certain criminal offences, and repealing Council Decision 2000/642/JHA
B3-10	Commission Delegated Regulation (EU) …/... of 13.2.2019 supplementing Directive (EU) 2015/849 of the European Parliament and of the Council by identifying high-risk third countries with strategic deficiencies, C(2019) 1326 final
B3-11	Regulation 2018/1805 of the European Parliament and of the Council on the mutual recognition of freezing and confiscation orders, L 303/1, Brussels, 14 November 2018
B3-12	Directive (EU) 2018/1673 of the European Parliament and of the Council of 23 October 2018 on combating money laundering by criminal law, L 284/22
B3-13	Directive (EU) 2018/843 of the European Parliament and of the Council of 30 May 2018 amending Directive (EU) 2015/849 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing, and amending Directives 2009/138/EC and 2013/36/EU (Text with EEA relevance), PE/72/2017/REV/1 OJ L 156, p. 43–74, 19 June 2018
B3-14	Directive (EU) 2017/541 of the European Parliament and of the Council of 15 March 2017 on combating terrorism and replacing Council Framework Decision 2002/475/JHA and amending Council Decision 2005/671/JHA
B3-15	Regulation (EU) 2016/1675 of 14 July 2016 supplementing Directive (EU) 2015/849 of the European Parliament and of the Council by identifying high-risk third countries with strategic deficiencies (Text with EEA relevance)
B3-16	Directive (EU) 2015/849 of the European Parliament and of the Council of 20 May 2015 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing, amending Regulation (EU) No 648/2012 of the European Parliament and of the Council, and repealing Directive 2005/60/EC of the European Parliament and of the Council and Commission Directive 2006/70/EC (Text with EEA relevance)
B3-17	Regulation (EU) 2015/847 of the European Parliament and of the Council of 20 May 2015 on information accompanying transfers of funds and repealing Regulation (EC) No 1781/2006 (Text with EEA relevance)

B3-18	Consolidated text: Directive 2014/42/EU of the European Parliament and of the Council of 3 April 2014 on the freezing and confiscation of instrumentalities and proceeds of crime in the European Union
B3-19	Regulation (EC) No 1889/2005 of the European Parliament and of the Council of 26 October 2005 on controls of cash entering or leaving the Community
B3-20	Council Framework Decision of 26 June 2001 on money laundering, the identification, tracing, freezing, seizing and confiscation of instrumentalities and the proceeds of crime (2001/500/JHA)
B3-21	Council Decision of 17 October 2000 concerning arrangements for cooperation between financial intelligence units of the Member States in respect of exchanging information (2000/642/JHA)

B4) Mutual recognition: Convictions

B4-01	Council Framework Decision 2009/829/JHA of 23 October 2009 on the application, between Member States of the European Union, of the principle of mutual recognition to decisions on supervision measures as an alternative to provisional detention *(OJ L 294/20; 11.11.2009)*
B4-02	Council Framework Decision 2008/947/JHA on the application of the principle of mutual recognition to judgments and probation decisions with a view to the supervision of probation measures and alternative sanctions *(OJ L 337/102; 16.12.2008)*
B4-03	Council Framework Decision 2008/909/JHA of 27 November 2008 on the application of the principle of mutual recognition to judgments in criminal matters imposing custodial sentences or measures involving deprivation of liberty for the purpose of their enforcement in the European Union *(OJ L 327/27; 5.12.2008)*
B4-04	Council Framework Decision 2008/675/JHA of 24 July 2008 on taking account of convictions in the Member States of the European Union in the course of new criminal proceedings *(OJ L 220/32; 15.08.2008*)
B4-05	Case C-234/18, Judgment of 20 March 2020
B4-06	Case C-390/16, Dániel Bertold Lada, Opinion of AG Bot, delivered on 06 February 2018
B4-07	Case C-171/16, Trayan Beshkov, Judgement of the Court (Fifth Chamber), 21 September 2017
B4-08	Case C-528/15, Policie ČR,Krajské ředitelství policie Ústeckého kraje, odbor cizinecké policie v Salah Al Chodor, Ajlin Al Chodor, Ajvar Al Chodor, Judgement of the Court (Second Chamber), 15 March 2017
B4-09	Case C-554/14, Ognyanov, Judgement of the Court (Grand Chamber), 8 November 2016
B4-10	Case C-439/16 PPU, Milev, Judgement of the Court (Fourth Chamber), 27 October 2016
B4-11	C-294/16 PPU, JZ v Śródmieście, Judgement of the Court (Fourth Chamber), 28 July 2016
B4-12	C-601/15 PPU, J. N. v Staatssecretaris voor Veiligheid en Justitie, Judgement of the Court (Grand Chamber), 15 February 2016
B4-13	C-474/13, Thi Ly Pham v Stadt Schweinfurt, Amt für Meldewesen und Statistik, Judgement of the Court (Grand Chamber), 17 July 2014
B4-14	Joined Cases C-473/13 and C-514/13, Bero and Bouzalmate, Judgement of the Court (Grand Chamber), 17 July 2014
B4-15	C-146/14 PPU, Bashir Mohamed Ali Mahdi, Judgement of the Court (Third Chamber), 5 June 2014
B4-16	Case C-383/13 PPU, M. G., N. R., Judgement of the Court (Second Chamber), 10 September 2013

B5) Mutual recognition in practice: evidence and e-evidence

B5-01	Regulation (EU) 2023/1543 of the European Parliament and of the Council of 12 July 2023 on European Production Orders and European Preservation Orders for electronic evidence in criminal proceedings and for the execution of custodial sentences following criminal proceedings, *(OJ L 191, 28.7.2023)*
B5-02	Directive (EU) 2023/1544 of the European Parliament and of the Council of 12 July 2023 laying down harmonised rules on the designation of designated establishments and the appointment of legal representatives for the purpose of gathering electronic evidence in criminal proceedings, *(OJ L 191, 28.7.2023)*
B5-03	REPORT FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT AND THE COUNCIL on the implementation of Directive 2014/41/EU of the European Parliament and of the Council of 3 April 2014 regarding the European Investigation Order in criminal matters, *(Brussels, 20.7.2021, COM(2021) 409 final)*
B5-04	The European Law Blog, „E-Evidence: The way forward. Summary of a Workshop held in Brussels on 25 September 2019, Theodore Christakis, 06 November 2019
B5-05	Joint Note of Eurojust and the European Judicial Network on the Practical Application of the European Investigation Order, June 2019
B5-06	European Commission, Press Release, „Security Union: Commission recommends negotiating international rules for obtaining electronic evidence", Brussels, 05 February 2019
B5-07	EURCRIM, "The European Commission's Proposal on Cross Border Access to e-Evidence – Overview and Critical Remarks" by Stanislaw Tosza, Issue 4/2018, pp. 212-219
B5-08	Recommendation for a Council Decision authorising the opening of negotiations in view of an agreement between the European Union and the United States of America on cross-border access to electronic evidence for judicial cooperation in criminal matters, COM(2019) 70 final, Brussels, 05 February 2019
B5-09	Annex to the Recommendation for a Council Decision authorising the opening of negotiations in view of an agreement between the European Union and the United States of America on cross-border access to electronic evidence for judicial cooperation in criminal matters, COM(2019) 70 final, Brussels, 05 February 2019
B5-10	Fair Trials, Policy Brief, „The impact on the procedural rights of defendants of cross-border access to electronic data through judicial cooperation in criminal matters", October 2018
B5-11	ECBA Opinion on European Commission Proposals for: (1) A Regulation on European Production and Preservation Orders for electronic evidence & (2) a Directive for harmonised rules on the appointment of legal representatives for the purpose of gathering evidence in criminal proceedings, Rapporteurs: Stefanie Schott (Germany), Julian Hayes (United Kingdom)
B5-12	Proposal for a Directive of the European Parliament and of the Council laying down harmonised rules on the appointment of legal representatives for the purpose of gathering evidence in criminal proceedings, COM(2018) 226 final, Strasbourg, 17 April 2018
B5-13	Proposal for a Regulation of the European Parliament and of the Council on European Production and Preservation Orders for electronic evidence in criminal matters, COM(2018) 225 final, Strasbourg, 17 April 2018

B5-14	Non-paper from the Commission services: Improving cross-border access to electronic evidence: Findings from the expert process and suggested way forward *(8 June 2017)*
B5-15	Non-paper: Progress Report following the Conclusions of the Council of the European Union on Improving Criminal Justice in Cyberspace *(7 December 2016)*
B5-16	ENISA 2014 - Electronic evidence - a basic guide for First Responders (Good practice material for CERT first responders)
B5-17	Directive 2014/41/EU of 3 April 2014 regarding the European Investigation Order in criminal matters (OJ L 130/1; 1.5.2014)
B5-18	Guidelines on Digital Forensic Procedures for OLAF Staff" (Ref. Ares(2013)3769761 - 19/12/2013, 1 January 2014
B5-19	ACPO Good Practice Guide for Digital Evidence *(March 2012)*
B5-20	Council Framework Decision 2008/978/JHA of 18 December 2008 on the European evidence warrant for the purpose of obtaining objects, documents and data for use in proceedings in criminal matters *(OJ L, 350/72, 30.12.2008*)
B5-21	Council Framework Decision 2003/577/JHA of 22 July 2003 on the execution in the European Union of orders freezing property or evidence *(OJ L 196/45; 2.8.2003*)
B5-22	Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market (Directive on electronic commerce*) (Official Journal L 178/1, 17.7.2000)*
B5-23	Communication from the Commission to the European Parliament, the Council, the Economic and Social Committee and the Committee of the Regions ensuring security and trust in electronic communication - Towards a European Framework for Digital Signatures and Encryption *(COM (97) 503)*, October 1997

B6) Criminal records, Interoperability

B6-01	Regulation (EU) 2019/816 of the European Parliament and of the Council of 17 April 2019 establishing a centralised system for the identification of Member States holding conviction information on third-country nationals and stateless persons (ECRIS-TCN) to supplement the European Criminal Records Information System and amending Regulation (EU) 2018/1726) (*OJ L135/85, 22.05.2019*)
B6-02	Regulation (EU) 2019/818 of the European Parliament and of the Council of 20 May 2019 on establishing a framework for interoperability between EU information systems in the field of police and judicial cooperation, asylum and migration and amending Regulations (EU) 2018/1726, (EU) 2018/1862 and (EU) 2019/816 (*OJ L 135/85, 22.05.2019*)
B6-03	Regulation (EU) 2019/817 of the European Parliament and of the Council of 20 May 2019 on establishing a framework for interoperability between EU information systems in the field of borders and visa and amending Regulations (EC) No 767/2008, (EU) 2016/399, (EU) 2017/2226, (EU) 2018/1240, (EU) 2018/1726 and (EU) 2018/1861 of the European Parliament and of the Council and Council Decisions 2004/512/EC and 2008/633/JHA (*OJ L 135/27, 22.05.2019*)
B6-04	Directive of the European Parliament and of the Council amending Council Framework Decision 2009/315/JHA, as regards the exchange of information on third-country nationals and as regards the European Criminal Records

	Information System (ECRIS), and replacing Council Decision 2009/316/JHA, PE-CONS 87/1/18, Strasbourg, 17 April 2019
B6-05	Report from the Commission to the European Parliament and the Council concerning the exchange through the European Criminal Records Information System (ECRIS) of information extracted from criminal records between the Member States. *(COM/2017/0341 final, 29.06.2017)*
B6-06	Council Framework Decision 2009/315/JHA of 26 February 2009 on the organisation and content of the exchange of information extracted from the criminal record between Member States *(OJ L 93/23; 07.4.2009)*
B6-07	Council Decision on the exchange of information extracted from criminal records – Manual of Procedure *(6397/5/06 REV 5; 15.1.2007)*
B6-08	Council Decision 2005/876/JHA of 21 November 2005 on the exchange of information extracted from the criminal record *(OJ L 322/33; 9.12.2005)*

B7) Conflicts of jurisdiction – *Ne bis in idem*

B7-01	Case law by the Court of Justice of the European Union on the principle of ne bis in idem in criminal matters, Eurojust, April 2020 Case-law by the Court of Justice of the European Union on the Principle of ne bis in idem in Criminal Matters, Eurojust, December 2021
B7-02	Council Framework Decision 2009/948/JHA of 30 November 2009 on prevention and settlement of conflicts of exercise of jurisdiction in criminal proceedings *(OJ L 328/42; 15.12.2009, P.42*)
B7-03	European Convention on the Transfer of Proceedings in Criminal Matters (Strasbourg, 15.V.1972)

C) Procedural guarantees in the EU

C-01	Report from the Commission to the European Parliament and the Council on the implementation of Directive (EU) 2016/1919 of the European Parliament and of the Council of 26 October 2016 on legal aid for suspects and accused persons in criminal proceedings and for requested persons in European arrest warrant proceedings, COM/2023/44 final, 1 February 2023
C-02	Commission Recommendation (EU) 2023/681 of 8 December 2022 on procedural rights of suspects and accused persons subject to pre-trial detention and on material detention conditions, *(OJ L 86, 24.3.2023)*
C-03	FRA Report, Presumption of innocence and related rights – Professional perspectives, Luxembourg, 31 March 2021
C-04	FRA Report, Rights in practice: Access to a lawyer and procedural rights in criminal and European Arrest Warrant proceedings, Luxembourg, 27 September 2019
C-05	Report from the Commission to the European Parliament and the Council on the implementation of Directive 2013/48/EU of the European Parliament and of the Council of 22 October 2013 on the right of access to a lawyer in criminal proceedings and in European arrest warrant proceedings, and on the right to have a third person informed upon deprivation of liberty and to communicate with third persons and with consular authorities while deprived of liberty, COM/2019/560 final, 26 September 2019
C-06	Report from the Commission to the European Parliament and the Council on the implementation of Directive 2010/64/EU of the European Parliament and of the Council of 20 October 2010 on the right to interpretation and

	translation in criminal proceedings, COM/2018/857 final, 18 December 2018
C-07	Report from the Commission to the European Parliament and the Council on the implementation of Directive 2012/13/EU of the European Parliament and of the Council of 22 May 2012 on the right to information in criminal proceedings, COM/2018/858 final, 18 December 2018
C-08	Directive (EU) 2016/1919 of the European Parliament and of the Council of 26 October 2016 on legal aid for suspects and accused persons in criminal proceedings and for requested persons in European arrest warrant proceedings (OJ L 297/1, 4.11.2016)
C-09	Directive (EU) 2016/800 of the European Parliament and of the Council of 11 May 2016 on procedural safeguards for children who are suspects or accused persons in criminal proceedings (OJ L 132 1; 21.5.2016)
C-10	Directive 2016/343 of 9 March 2016 on the strengthening of certain aspects of the presumption of innocence and of the right to be present at the trial in criminal proceedings (11.3.2016; OJ L 65/1)
C-11	Directive 2013/48/EU of 22 October 2013 on the right of access to a lawyer in criminal proceedings and in European arrest warrant proceedings, and on the right to have a third party informed upon deprivation of liberty and to communicate with third persons and with consular authorities while deprived of liberty (OJ L 294/1; 6.11.2013)
C-12	Directive 2012/13/EU of the European Parliament and of the Council of 22 May 2012 on the right to information in criminal proceedings (1.6.2012; OJ L 142/1)
C-13	Directive 2010/64/EU of the European Parliament and of the Council of 20 October 2010 on the right to interpretation and translation in criminal proceedings *(OJ L 280/1; 26.10.2010*)
C-14	C-209/22 - Rayonna prokuratura Lovech, TO Lukovit (Fouille corporelle), 7 September 2023
C-15	C-660/21 - K.B. and F.S. (Relevé d'office dans le domaine pénal), 22 June 2023
C-16	C-430/22, C-468/22 - VB (Information du condamné par défaut), 8 June 2023
C-17	C-608/21 - Politseyski organ pri 02 RU SDVR, 25 May 2023
C-18	C-694/20 - Orde van Vlaamse Balies i in., 8 December 2022
C-19	C-348/21 - HYA and Others (Impossibilité d'interroger les témoins à charge), 8 December 2022
C-20	C-347/21 - DD (Réitération de l'audition d'un témoin), 15 September 2022
C-21	C-242/22 PPU - TL () and de traduction), 1 August 2022
C-22	C-564/19 - IS (Illégalité de l'ordonnance de renvoi), 23 November 2021
C-23	C-282/20 - ZX (Régularisation de l'acte d'accusation), 21 October 2021
C-24	C-649/19 - Spetsializirana prokuratura (Déclaration des droits), 28 January 2021
C-25	Case C-659/18, Judgement of the Court of 2 March 2020
C-26	Case C-688/18, Judgement of the Court of 3 February 2020
C-27	Case C467/18, Rayonna prokuratura Lom, Judgment of the Court of 19 September 2019
C-28	Case C-467/18 on directive 2013/48/EU on the right of access to a lawyer in criminal proceedings, EP, Judgement of the court (Third Chamber), 19. September 2019
C-29	Case C377/18, AH a. o., Judgment of the Court of 05 September 2019

C-30	Case C-646/17 on directive 2012/13/EU on the right to information in criminal proceedings, Gianluca Moro, Judgement of the Court (First Chamber), 13 June 2019
C-31	Case C-8/19 PPU, criminal proceedings against RH (presumption of innocence), Decision of the Court (First Chamber), 12. February 2019
C-32	Case C646/17, Gianluca Moro, Opinion of the AG Bobek, 05 February 2019
C-33	Case C-551/18 PPU, IK, Judgment of the Court (First Chamber), 6 December 2018
C-34	Case C-327/18 PPU, RO, Judgment of 19 September 2018 (First Chamber)
C-35	Case C-268/17, AY, Judgment of the Court (Fifth Chamber), 25 July 2018
C-36	Case C-216/18 PPU, LM, Judgment of 25 July 2018 (Grand Chamber)
C-37	Joined Cases C-124/16, C-188/16 and C-213/16 on Directive 2012/13/EU on the right to information in criminal proceedings Ianos Tranca, Tanja Reiter and Ionel Opria, Judgment of 22 March 2017 (Fifth Chamber)
C-38	Case C-439/16 PPU, Emil Milev (presumption of innocence), Judgment of the Court (Fourth Chamber), 27 October 2016
C-39	Case C-278/16 Frank Sleutjes ("essential document" under Article 3 of Directive 2010/64), Judgment of 12 October 2017 (Fifth Chamber)
C-40	C-25/15, István Balogh, Judgment of 9 June 2016 (Fifth Chamber)
C-41	Opinion of Advocate General Sharpston, delivered on 10 March 2016, Case C543/14
C-42	C-216/14 Covaci, Judgment of 15 October 2015 (First Chamber)

D) Approximating criminal law and Victims´ Rights

D1) Terrorism

D1-01	EU Centre of Expertise for Victims of Terrorism
D1-02	EU's Counter-Terrorism Coordinator
D1-03	Eurojust Meeting on Counter-Terrorism, 16-17 November 2022, Summary of Discussions, 05 April 2023
D1-04	Eurojust Casework on Counter-Terrorism: Insights 2020 – 2021, December 2021
D1-05	Regulation (EU) 2021/784 of the European Parliament and of the Council of 29 April 2021 on addressing the dissemination of terrorist content online (Text with EEA relevance), *(OJ L 172, 17.5.2021)*
D1-06	European Commission, EU Handbook on Victims of Terrorism, January 2021
D1-07	2019 Eurojust Report on Counter- Terrorism, 09 December 2020
D1-08	Communication from the Commission to the European Parliament, the European Council, the Council, the European Economic and Social Committee and the Committee of the Regions: A Counter-Terrorism Agenda for the EU: Anticipate, Prevent, Protect, Respond, 9 December 2020, COM(2020) 795 final
D1-09	Report from the Commission to the European Parliament and the Council based on Article 29(1) of Directive (EU) 2017/541 of the European Parliament and of the Council of 15 March 2017 on combating terrorism and replacing Council Framework Decision 2002/475/JHA and amending Council Decision 2005/671/JHA, COM(2020) 619 final, Brussels, 30 September 2020
D1-10	Communication from the Commission to the European Parliament, the European Council, the Council, the European Economic and Social

	Committee and the Committee of the Regions on the EU Security Union Strategy, 24 July 2020, *(COM (2020) 605 final)*
D1-11	Council Conclusions on EU External Action on Preventing and Countering Terrorism and Violent Extremism, Brussels, 16 June 2020
D1-12	Terrorism Situation and Trend Report (TE-SAT) 2019
D1-13	Communication from the Commission to the European Parliament, the European Council and the Council, Twentieth Progress Report towards an effective and genuine Security Union, COM(2019) 552 final, Brussels, 30 October 2019
D1-14	Communication from the Commission to the European Parliament, and the Council, Towards better Implementation of the EU‘s anti-money laundering and countering the financing of terrorism framework, COM(2019) 360 final, Brussels, 24 July 2019
D1-15	Directive (EU) 2019/713 of the European Parliament and of the Council of 17 April 2019 on combating fraud and counterfeiting of non-cash means of payment and replacing Council Framework Decision 2001/413/JHA, L 123/18
D1-16	Commission Delegated Regulation (EU) 2019/758 of 31 January 2019 amending Directive (EU) 2015/849 of the European Parliament and of the Council with regard to regulatory technical standards for the minimum action and the type of additional measures credit and financial institutions must take to mitigate money laundering and terrorist financing risk in certain third countries, L 125/4 (Text with EEA relevance)
D1-17	Council Decision (CFSP) 2019/25 of 08 January 2019 updating the list of persons, groups and entities subject to Articles 2, 3 and 4 of Common Position 2001/931/CFSP on the application of specific measures to combat terrorism and repealing Decision (CFSP) 2016/1136, Brussels, 08 January 2019
D1-18	Proposal for a Regulation of the European Parliament and of the Council on preventing the dissemination of terrorist content online, Brussels, 12.9.2018, *(COM(2018) 640 final)*
D1-19	Directive (EU) 2018/843 of the European Parliament and of the Council of 30 May 2018 amending Directive (EU) 2015/849 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing, and amending Directives 2009/138/EC and 2013/36/EU (Text with EEA relevance), *(OJ L 156, 19.6.2018)*
D1-20	Regulation (EU) 2017/2226 of the European Parliament and of the Council of 30 November 2017 establishing an Entry/Exit System (EES) to register entry and exit data and refusal of entry data of third-country nationals crossing the external borders of the Member States and determining the conditions for access to the EES for law enforcement purposes, and amending the Convention implementing the Schengen Agreement and Regulations (EC) No 767/2008 and (EU) No 1077/2011 (OJ L 327/20; 9.12.2017)
D1-21	Directive (EU) 2017/541 of the European Parliament and of the Council of 15 March 2017 on combating terrorism and replacing Council Framework Decision 2002/475/JHA and amending Council Decision 2005/671/JHA (OJ L 88/6)
D1-22	Council Decision (CFSP) 2016/1693 of 20 September 2016 concerning restrictive measures against ISIL (Da'esh) and Al-Qaeda and persons, groups, undertakings and entities associated with them and repealing Common Position 2002/402/CFSP, *(OJ L 255, 21.9.2016)*

D1-23	Directive (EU) 2016/681 of the European Parliament and of the Council of 27 April 2016 on the use of passenger name record (PNR) data for the prevention, detection, investigation and prosecution of terrorist offences and serious crime (OJ L 119/132; 4.5.2016)
D1-24	Council Regulation (EC) No 2580/2001 of 27 December 2001 on specific restrictive measures directed against certain persons and entities with a view to combating terrorism, *(OJ L 344, 28.12.2001)*

D2) Trafficking in Human Beings, Migrant Smuggling and Sexual Exploitation of Children

D2-01	European Parliament Briefing: Preventing and combating trafficking in human beings, June 2023
D2-02	European Parliament Briefing: Anti-trafficking in human beings, June 2023
D2-03	European Parliament resolution of 15 September 2022 on human rights violations in the context of the forced deportation of Ukrainian civilians to and the forced adoption of Ukrainian children in Russia (2022/2825(RSP)), *(OJ C 125, 5.4.2023)*
D2-04	Proposal for a DIRECTIVE OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL amending Directive 2011/36/EU on preventing and combating trafficking in human beings and protecting its victims, *(COM/2022/732 final, 19 December 2022)*
D2-05	Report from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions report on the progress made in the fight against trafficking in human beings (Fourth Report), *(COM/2022/736 final, 19 December 2022)*
D2-06	Commission Staff Working Document Impact Assessment Report accompanying the document Proposal for a Directive of the European Parliament and of the Council amending Directive 2011/36/EU on preventing and combating trafficking in human beings and protecting its victims, *(SWD/2022/425 final, 19 December 2022)*
D2-07	European Parliament resolution of 5 May 2022 on the impact of the war against Ukraine on women (2022/2633(RSP)), *(OJ C 465, 6.12.2022)*
D2-08	European Parliament At Glance: Russia's war on Ukraine: The risk of trafficking of human beings, May 2022
D2-09	Commission Staff Working Document Evaluation of Directive 2012/29/EU of the European Parliament and of the Council of 25 October 2012 establishing minimum standards on the rights, support, and protection of victims of crime, and replacing Council Framework Decision *(2001/220/JHA, SWD/2022/0179 final, 2022)*
D2-10	European Migrant Smuggling Centre 6th Annual Report – 2022
D2-11	Europol: The challenges of countering human trafficking in the digital era, As of 6 December 2021
D2-12	Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee, and the Committee of the Regions on the application of Directive 2009/52/EC of 18 June 2009 providing for minimum standards on sanctions and measures against employers of illegally staying third-country nationals, *(COM/2021/592 final, 29 September 2021)*
D2-13	Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions on the EU Strategy on Combatting Trafficking in Human Beings 2021-2025, *(COM/2021/171 final, 14 April 2021)*

D2-14	Eurojust Report on Trafficking in Human Beings, Best practice and issues in judicial cooperation, February 2021
D2-15	Report from the European Commission to the European Parliament and the Council, Third report on the progress made in the fight against trafficking in human beings (2020) as required under Article 20 of Directive 2011/36/EU on preventing and combating trafficking in human beings and protecting its victims, *(COM(2020) 661 final, Brussels, 20 October 2020)*
D2-16	Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions on a New Pact on Migration and Asylum, *(COM (2020) 609 final, 23 September 2020)*
D2-17	European Commission, Study on Data collection on Trafficking in Human Beings in the EU, September 2020
D2-18	Regulation of the European Parliament and of the Council amending Regulation (EC) No 810/2009 establishing a Community Code on Visas (Visa Code), PE-CONS 29/19, Brussels, 15 May 2019
D2-19	European Migrant Smuggling Centre - EMSC
D2-20	European Migrant Smuggling Centre – 4th Annual Activity Report, The Hague, 15 May 2020
D2-21	Report from the European Commission to the European Parliament and the Council, Second report on the progress made in the fight against trafficking in human beings (2018) as required under Article 20 of Directive 2011/36/EU on preventing and combating trafficking in human beings and protecting its victims, COM(2018) 777 final, Brussels, 03 December 2018
D2-22	European Institute for Gender Equality (EIGE) report: Gender-specific measures in anti-trafficking actions, 17 October 2018
D2-23	UNODC – Global Study on Smuggling of Migrants 2018, Vienna/New York, June 2018
D2-24	Council Conclusions on setting the EU‘s priorities for the fight against organised and serious international crime between 2018 and 2021, Brussels, 9450/17, 19 May 2017
D2-25	Directive 2011/36/EU of 5 April 2011 on preventing and combating trafficking in human beings and protecting its victims, and replacing Council Framework Decision 2002/629/JHA

D3) Cybercrime

D3-01	Internet Organised Crime Threat Assessment (IOCTA) 2023
D3-02	European Parliament Legislative Train Schedule: Horizontal cybersecurity requirements for products with digital elements in “A Europe Fit for the Digital Age”, As of 20 September 2023
D3-03	European Parliament Legislative Train Schedule: Review of the Directive on security of network and information systems in “A Europe Fit for the Digital Age”, As of 20 September 2023
D3-04	European Parliament Legislative Train Schedule: Digital operational resilience for the financial sector in “A Europe Fit for the Digital Age”, As of 20 September 2023
D3-05	European Parliament Briefing: EU cyber-resilience act, May 2023
D3-06	Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive) (Text with EEA relevance), *(OJ L 333, 27.12.2022)*
D3-07	Regulation (EU) 2022/2554 of the European Parliament and of the Council of 14 December 2022 on digital operational resilience for the financial sector

	and amending Regulations (EC) No 1060/2009, (EU) No 648/2012, (EU) No 600/2014, (EU) No 909/2014 and (EU) 2016/1011 (Text with EEA relevance), *(OJ L 333, 27.12.2022)*
D3-08	Directive (EU) 2022/2557 of the European Parliament and of the Council of 14 December 2022 on the resilience of critical entities and repealing Council Directive 2008/114/EC (Text with EEA relevance), *(OJ L 333, 27.12.2022)*
D3-09	Proposal for a Regulation of the European Parliament and of the Council on horizontal cybersecurity requirements for products with digital elements and amending Regulation (EU) 2019/1020, *(COM/2022/454 final, 15 September 2022)*
D3-10	Internet Organised Crime Threat Assessment (IOCTA) 2021
D3-11	Regulation (EU) 2021/1232 of the European Parliament and of the Council of 14 July 2021 on a temporary derogation from certain provisions of Directive 2002/58/EC as regards the use of technologies by providers of number-independent interpersonal communications services for the processing of personal and other data for the purpose of combating online child sexual abuse (Text with EEA relevance), *(OJ L 274, 30.7.2021)*
D3-12	European Commission, Public consultation on Fighting child sexual abuse: detection, removal and reporting of illegal content online, 11 February 2021
D3-13	European Judicial Cybercrime Network 9th Plenary Meeting - 2nd Outcome report 2020, 27 January 2021
D3-14	European Commission, Study on the retention of electronic communications non-content data for law enforcement purposes, Final report, September 2020
D3-15	Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions: EU strategy for a more effective fight against child sexual abuse, *(COM (2020) 607 final, Brussels, 24 July 2020)*
D3-16	Internet Organised Crime Threat Assessment (IOCTA) 2020
D3-17	Internet Organised Crime Threat Assement (IOCTA) 2019
D3-18	Special Eurobarometer 480, Report, “Europeans´ Attitudes towards Internet Security”, Brussels, March 2019
D3-19	Directive 2013/40/EU of the European Parliament and of the Council of 12 august 2013 on attacks against information systems and replacing Council Framework Decision 2005/222/JHA (Official Journal L 218/8 of 14.08.2013)
D3-20	Directive of the European Parliament and of the Council on combating the sexual abuse, sexual exploitation of children and child pornography, repealing Framework Decision 2004/68/JHA *(OJ L 335/; 17.12.2011*)
D3-21	Council Framework Decision 2005/222/JHA of 24 February 2005 on attacks against information systems *(OJ L 69/67; 16.3.2005*)
D3-22	Council Framework Decision 2004/68/JHA of 22 December 2003 on combating the sexual exploitation of children and child pornography (*OJ L 13/44; 20.1.2004*)
D3-23	Additional Protocol to the Convention on cybercrime, concerning the criminalisation of acts of a racist and xenophobic nature committed through computer systems (Strasbourg, 28.I.2003)
D3-24	Convention on Cybercrime (Budapest, 23.XI.2001)

D4) Protecting Victims´ Rights

D4-01	Proposal for a Directive of the European Parliament and of the Council amending Directive 2012/29/EU establishing minimum standards on the rights, support, and protection of victims of crime, and replacing Council Framework Decision 2001/220/JHA *(COM/2023/424 final, 12 July 2023)*

D4-02	Commission Staff Working Document: Evaluation of Directive 2012/29/EU of the European Parliament and of the Council of 25 October 2012 establishing minimum standards on the rights, support, and protection of victims of crime, and replacing Council Framework Decision 2001/220/JHA *(SWD/2022/0179 final, 28 June 2022)*
D4-03	FRA Report: "Underpinning victims' rights: support services, reporting and protection", 22 February 2023
D4-04	Proposal for a Directive of the European Parliament and of the Council on combating violence against women and domestic violence *(COM/2022/105 final, 8 March 2022)*
D4-05	D4-01 Victim Support Europe, Paper: Victim Support and Data Protection, 1st March 2021
D4-06	European Union Agency for Fundamental Rights (FRA), Report: Crime, safety, and victims' rights – Fundamental Rights Survey, 19 February 2021
D4-07	European Commission, EU Strategy on victims' rights (2020-2025), COM (2020) 258 final, Brussels, 24 June 2020
D4-08	Factsheet – EU Strategy on Victims' Rights (2020-2025), 24 June 2020
D4-09	Report from the Commission to the European Parliament and the Council on the implementation of Directive 2012/29/EU of the European Parliament and of the Council of 25 October 2012 establishing minimum standards on the rights, support, and protection of victims of crime, and replacing Council Framework Decision 2001/220/JHA *(COM/2020/188 final, 11 May 2020)*
D4-10	European Commission, Executive Summary of the Report on strengthening Victims´ Rights: From Compensation to Reparation – For a new EU Victims´ Rights Strategy 2020-2025, Report of the Special Adviser Joëlle Milquet to the President of the European Commission, Brussels, 11 March 2019
D4-11	European Commission Factsheet: The Victims' Rights Directive: What does it bring?, February 2017
D4-12	Regulation (EU) No 606/2013 of the European Parliament and of the Council of 12 June 2013 on mutual recognition of protection measures in civil matters
D4-13	European Commission, DG Justice Guidance Document related to the transposition and implementation of Directive 2012/29/EU of the European Parliament and of the Council of 25 October 2012 establishing minimum standards on the rights, support and protection of victims of crime, and replacing Council Framework Decision 2001/220/JHA
D4-14	Directive 2012/29/EU of the European Parliament and of the Council of 25 October 2012 establishing minimum standards on the rights, support and protection of victims of crime, and replacing Council Framework Decision 2001/220/JHA
D4-15	Directive 2011/99/EU of the European Parliament and of the Council of 13 December 2011 on the European protection order
D4-16	Council Directive 2004/80/EC of 29 April 2004 relating to compensation to crime victims
D4-17	Website of the European Union Agency for Fundamental Rights (FRA) – Victims' rights
D4-18	Victim Support Europe
D4-19	European Commission: Victims' Rights Platform
D4-20	EC Coordinator for victims' rights

E) Criminal justice bodies and networks

E1) European Judicial Network

E1-01	European Judicial Network, The Report on activities and management 2019-20
E1-02	Council Decision 2008/976/JHA of 16 December 2008 on the European Judicial Network (*OJ L 348/130, 24.12.2008, P. 130*)

E2) Eurojust

E2-01	Eurojust quarterly newsletter
E2-02	Eurojust Guidelines on Jurisdiction
E2-03	Working Arrangement Between The European Anti-fraud Office And the European Union Agency for Criminal Justice Cooperation, 29 March 2023
E2-04	Eurojust Annual Report 2022
E2-05	Eurojust collection of anniversary essays, 20 years of Eurojust: EU judicial cooperation in the making, 8 August 2022
E2-06	Regulation (EU) 2022/838 of the European Parliament and of the Council of 30 May 2022 amending Regulation (EU) 2018/1727 as regards the preservation, analysis and storage at Eurojust of evidence relating to genocide, crimes against humanity, war crimes and related criminal offences *(OJ L 148, 31.5.2022)*
E2-07	Guidelines for deciding on competing requests for surrender and extradition, October 2019
E2-08	Regulation (EU) 2018/1727 of the European Parliament and of the Council of 14 November 2018 on the European Union Agency for Criminal Justice Cooperation (Eurojust), and replacing and repealing Council Decision 2002/187/JHA

E3) Europol

E3-01	Europol Spotlight Series
E3-02	Europol Joint Reports
E3-03	Europol Consolidated Annual Activity Report (CAAR) 2022, 7 June 2023
E3-04	Europol Strategy: DELIVERING SECURITY IN PARTNERSHIP, 6 June 2023
E3-05	The European Union Agency for Law Enforcement Cooperation in Brief, 17 January 2023
E3-06	Europol Programming Document 2023 – 2025, Europol Public Information The Hague, 20 December 2022
E3-07	Case T-578/22: Action brought on 16 September 2022 — EDPS v Parliament and Council, *(OJ C 424, 7.11.2022)*
E3-08	Regulation (EU) 2022/991 of the European Parliament and of the Council of 8 June 2022 amending Regulation (EU) 2016/794, as regards Europol's cooperation with private parties, the processing of personal data by Europol in support of criminal investigations, and Europol's role in research and innovation, *(OJ L 169, 27.6.2022)*
E3-09	Europol Report – Beyond the Pandemic – How COVID-19 will shape the serious and organised crime landscape in the EU, 30 April 2020
E3-10	Regulation (EU) 2015/2219 of the European Parliament and of the Council of 25 November 2015 on the European Union Agency for Law Enforcement Training (CEPOL) and replacing and repealing Council Decision 2005/681/JHA

E4) European Public Prosecutor's Office

E4-01	EPPO: Internal Rules of Procedure, 29 June 2022
E4-02	Commission Implementing Regulation (EU) 2022/1504 of 6 April 2022 laying down detailed rules for the application of Council Regulation (EU) No 904/2010 as regards the creation of a central electronic system of payment information (CESOP) to combat VAT fraud, *(OJ L 235, 12.9.2022)*
E4-03	Commission Implementing Decision (EU) 2021/856 of 25 May 2021 determining the date on which the European Public Prosecutor's Office assumes its investigative and prosecutorial tasks, *(OJ L 188, 28.5.2021)*
E4-04	Working Arrangement between Eurojust and EPPO, 2021/00064, February 2021
E4-05	Working Arrangement establishing cooperative relations between the European Public Prosecutor's Office and the European Union Agency for Law Enforcement Cooperation, January 2021
E4-06	Regulation (EU, Euratom) 2020/2223 of the European Parliament and of the Council of 23 December 2020 amending Regulation (EU, Euratom) No 883/2013, as regards cooperation with the European Public Prosecutor's Office and the effectiveness of the European Anti-Fraud Office investigations, *(OJ L 437, 28.12.2020)*
E4-07	Commission Delegated Regulation (EU) 2020/2153 of 14 October 2020 amending Council Regulation (EU) 2017/1939 as regards the categories of operational personal data and the categories of data subjects whose operational personal data may be processed in the index of case files by the European Public Prosecutor's Office, *(OJ L 431, 21.12.2020)*
E4-08	Council Implementing Decision (EU) 2020/1117 of 27 July 2020 appointing the European Prosecutors of the European Public Prosecutor's Office, *(OJ L 244, 29.7.2020)*
E4-09	Decision 2019/1798 of the European Parliament and of the Council of 14 October 2019 appointing the European Chief Prosecutor of the European Public Prosecutor's Office (*OJ L 274/1, 28.10.2019*)
E4-10	Opinion on the proposal for a regulation of the European Parliament and of the Council amending Regulation (EU, Euratom) No 883/2013 concerning investigations conducted by the European Anti-Fraud Office (OLAF) as regards cooperation with the European Public Prosecutor's Office and the effectiveness of OLAF investigations Committee on Civil Liberties, Justice and Home Affairs, Rapporteur for opinion: Monica Macovei, 11.1.2019
E4-11	German Judges' Association: Opinion on the European Commission's initiative to extend the jurisdiction of the European Public Prosecutor's Office to include cross-border terrorist offences, December 2018 (only available in German)
E4-12	Communication from the Commission to the European Parliament and the European Council: A Europe that protects: an initiative to extend the competences of the European Public Prosecutor's Office to cross-border terrorist crimes, Brussels, 12.9.2018, COM(2018) 641 final
E4-13	Annex to the Communication from the Commission to the European Parliament and the European Council: A Europe that protects: an initiative to extend the competences of the European Public Prosecutor's Office to cross-border terrorist crimes, Brussels, 12.9.2018, COM (2018) 641 final
E4-14	Council Implementing Decision (EU) 2018/1696 of 13 July 2018 on the operating rules of the selection panel provided for in Article 14(3) of Regulation (EU) 2017/1939 implementing Enhanced cooperation on the establishment of the European Public Prosecutor's Office ('the EPPO')

E4-15	Annex to the Proposal for a Council Implementing Decision on the operating rules of the selection panel provided for in Article 14(3) of Regulation (EU) 2017/1939 implementing enhanced cooperation on the establishment of the European Public Prosecutor's Office (''the EPPO''), Brussels, 25.5.2018, COM(2018) 318 final)
E4-16	Csonka P, Juszczak A and Sason E, 'The Establishment of the European Public Prosecutor's Office : The Road from Vision to Reality', Eucrim - The European Criminal Law Associations' Forum, 15 January 2018
E4-17	Council Regulation (EU) 2017/1939 of 12 October 2017 implementing enhanced cooperation on the establishment of the European Public Prosecutor's Office ('the EPPO')
E4-18	Directive (EU) 2017/1371 of the European Parliament and of the Council of 5 July 2017 on the fight against fraud to the Union's financial interests by means of criminal law, *(OJ L 198, 28.7.2017)*

F) Data Protection

F-01	European Data Protection Board (EDPB)
F-02	European Data Protection Supervisor (EDPS)
F-03	Proposal for a Regulation of the European Parliament and of the Council amending Council Decision 2009/917/JHA, as regards its alignment with Union rules on the protection of personal data *(COM/2023/244 final, 11.5.2023)*
F-04	Directive (EU) 2022/228 of the European Parliament and of the Council of 16 February 2022 amending Directive 2014/41/EU, as regards its alignment with Union rules on the protection of personal data, *(OJ L 39, 21.2.2022)*
F-05	Directive (EU) 2022/211 of the European Parliament and of the Council of 16 February 2022 amending Council Framework Decision 2002/465/JHA, as regards its alignment with Union rules on the protection of personal data, *(OJ L 37, 18.2.2022)*
F-06	European Parliament Legislative Observatory, Police cooperation - joint investigation teams: alignment with EU rules on the protection of personal data, 2021/0008(COD)
F-07	EPPO College Decision 009/2020, Rules concerning the processing of personal data by the European Public Prosecutor's Office, 28 October 2020
F-08	Communication from the Commission to the European Parliament and the Council: Way forward on aligning the former third pillar acquis with data protection rules, *(COM (2020) 262 final, 24 June 2020)*
F-09	Council Decision (EU) 2016/2220 of 2 December 2016 on the conclusion, on behalf of the European Union, of the Agreement between the United States of America and the European Union on the protection of personal information relating to the prevention, investigation, detection, and prosecution of criminal offences, *(OJ L 336, 10.12.2016)*
F-10	Directive (EU) 2016/681 of the European Parliament and of the Council of 27 April 2016 on the use of passenger name record (PNR) data for the prevention, detection, investigation and prosecution of terrorist offences and serious crime, *(OJ L 119/132; 4.5.2016)*
F-11	Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such

	data, and repealing Council Framework Decision 2008/977/JHA (4.5.2016; OJ L 119/89)

G) Police Cooperation in the EU

G1) General

G1-01	Directive (EU) 2023/977 of the European Parliament and of the Council of 10 May 2023 on the exchange of information between the law enforcement authorities of Member States and repealing Council Framework Decision 2006/960/JHA, *(OJ L 134, 22 May 2023)*
G1-02	Council Recommendation (EU) 2022/915 of 9 June 2022 on operational law enforcement cooperation, *(OJ L 158, 13 June 2022)*
G1-03	Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee, and the Committee of the Regions on the EU Strategy to tackle Organised Crime 2021-2025 *(COM/2021/170 final, 14 April 2022)*
G1-04	Proposal for a Regulation of the European Parliament and of the Council on automated data exchange for police cooperation ("Prüm II"), amending Council Decisions 2008/615/JHA and 2008/616/JHA and Regulations (EU) 2018/1726, 2019/817, and 2019/818 of the European Parliament and of the Council, *(COM/2021/784 final, 8 December 2021)*
G1-05	European Commission, Press Release, "Police Cooperation Code: Boosting police cooperation across borders for enhanced security", 8 December 2021
G1-06	European Commission, Factsheet, "Reinforcing police cooperation across Europe", 8 December 2021
G1-07	Commission Staff Working Document: Impact Assessment Report accompanying the document Proposal for a Regulation of the European Parliament and of the Council on automated data exchange for police cooperation ("Prüm II"), amending Council Decisions 2008/615/JHA and 2008/616/JHA and Regulations (EU) 2018/1726, 2019/817, and 2019/818 of the European Parliament and of the Council, *(SWD/2021/378 final, Brussels, 8.12.2021)*
G1-08	Proposal for a Regulation of the European Parliament and of the Council amending Regulation (EU) 2018/1862 on the establishment, operation and use of the Schengen Information System (SIS) in the field of police cooperation and judicial cooperation in criminal matters as regards the entry of alerts by Europol, *(COM(2020) 791 final, Brussels, 9 December 2020)*
G1-09	European Commission, Inception Impact Assessment on EU Police Cooperation Code (PCC), Ref. Ares(2020)5077685, 28 September 2020
G1-10	Regulation (EU) 2018/1862 of the European Parliament and of the Council of 28 November 2018 on the establishment, operation and use of the Schengen Information System (SIS) in the field of police cooperation and judicial cooperation in criminal matters, amending and repealing Council Decision 2007/533/JHA, and repealing Regulation (EC) No 1986/2006 of the European Parliament and of the Council and Commission Decision 2010/261/EU Regulation (EU) 2022/1190 of the European Parliament and of the Council of 6 July 2022 amending Regulation (EU) 2018/1862 as regards the entry of information alerts into the Schengen Information System (SIS) on third-country nationals in the interest of the Union, *(OJ L 185, 12.7.2022)*

G1-11	Council Decision 2008/617/JHA of 23 June 2008 on the improvement of cooperation between the special intervention units of the Member States of the European Union in crisis situations, *(OJ L 210, 6.8.2008)*
G1-12	Council Decision 2008/616/JHA of 23 June 2008 on the implementation of Decision 2008/615/JHA on the stepping up of cross-border cooperation, particularly in combating terrorism and cross-border crime *(OJ L 210/12; 06.08.2008)*
G1-13	Council Decision 2008/615/JHA of 23 June 2008 on the stepping up of cross-border cooperation, particularly in combating terrorism and cross-border crime *(OJ L 210/1; 06.08.2008)*
G1-14	Council Framework Decision of 18 December 2006 on simplifying the exchange of information and intelligence between law enforcement authorities of the Member States of the European Union *(OJ L 386/89; 29.12.2006, P. 89)*
G1-15	Convention on the stepping up of cross-border cooperation, particularly in combating terrorism, cross-border crime and illegal migration of 27. May 2005 *(10900/05; 27.5.2005)*

G2) Joint Investigation Teams (JITs)

G2-01	Eurojust Information on JITs
G2-02	Europol Information on JITs
G2-03	JIT Evaluation Form
G2-04	Council of Europe: Guidelines on the use of Joint Investigation Teams
G2-05	Riehle, C. “20 years of Joint Investigations Teams (JITs) in the EU”: An overview of their development, actors and tools. ERA Forum 24, 163–167, 29 June 2023
G2-06	Checklist for multilateral joint investigation teams, 22 June 2023
G2-07	Latest trends and novelties in JIT operations: first-hand experiences of JIT practitioners and Eurojust | Eurojust | European Union Agency for Criminal Justice Cooperation (europa.eu) Fourth JITs Evaluation Report, 14 June 2023
G2-08	Regulation (EU) 2023/969 of the European Parliament and of the Council of 10 May 2023 establishing a collaboration platform to support the functioning of joint investigation teams and amending Regulation (EU) 2018/1726, OJ L 132, 17 May 2023
G2-09	Guidelines on the Network of National Experts on Joint Investigation Teams, 2 December 2020
G2-10	Third JIT Evaluation Report, Eurojust, March 2020
G-11	Joint Investigation Teams: Practical Guide, 16 December 2021
G2-12	Council Resolution on a Model Agreement for Setting up a Joint Investigation Team (JIT) – 2017/C18/01, Strasbourg, 19 January 2017
G2-13	Council Document establishing the JITs Network, 08 July 2005
G2-14	Council Framework Decision of 13 June 2002 on joint investigation teams (*OJ L 162/1; 20.6.2002*)