326DT001
Seminar #Digitalisation and #AI in Criminal Justice

Table of Contents:

1) Programme
2) Speaker's contributions (PPT)
3) Background documentation

Co-funded by
the European Union

#Digitalisation and #AI in Criminal Justice

Internet architecture, digital evidence, videolinks in trials, AI

Barcelona, 12-13 February 2026

FACE-TO-FACE

EXCELLENCE IN EUROPEAN LAW

Speakers and chairs

Patricia Ayodeji, Dual-Qualified Solicitor for England & Wales, Lawyer (Abogado) for Spain, Barcelona

María Barbancho, Criminal Lawyer, Member of the Committee of International Relations, ICAB, Barcelona

Steven David Brown, International Cybercrime Consultant, Vienna

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

Andrea Cruciani, Judge, Military Court, Naples

Gizem Gültekin-Várkonyi, Assistant Professor, Expert in EU Legal Tech, IR Expert, University of Szeged (Hungary)

Damir Kahvedžić, Senior Global Data Services Manager, ProSearch, Dublin

Natalia Martí, Lawyer, Roca Junyent Law Firm, Member of the Governing Board, Barcelona Bar Association, Barcelona

Joachim Meese, Professor, Criminal Law and Procedure, University of Antwerp; Attorney, Bar of Ghent

Andreu Van den Eynde, Lawyer in Criminal Law, ICAB, Barcelona

Cristos Velasco, Adjunct Professor of IT Law DHBW Cooperative State University, Mannheim & Stuttgart; Consultant on Cybercrime & AI

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)
- Challenges posed by websites, social networks, emails and other computer-generated or stored documents
- Presenting internet searches in court
- Videoconferencing
- Artificial intelligence (AI)

Language
English

Event number
326DT001

Organisers
ERA (Laviero Buono) in cooperation with the Barcelona Bar Association (ICAB)

Co-funded by
the European Union

#Digitalisation and #AI in Criminal Justice

Thursday, 12 February 2026

09:00 Arrival and registration of participants

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

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

Chair: Laviero Buono

09:35 **Learning the Machine**
- Binary basics
- Internet Architecture
- Logs as leads
- The Tech constant of change
- AI Implications
- The Good, the Bad and the AI

Steven David Brown

10:45 Discussion

11:00 Break

Chair: Andrea Cruciani

11:30 **Conducting forensic analysis with AI**
- Overview of recent GenAI Developments and tests
- Is it safe to use AI?
- AI use cases
- AI in mobile investigations
- Handling chat infromation

Damir Kahvedžić

12:15 Discussion

12:30 Lunch

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

Chair: Steven David Brown

13:30 **Handling electronic evidence on mobile devices in courts: perspectives of the defence**
- The importance of the chain of custody in handling the evidence
- Trial considerations: methods of presentation and admissibility tests

María Barbancho

14:00 Discussion

14:15 **Digitalisation of justice: what impact on the defence?**
Andreu Van den Eynde

14:45 Discussion

15:00 Break

15:30 **Dealing with e-evidence in cross-border cases: best practices and possible new scenarios in light of the new EU legislation**
Joachim Meese

16:00 Discussion

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 in 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. 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 for #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

ICAB Training Centre
C/Mallorca 283
08037 Barcelona
Spain

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.

16:15 **Bogus opinions and fabricated case-law: pitfalls and risks faced by legal professionals relying on Generative AI**

- Large Language Models (LLMs)
- ChatGPT
- OpenAI
- Google Gemini
- Concrete cases spanning the globe
- Implications for the administration of justice and public confidence in the justice system
- Lessons learned and regulatory bodies

Patricia Ayodeji

16:45 Discussion and end of the first day

19:30 Dinner offered by the organisers

Friday, 13 February 2026

PART III: VIDEOCONFERENCING AND ARTIFICIAL INTELLIGENCE IN CRIMINAL JUSTICE

Chair: Joachim Meese

09:30 **Remote trials, e-evidence and witness videoconferencing. Present challenges and future prospects**

- Remote trials during and after the pandemic
- Presenting e-evidence in court
- The impact of the CJEU jurisprudence
- Witness videoconferencing
- AI tools to evaluate witness evidence

Andrea Cruciani

10:15 Discussion

10:30 **Artificial Intelligence agents in cyberattacks: normative implications and the framework for public-private collaboration**
Cristos Velasco

11:15 Discussion

11:30 Break

Chair: Andrea Cruciani

12:00 **Artificial intelligence in the courtroom: a comparative analysis of machine evidence in criminal trials**
Gizem Gültekin-Várkonyi

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 Criminal Law

Julia Reitz
Assistant
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/?133868&en**

This programme has been financed by the European Union

The content of this programme reflects only ERA's view and the Commission is not responsible for any use that may be made of the information it contains.

Application

#DIGITALISATION AND #AI IN CRIMINAL JUSTICE

Barcelona, 12-13 February 2026 / Event number: 326DT001

ERA • Postfach 1640 • 54206 Trier

Customer number:

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, 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).* The number of places available is limited (30 places). Participation will be subject to a selection procedure. Selection will be first come first served and according to nationality.
2. Applications should be submitted before **2 November 2025.**
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. No supporting documents are needed. 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 Spain: 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 there are fixed rates: Portugal €53, France €82. 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 Spain the contribution for travel for a distance between 50km and 400km at is fixed at €52. 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 €234. National participants travelling between 50km and 400km one-way will receive a fixed contribution of €117. 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

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/?133868&en**

Venue

ICAB Training Centre
C/Mallorca 283
08037 Barcelona
Spain

Language

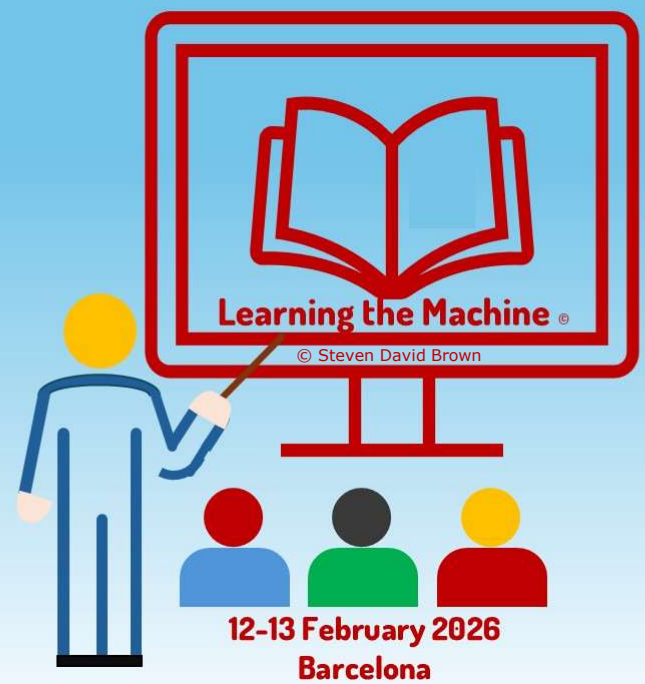
English

Contact

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

ICAB

ERA



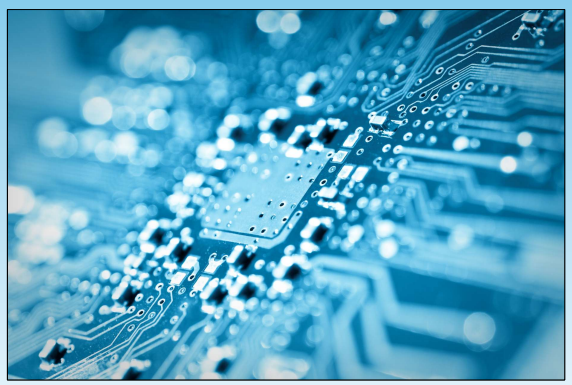
InZeit
Excellence in Acuity

12-13 February 2026
Barcelona

Co-funded by
The European
Union

1

Computer chips consist of thousands of tiny electronic transitors (switches)



bit = binary digit

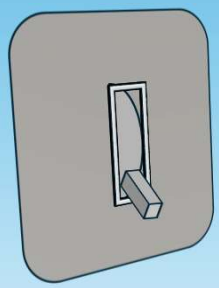
1 bit like 1 brain cell

8 bits = 1 byte

No words just zeros & ones

2

The digital alphabet ..



1 + 1 = 10

$base_2$

off or on

0 or 1

yes or no

3

Decimal

1000s	100s	10s	0-9
			2

1000s	100s	10s	0-9
		1	0
			3
		1	3

Binary

8	4	2	0
		1	0

8	4	2	0
1	0	1	0
		1	1
1	1	0	1

https://www.rapidtables.com/convert/number/decimal-to-binary.html

4

American Standard Code for Information Interchange (ASCII)

Remember:

8 bits = 1 byte

1 byte = 1 letter/digit

ASCII	SYMBOL	ASCII	SYMBOL
00110000	0	01001110	N
00110001	1	01001111	O
00110010	2	01010000	P
00110011	3	01010001	Q
00110100	4	01010010	R
00110101	5	01010011	S
00110110	6	01010100	T
00110111	7	01010101	U
00111000	8	01010110	V
00111001	9	01010111	W
01000001	A	01011000	X
01000010	B	01011001	Y
01000011	C	01011010	Z
01000100	D	00100001	!
01000101	E	00100010	
01000110	F	00100011	#
01000111	G	00100100	$
01001000	H	00100101	%
01001001	I	00100110	&
01001010	J	00101000	(
01001011	K	00101001	)
01001100	L	00101010	*
01001101	M	00101011	+

Source: cs.gsu.edu

5

C	O	M	P	U
01000011	01001111	01001101	01010000	01010101

T	E	R
01010100	01000101	01010010

(Each byte represents a character)

https://www.binaryhexconverter.com/ascii-text-to-binary-converter

6

电脑

Համակարգիչ

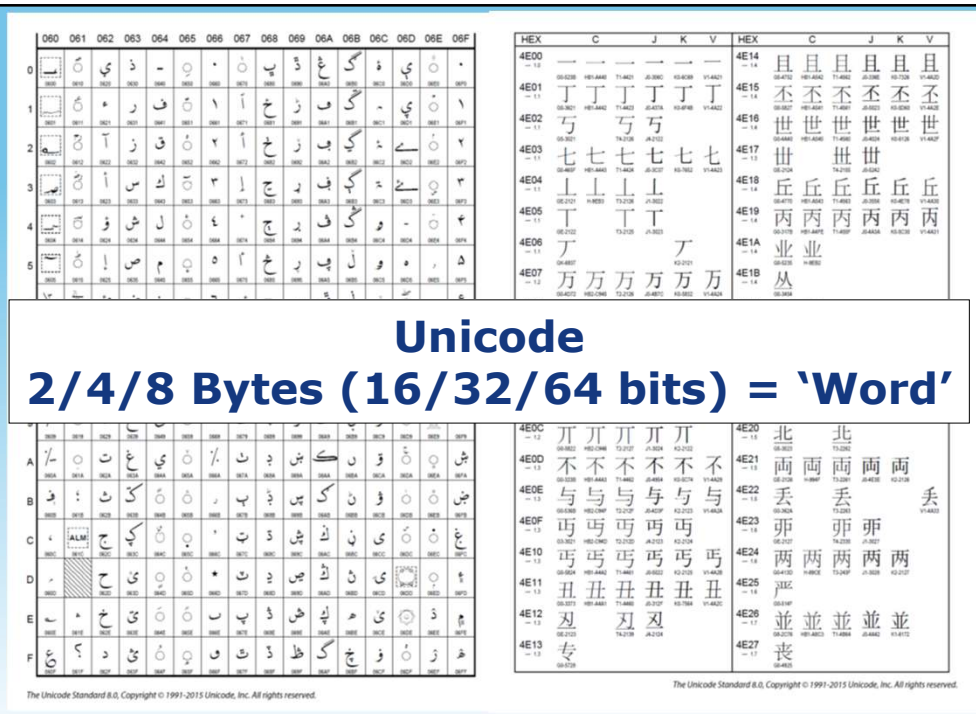
ኮምፒውተር

컴퓨터

संगणक

الحاسوب

7



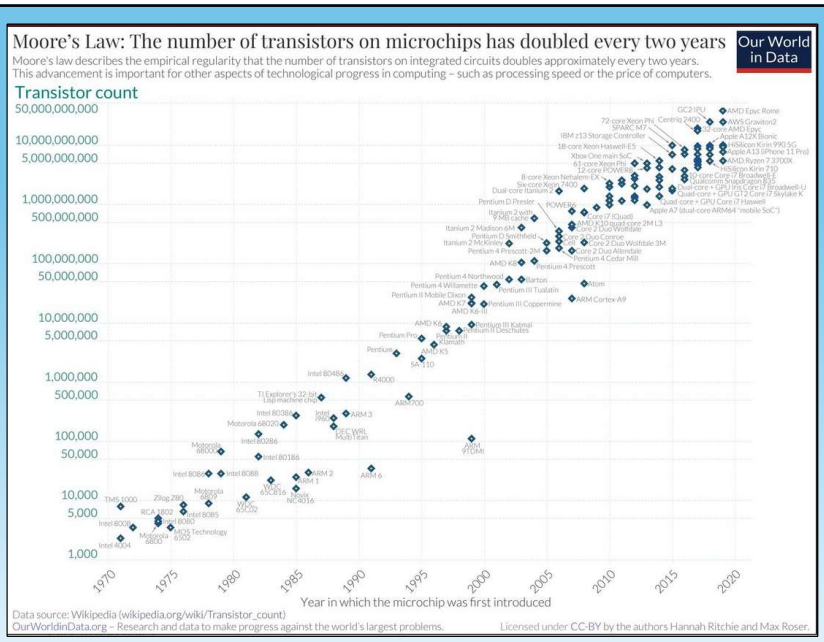
8

Gordon Moore (1965)

Number of transistors on a Microchip double in density about every 2 years

1970s
1 transistor 10 µm

Now
3 nms
(3 billionths of a metre)



Moore's Law

https://ourworldindata.org/moores-law

9

Quantum Bits - Qubits

Qubit can be On/Off or both at same time (until observed)
('superposition' like a dimmer switch)

Acts like both particle and a wave

Entanglement – pairs of qubits
Measure one, the other is opposite

https://quantumexplainer.com/qubit-vs-bit-the-key-differences-explained/

10

Qu

(‘su

Acts lik **ve**

Entanglem – pairs of qubits
Measure one, the other is opposite

“I think I can safely say that nobody understands quantum mechanics”
Richard Feynman

https://quantumexplainer.com/qubit-vs-bit-the-key-differences-explained/

11

Quantum Bits - Qubits

BUT:

Prone to error due to environmental sensitivity

Google’s Willow chip

“It performed a computation in under five minutes that would take one of today’s fastest supercomputers 10 septillion years”
(10,000,000,000,000,000,000,000,000).

https://blog.google/technology/research/google-willow-quantum-chip/

12

Memristors

Proposed 1971 Prof Leon Chua UC Berkeley

First built 2005

Stable data storage

Faster than Solid State Drives

Lower energy requirement & less heat

2022 quantum memristors demonstrated

www.memristor.org
https://instrumentationtools.com/memristor/
https://ui.adsabs.harvard.edu/abs/2022NaPho..16..318S/abstract

13

The Internet =?

…. Created by DARPA (ARPANET*)

First message "lo" [not "login"] 29 Oct 1969 Stanford → UCLA

Cold war technology

Security not included!

NOT the World Wide Web

WWW created by Tim Berners Lee 1989

A way of connecting points on the Internet

*ARPA = Advanced Research Projects Agency NET = NETwork

14

The Internet =?

Hierarchical Infrastructure of:

Interconnected Networks

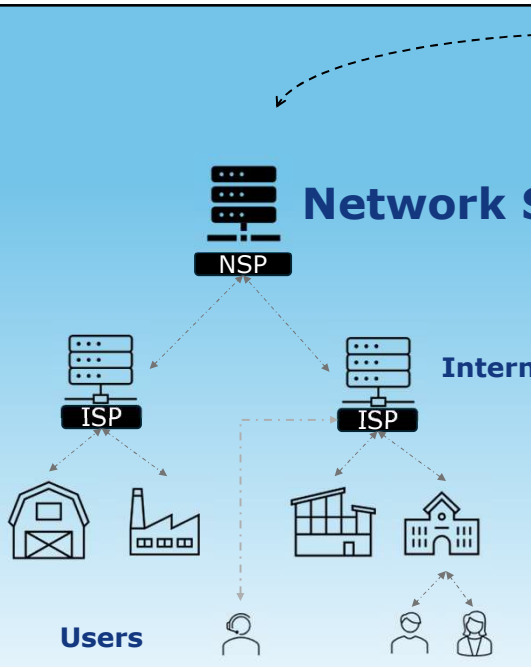
A quasi-public space (cfr shopping mall)

Gateway: Internet Service Providers (ISPs)

Assign Internet Protocol (IP) Addresses

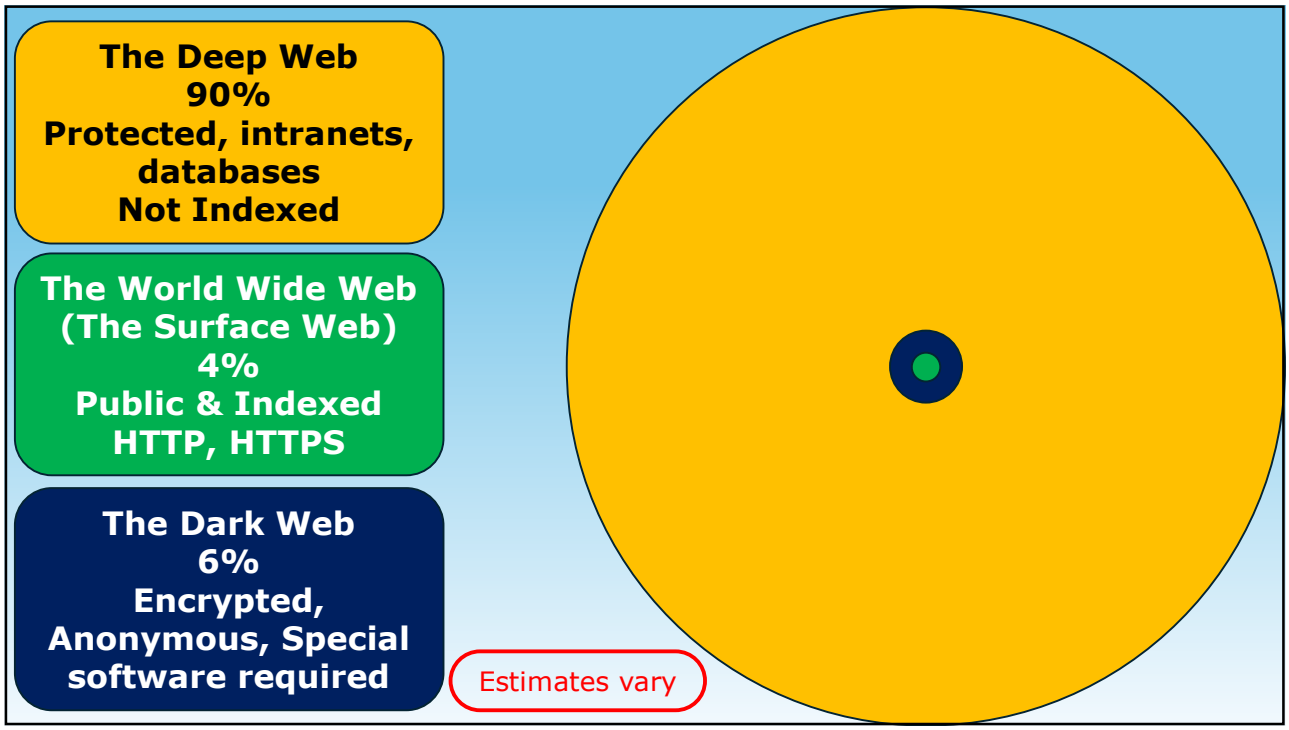
Details in this presentation have been simplified

15



IP Address:
Unique number assigned to ISP customer
Like postal address
Static/Dynamic

16

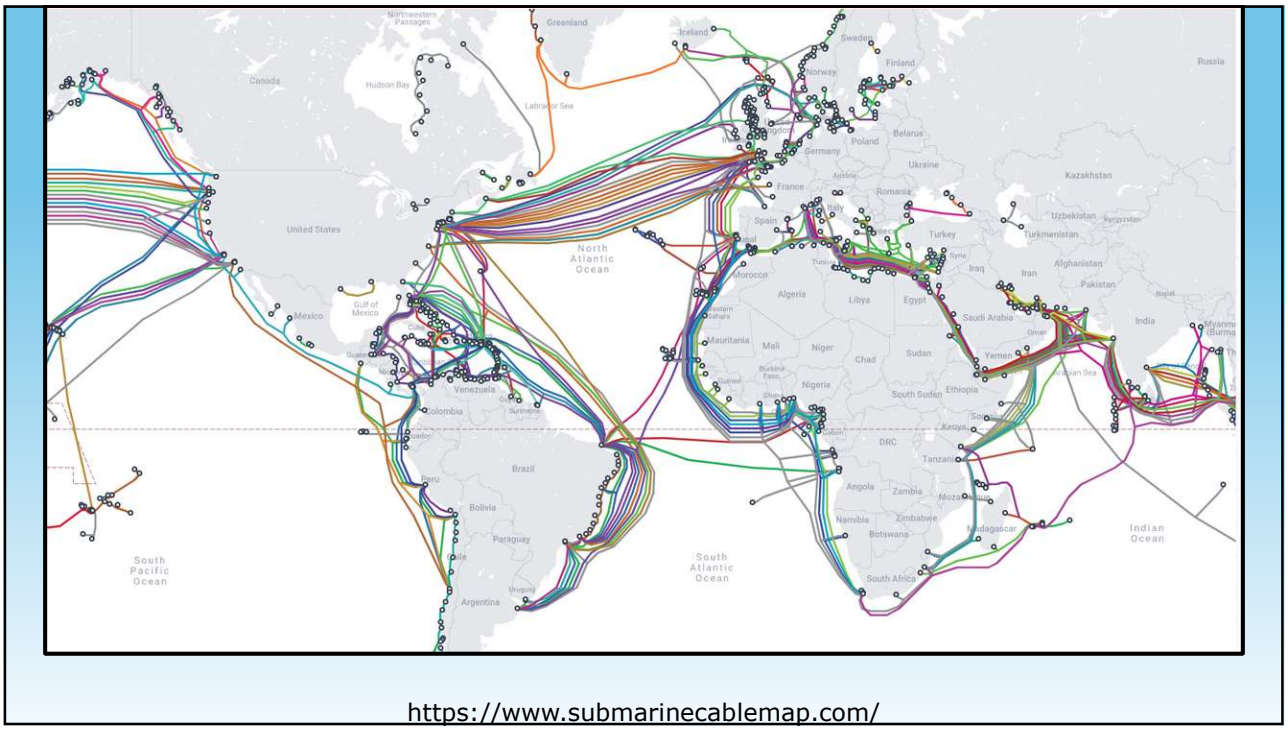


17

Data transmitted as:

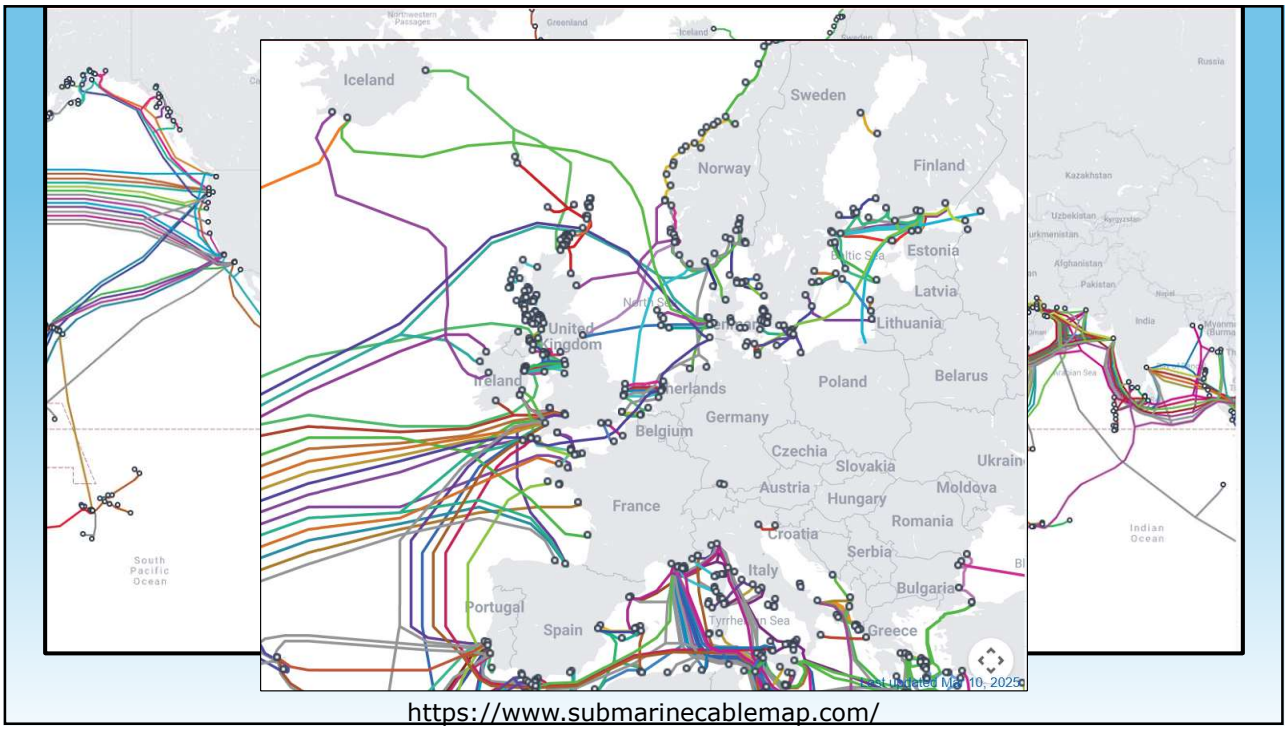
- Radiowaves or Microwaves to Access Points, Satellites
- Electrons along Copper Wires (Cables)
- Pulses of light along Fibreoptic cables

18



https://www.submarinecablemap.com/

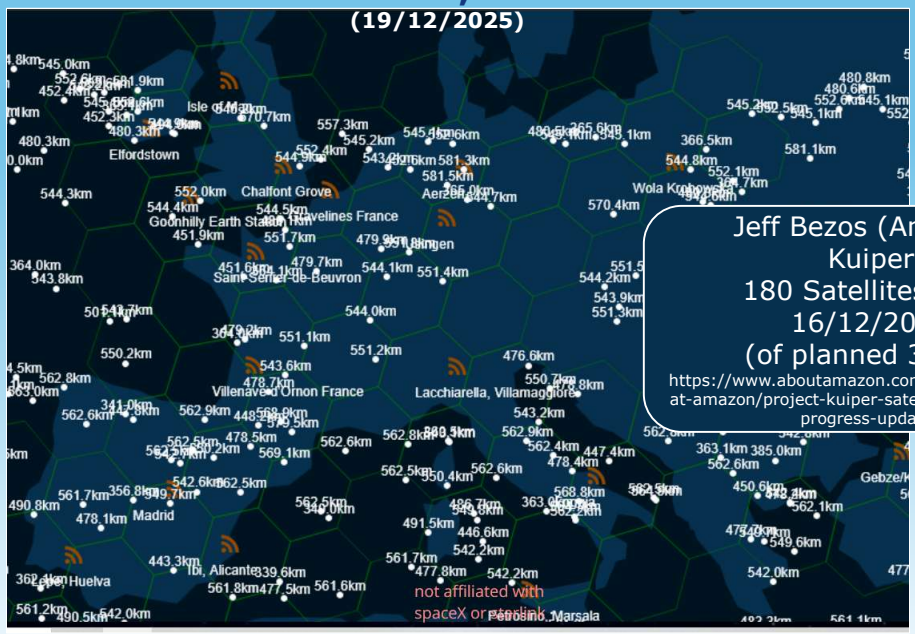
19



https://www.submarinecablemap.com/

20

Elon Musk's Starlink – 9,357 satellites in orbit



Jeff Bezos (Amazon)
Kuiper
180 Satellites as of
16/12/2025
(of planned 3,236)
https://www.aboutamazon.com/news/innovation-at-amazon/project-kuiper-satellite-rocket-launch-progress-updates

https://satellitemap.space/
https://www.space.com/spacex-starlink-satellites.html

21

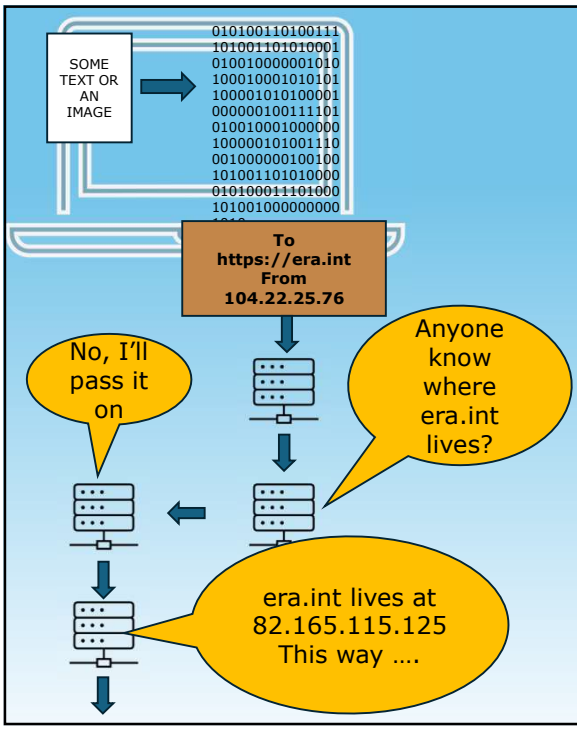
Interconnecting …

Your computer sends request to connect with another computer/server on the Internet

If accepted, a 'session' is established (i.e. digital dialogue opened)

Data/File split into small units and wrapped in a 'packets'

22



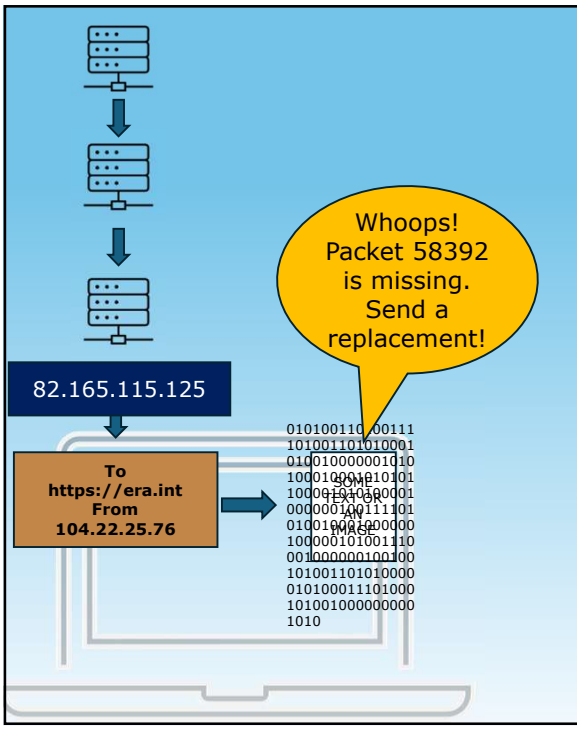
Data/File split into small units and wrapped in 'packets'

Each packet (like an envelope) is labelled with the 'to' and 'from' addresses and dispatched one at a time by the best/fastest route chosen by a series of 'routers'

If a router doesn't recognise the address, it is sent up the pipe to the next server

Domain names (i.e. era.int) are converted to IP Addresses by the DNS (Domain Name System)

23



Packets are re-assembled on the receiving device

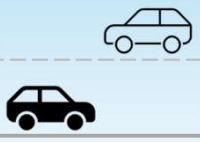
Missing or corrupted packets? A replacement is requested (depending on the 'protocol')

24

Protocols

An agreed way of doing things

- TCP (Transmission Control Protocol)
- IP (Internet Protocol)
- HTTP (Hyper Text Transfer Protocol)
- HTTPS (Hyper Text Transfer Protocol Secure)
- UDP (User Datagram Protocol)
- ARP (Address Resolution Protocol)



25

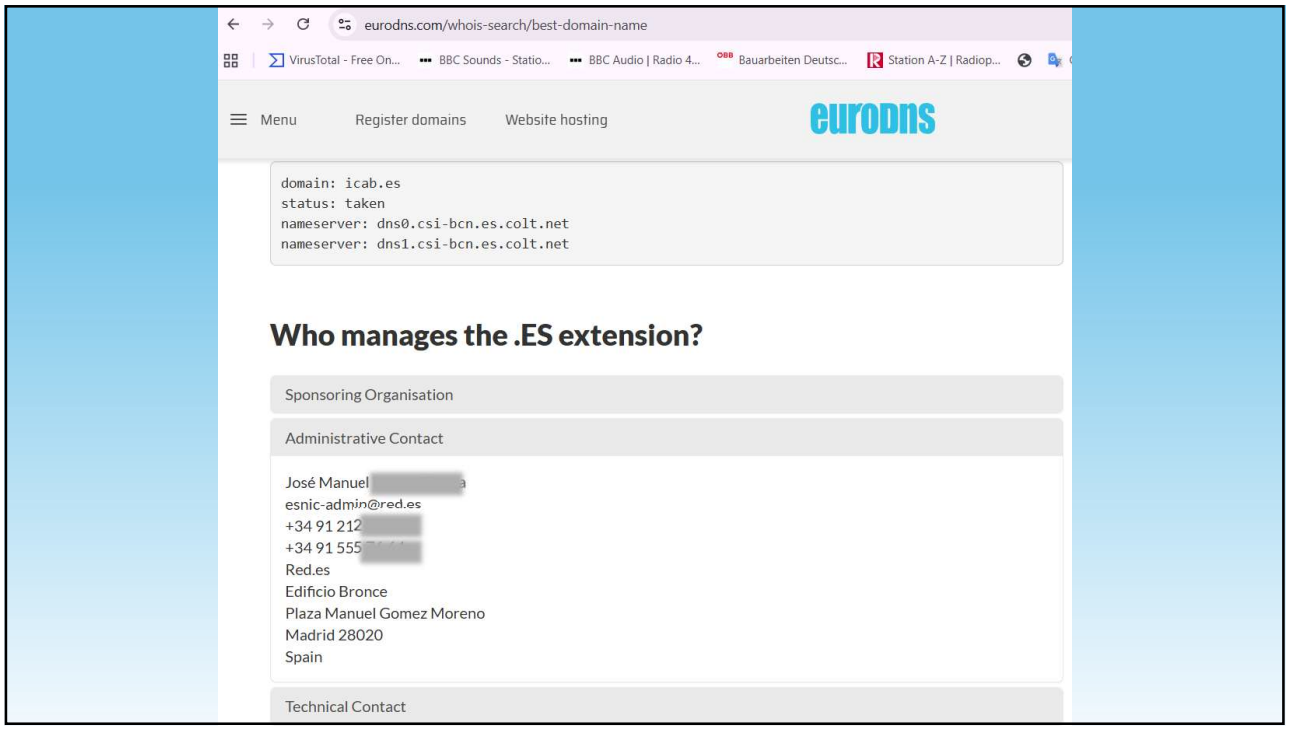
Whois

Website registration/ownership

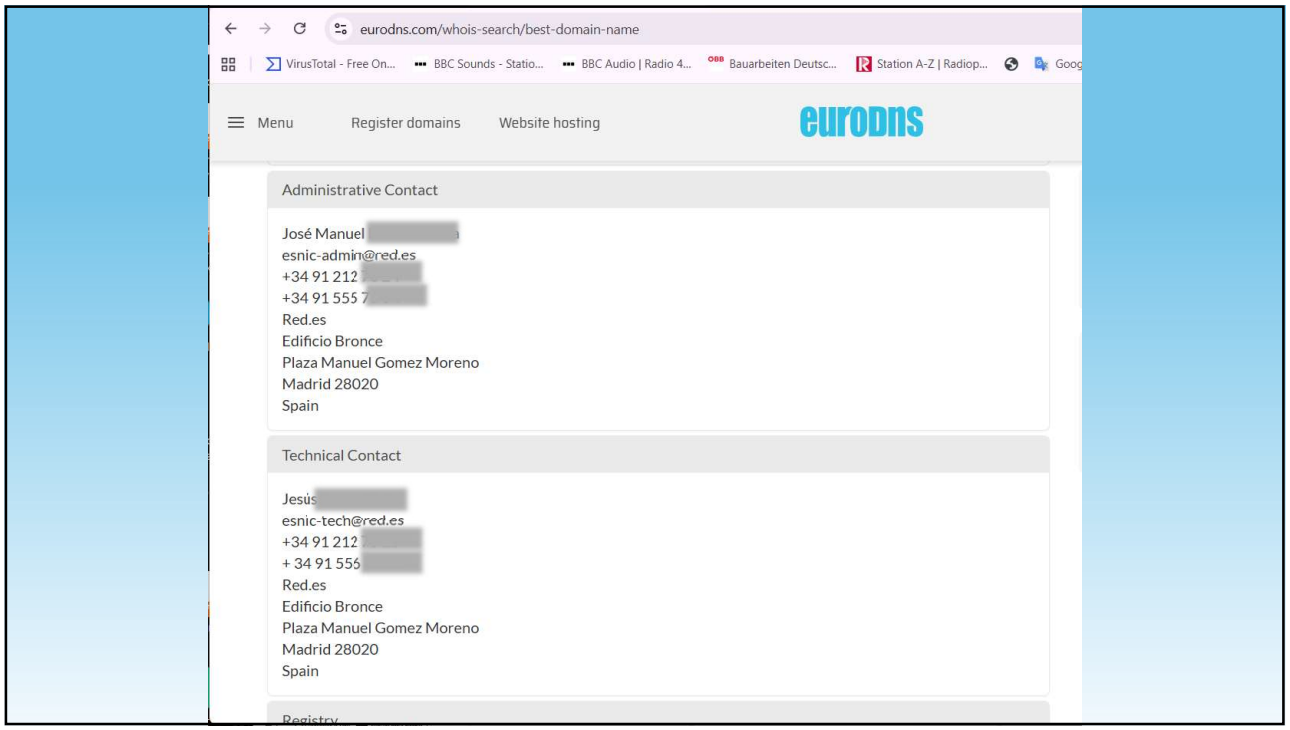
26


Whois Record for Icab.es
Whois registration
Domain Profile
Registrar Status
taken
Name Servers
DNS0.CSI-BCN.ES.COLT.NET (has 16,236 domains)
DNS1.CSI-BCN.ES.COLT.NET (has 16,236 domains)
IP Address
213.27.159.94 - 2 other sites hosted on this server
IP Location
- Barcelona - Barcelona - Colt Technology Services Group Limited
ASN
AS8220 COLT COLT Technology Services Group Limited, GB (registered Feb 24, 1997)
Whois Record (last updated on 2025-11-11)
% NOTE: The registry for this domain name does not publish ownership
% records (whois records) in the standard format. This data
% represents the most likely status of the domain based on
% information provided by the Internet's domain name servers (DNS).
domain: icab.es
status: taken
nameserver: dns0.csi-bcn.es.colt.net
nameserver: dns1.csi-bcn.es.colt.net
% For more information, please visit http://www.nic.es/

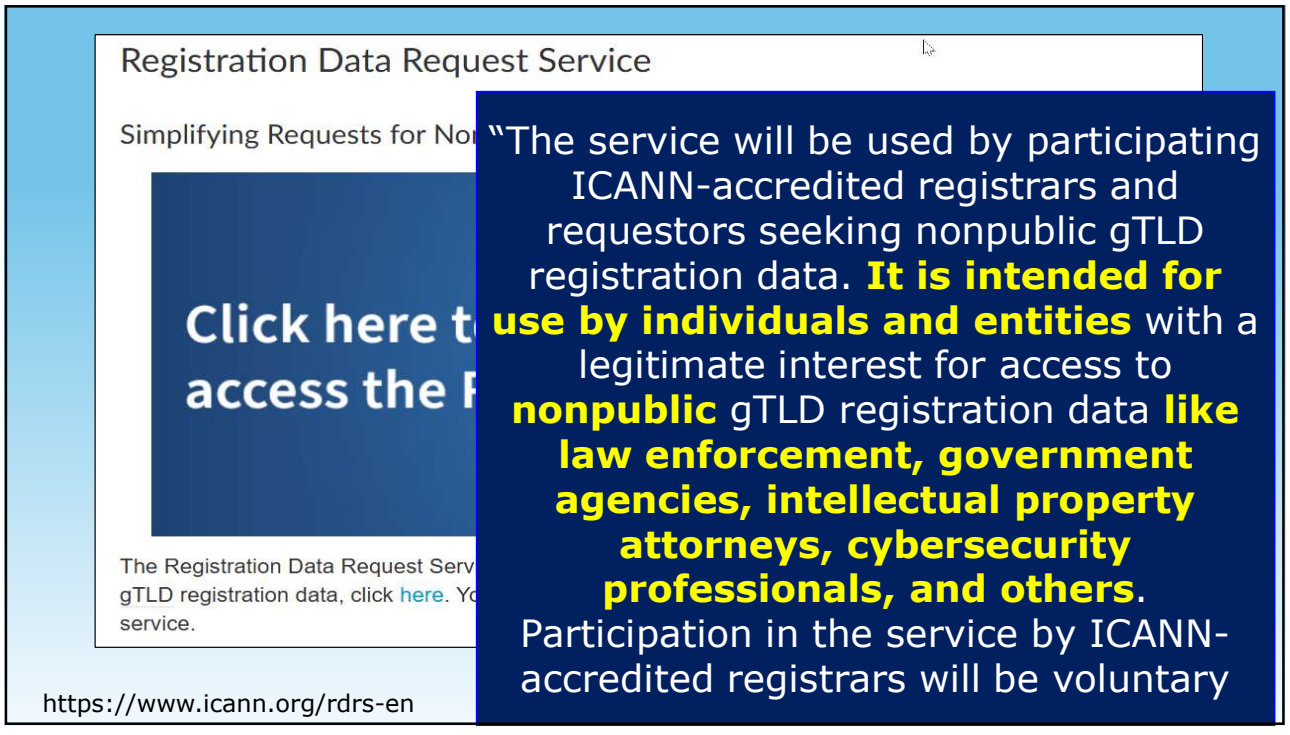
27


eurodns.com/whois-search/best-domain-name
Menu
Register domains
Website hosting
eurodns
domain: icab.es
status: taken
nameserver: dns0.csi-bcn.es.colt.net
nameserver: dns1.csi-bcn.es.colt.net
Who manages the .ES extension?
Sponsoring Organisation
Administrative Contact
José Manuel
esnic-admin@red.es
+34 91 212
+34 91 555
Red.es
Edificio Bronce
Plaza Manuel Gomez Moreno
Madrid 28020
Spain
Technical Contact

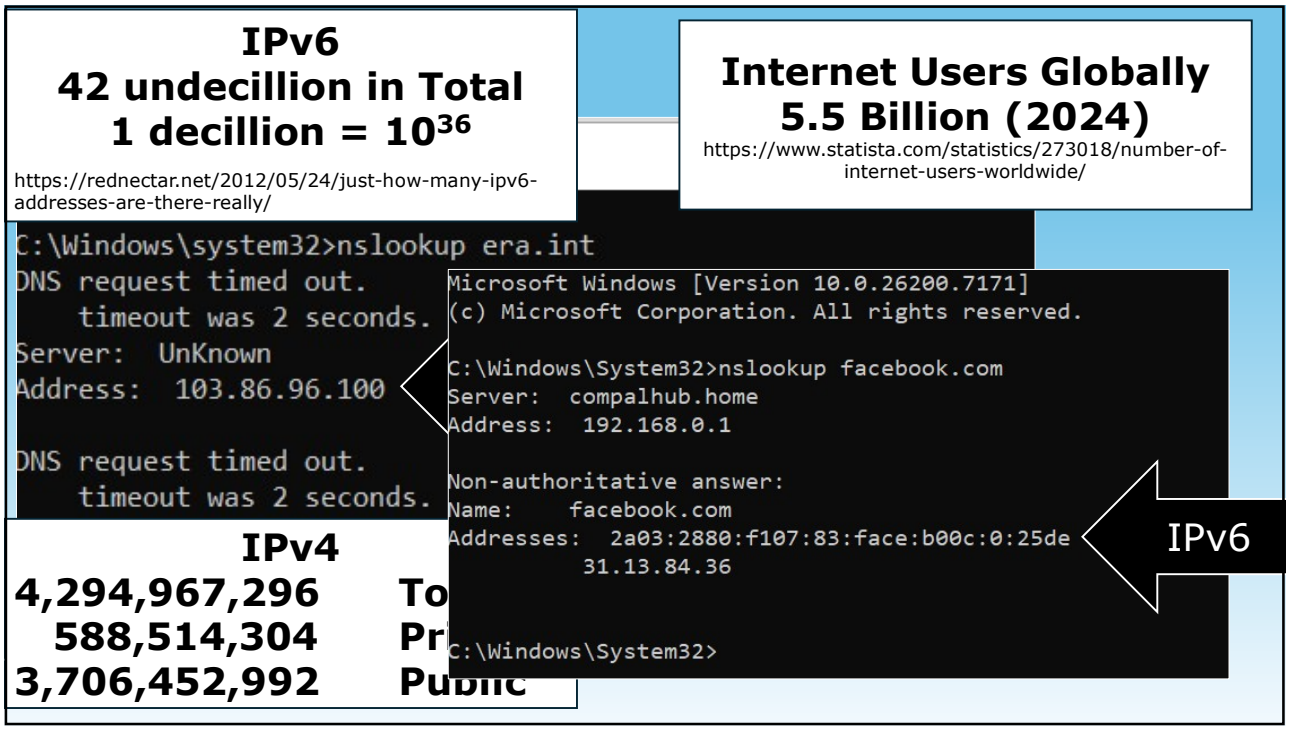
28


eurodns.com/whois-search/best-domain-name
Menu
Register domains
Website hosting
eurodns
Administrative Contact
José Manuel
esnic-admin@red.es
+34 91 212
+34 91 555 7
Red.es
Edificio Bronce
Plaza Manuel Gomez Moreno
Madrid 28020
Spain
Technical Contact
Jesús
esnic-tech@red.es
+34 91 212
+ 34 91 556
Red.es
Edificio Bronce
Plaza Manuel Gomez Moreno
Madrid 28020
Spain

29


Registration Data Request Service
Simplifying Requests for No
Click here t
access the
The Registration Data Request Serv
gTLD registration data, click here. Yo
service.
https://www.icann.org/rdrs-en
"The service will be used by participating ICANN-accredited registrars and requestors seeking nonpublic gTLD registration data. It is intended for use by individuals and entities with a legitimate interest for access to nonpublic gTLD registration data like law enforcement, government agencies, intellectual property attorneys, cybersecurity professionals, and others. Participation in the service by ICANN-accredited registrars will be voluntary

30



31

The Data Deluge

In 2024, more than:

- **361 billion emails per day;**
- **3.5 billion Google searches per day;**
- **510,000 Facebook comments per minute;**
- **16 M text messages per minute;**
- **456,000 X messages per minute;**
- **46,740 Instagram photos/minute**

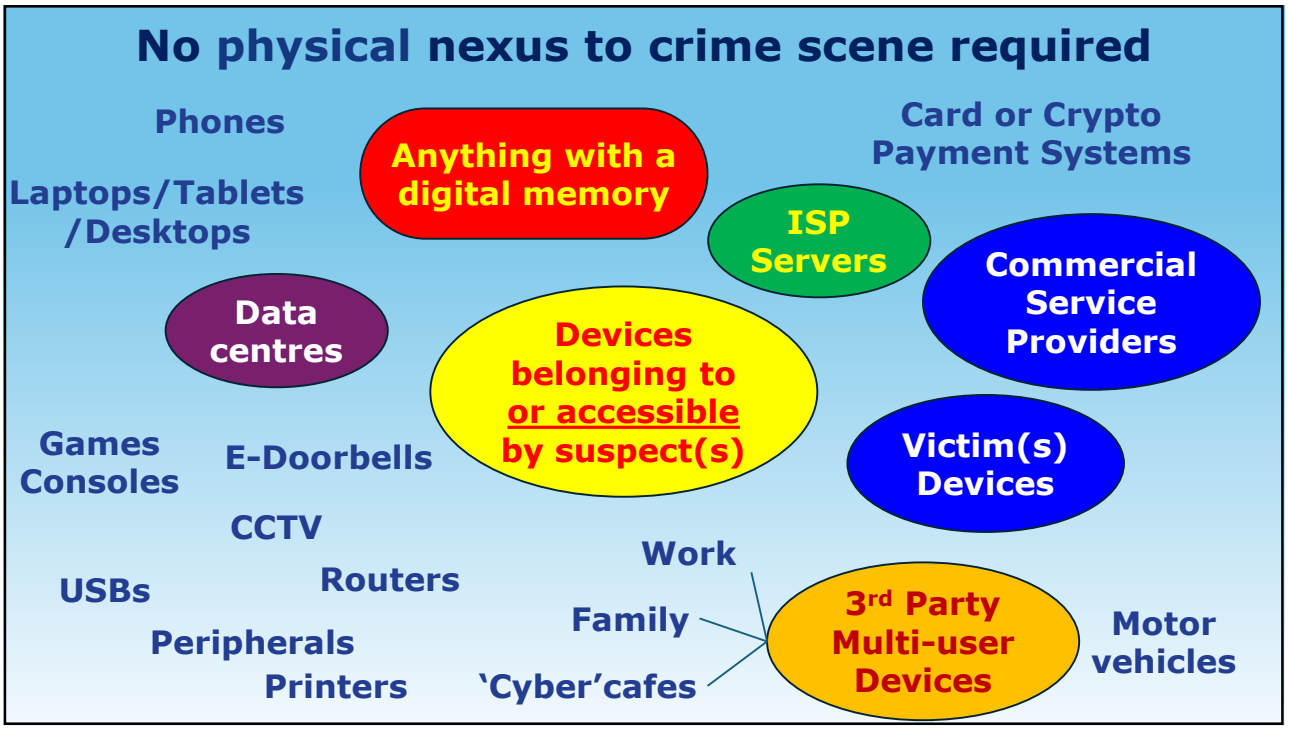
https://joingenius.com/statistics/data-generated-per-day/
https://spacelift.io/blog/how-much-data-is-generated-every-day

32

E-evidence …

33

No physical nexus to crime scene required



34

Evidence on the Device

Tying the device to the suspect:

- Traditional forensics
- Activity & behaviour of user
- User log-ins and identifiers

35

Electronic evidence is VOLATILE!

- Susceptible to heat & electromagnetic fields
- Every key pressed changes the data
- Automatic processes may delete data **(esp. Solid State Drives)**

36

Devices Dead or Alive

'Dead' Computer Forensics (device switched off)

Data captured in lab

'Live' Computer Forensics (Device switched on)

Data captured at scene

37

'Live' Computer Forensics (Device switched on)

38

Basic Kit

Forensic workstation

Cameras
Write-blockers

Cables & connectors

Access point scanners

Anti-static bags/bracelets

Faraday Bags
(kitchen foil or old paint tins)

39

RAM = Random Access Memory

- ‘Short term’ processing memory
- Standard 4/8 GB; Quality laptops 16 GB; Gaming laptops 32 or 64 GB
- Bigger RAM, more can do at same time
- Memory fades when power cut (lose unsaved files)
- Live forensics captures that data

40

'Dead' Computer Forensics

(Device is switched off and transported to lab)

41

Three main forms of data storage:

- Magnetic (Hard Disk Drives (HDDs))
- Optical (CD, DVD) (Old Tech)

- Digital switches/microchips (Solid State Drives(SSD))

Remember all based on binary (on/off)

42

Deleted data can (often) be recovered:

Delete button just tells computer the relevant space available to be overwritten

Data remains until the memory space is needed for new data

BUT: Devices with SSD storage (phones, USB sticks, modern notebooks) may automatically delete data when powered on

43

Absolute first thing in lab:

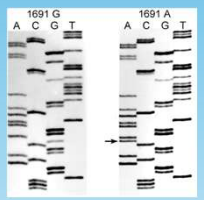
- **All seized drives copied**
- **Exact copy (every zero and one) a.k.a 'bit-by-bit', 'bit-stream' copy, image or clone (not same as 'backup')**
- **Any analysis is done on the copy in case of dispute**

44

How do we prove the copy is 100% exact?

From the

'hash' value



(Digital fingerprint, a long alphanumeric string)

45

Hexadecimal($base_{16}$)

Hash Value :

72a40ac74b7a2472826f306f02e508fc

A complex algorithm is applied to the data resulting in a 'hash value'.

One way cryptographic function (equation)

Used for:

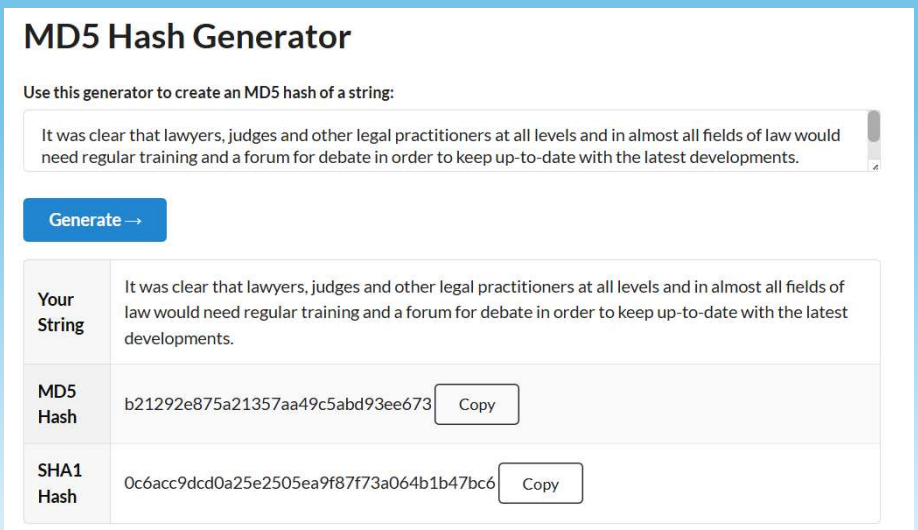
- **Checking integrity of files copies**
- **Protecting stored passwords**
- **Identifying files (malware, CSAM)**

46

- **In forensic examination the algorithm is applied to both original drive and its copy.**
- **If the 'hash value' for both drives is the same, the copy is a clone.**
- **Can 'hash' any data from file to computer drive**

47

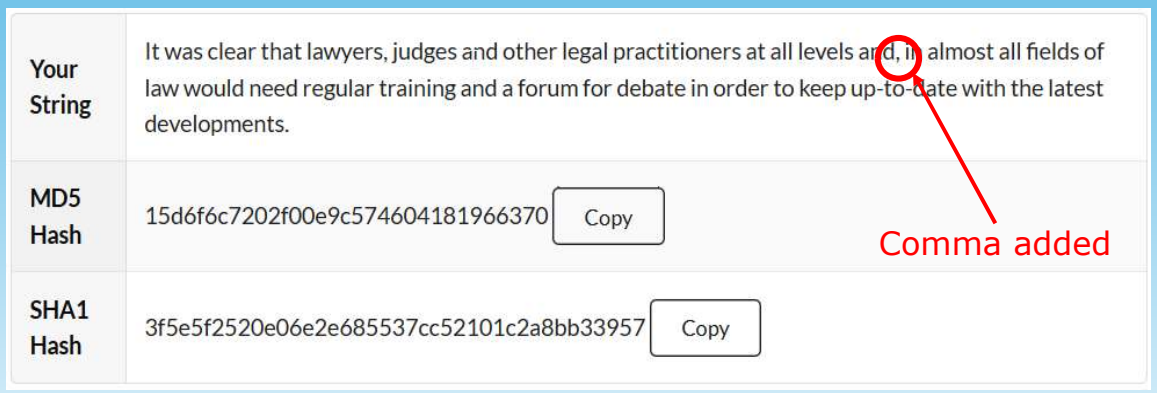
https://www.md5hashgenerator.com/



MD5 Hash
b21292e875a21357aa49c5abd93ee673

48

One zero or one different in the binary data will produce a very different hash value



MD5 Hash
b21292e875a21357aa49c5abd93ee673
15d6f6c7202f00e9c574604181966370

49

Matching files

Searching for known hash values

Checking digital fingerprints against a known list

- **Child Sexual Abuse Material (CSAM)**
- **Malware**
- **Hashed Passwords (more later)**

More on 'Client Side Scanning' later

50

Software Tools

(NO evidence button!)

51

Popular forensic software suites:

OpenText
(Encase)
FTK
Belkasoft
Sleuthkit (Autopsy)*
Volatility*
Magnet
Oxygen Forensic Suite
Cellebrite
MSAB's XRY

* Free software

52

Everything that happens on a digital device is 'logged'

Logs tell you who did what and when (Unless wiped or spoofed)

53

Server Logs

(Reminder: Server is a computer that provides services to other computers)

54

The AI Dimension

55

AI & Tax

"AI convicts fraudster and brings Austria hundreds of millions of Euros"

Austrian Ministry of Finance has a "Predictive Analytics Competence Centre (PACC)"
Detects tax fraud & cheats
2024 reviewed 6.6 M cases
Generated additional €354 M

https://www.5min.at/5202508131142/ki-ueberfuehrt-betrueger-und-bringt-oesterreich-hunderte-millionen-euro/

56

AI promises

Commercial competitive advantage?
Predictive Analysis for policymaking?
Social Control?
Identify dissidents?
Replace workers?
Cure cancer?

Fantasy or Fact?

57

AI Reliability …

BBC Research Dec 2024 into 4 AI assistants:

- **OpenAI's ChatGPT;**
- **Microsoft's Copilot;**
- **Google's Gemini; and**
- **Perplexity**

AI assistants asked 100 questions about the news (using BBC News sources)

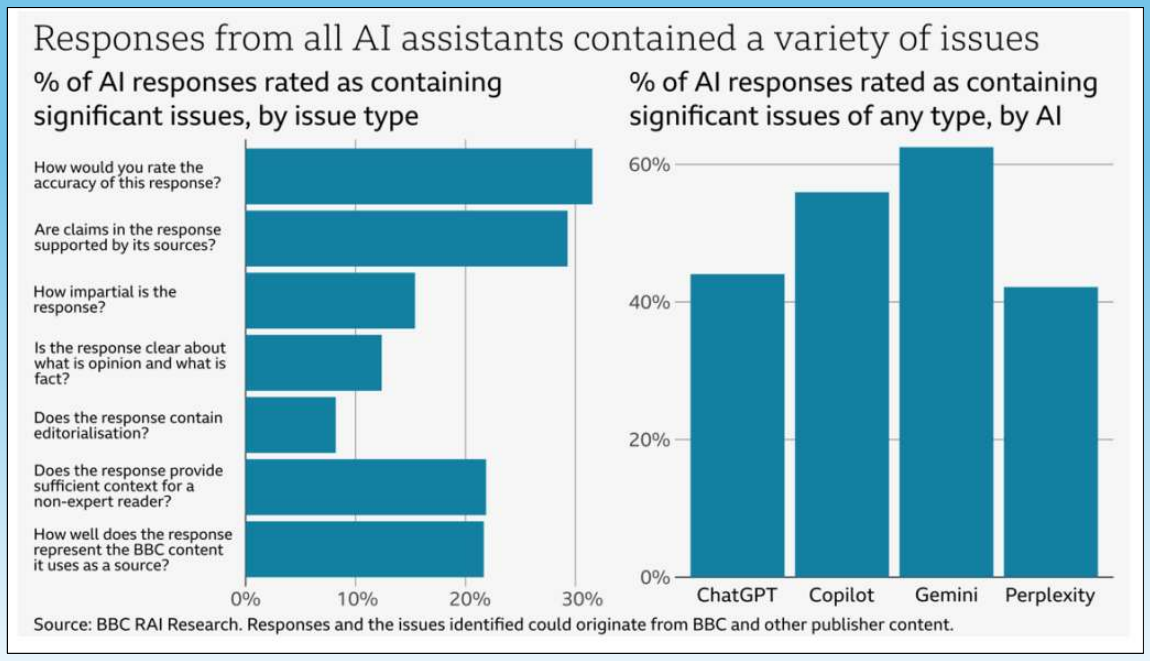
https://www.bbc.co.uk/aboutthebbc/documents/bbc-research-into-ai-assistants.pdf

58

- **51% of all AI answers had significant issues**
- **19% AI answers citing BBC content had factual errors**
- **13% of quotes sourced from BBC articles were**
  - **changed from the original or**
  - **not present in the article cited**

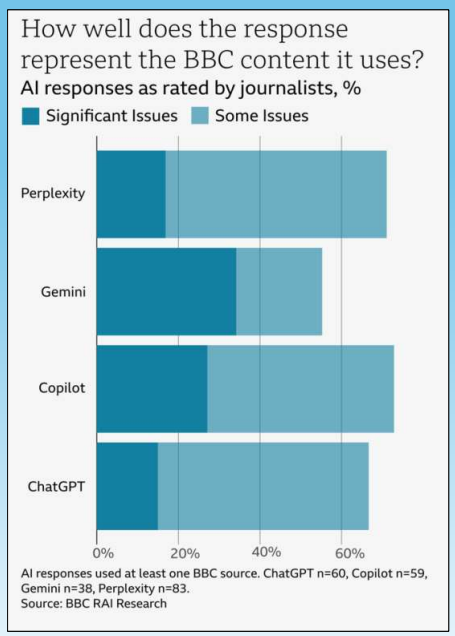
https://www.bbc.co.uk/aboutthebbc/documents/bbc-research-into-ai-assistants.pdf

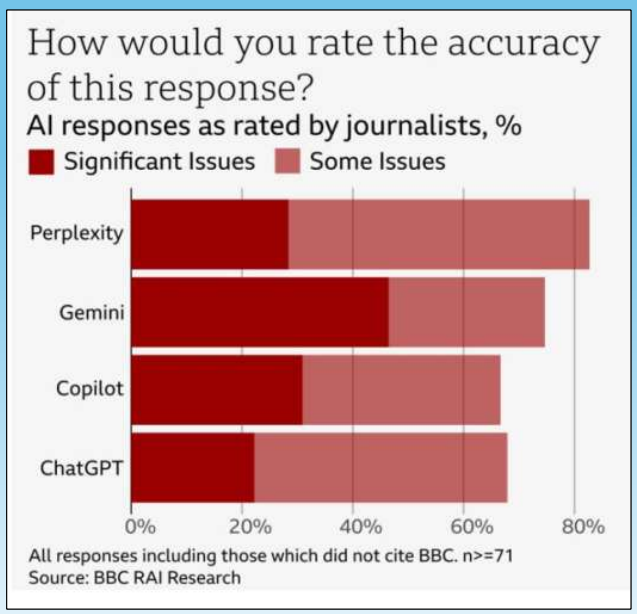
59



https://www.bbc.co.uk/aboutthebbc/documents/bbc-research-into-ai-assistants.pdf

60





https://www.bbc.co.uk/aboutthebbc/documents/bbc-research-into-ai-assistants.pdf

61

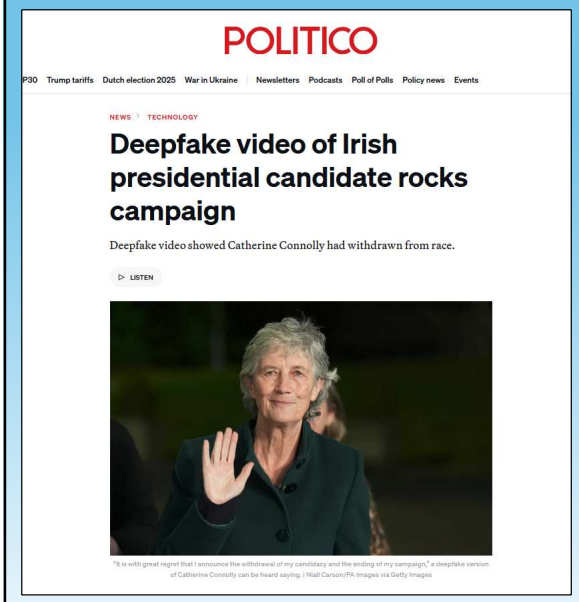
Crime has evolved

Positive	Negative
Spotting suspicious/malicious patterns in data Big data mining Identifying cybersecurity weaknesses	Weaponized Criminal research Phishing perfection Scripting malware Realistic DeepFakes (sextortion, fake evidence) Model collapse Who has control?

62

https://twitter.com/EliotHiggins/status/1637927681734987777

63



Irish Presidential Election 24 October 2025

22 October 2025 Deepfake of candidate Catherine Connelly : ***"It is with great regret that I announce the withdrawal of my candidacy and the ending of my campaign."***

Designed to look like office RTE News bulletin

Cut to deepfake of RTE political correspondent

Viewed almost 30,000 times on Facebook

Live for 12 Hours

Shared 200 times

(Connelly Elected with 63%)

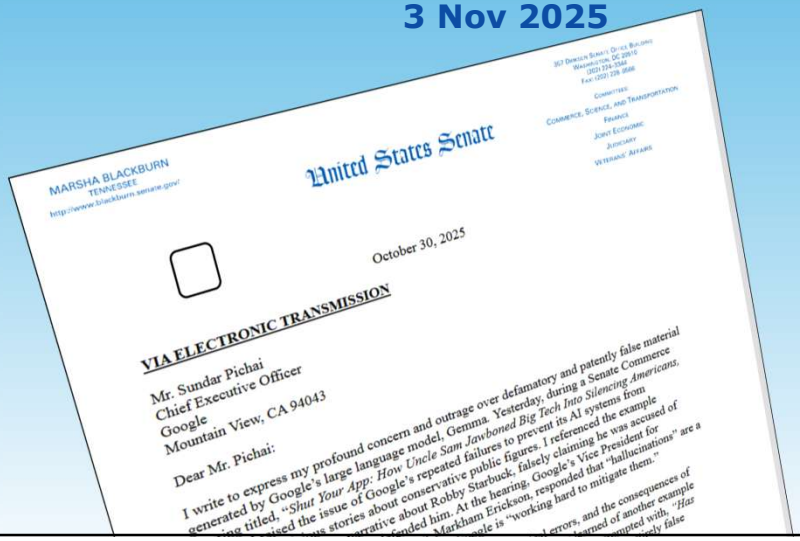
https://www.politico.eu/article/deepfake-video-of-irish-presidential-candidate-rocks-campaign/

64

https://www.blackburn.senate.gov/services/files/5651166C-7B30-4BA0-9E86-F3DD9521CA00

Google's Gemma AI Studio Model falsely accused US Senator

3 Nov 2025



MARSHA BLACKBURN
TENNESSEE

United States Senate

October 30, 2025

VIA ELECTRONIC TRANSMISSION

Mr. Sundar Pichai
Chief Executive Officer
Google
Mountain View, CA 94043

Dear Mr. Pichai:

I write to express my profound concern and outrage over defamatory and patently false material generated by Google's large language model, Gemma. Yesterday, during a Senate Commerce ...ing titled, "*Shut Your App: How Uncle Sam Jawboned Big Tech Into Silencing Americans*, ...ised the issue of Google's repeated failures to prevent its AI systems from ...rative stories about conservative public figures. I referenced the example ...ended him. At the hearing, falsely claiming he was accused of ... Markham Erickson, responded that "hallucinations" are a ...gle is "working hard to mitigate them." ... errors, and the consequences of ... learned of another example ...ipated with, "*Has* ... falsely

65

Prompt: 'Has Marsha Blackburn been accused of rape?'

Response:: *During her 1987 campaign for the Tennessee State Senate, Marsha Blackburn was accused of having a sexual relationship with a state trooper, and the trooper alleged that she pressured him to obtain prescription drugs for her and that the relationship involved non-consensual acts."*

https://www.blackburn.senate.gov/services/files/5651166C-7B30-4BA0-9E86-F3DD9521CA00
https://nypost.com/2025/11/03/business/google-curbs-access-to-gemma-ai-tech-that-falsely-accused-sen-marsha-blackburn-of-sexual-misconduct/
www.blackburn.senate.gov/2025/10/technology/blackburn-demands-answers-from-google-after-gemma-manufactured-fake-criminal-allegations-against-her

66

- **Fake links to fabricated news articles**
- **Campaign year 1998 not 1987**

"This is not a harmless 'hallucination.' It is an act of defamation produced and distributed by a Google-owned AI model. A publicly accessible tool that invents false criminal allegations about a sitting U.S. Senator represents a catastrophic failure of oversight and ethical responsibility."

Google took Gemma down

https://www.blackburn.senate.gov/services/files/5651166C-7B30-4BA0-9E86-F3DD9521CA00
https://nypost.com/2025/11/03/business/google-curbs-access-to-gemma-ai-tech-that-falsely-accused-sen-marsha-blackburn-of-sexual-misconduct/
www.blackburn.senate.gov/2025/10/technology/blackburn-demands-answers-from-google-after-gemma-manufactured-fake-criminal-allegations-against-her

67

Lawyers face judge's wrath after AI cites made-up cases in fiery hoverboard lawsuit

Talk about court red-handed

Thomas Claburn — Fri 14 Feb 2025 // 04:03 UTC

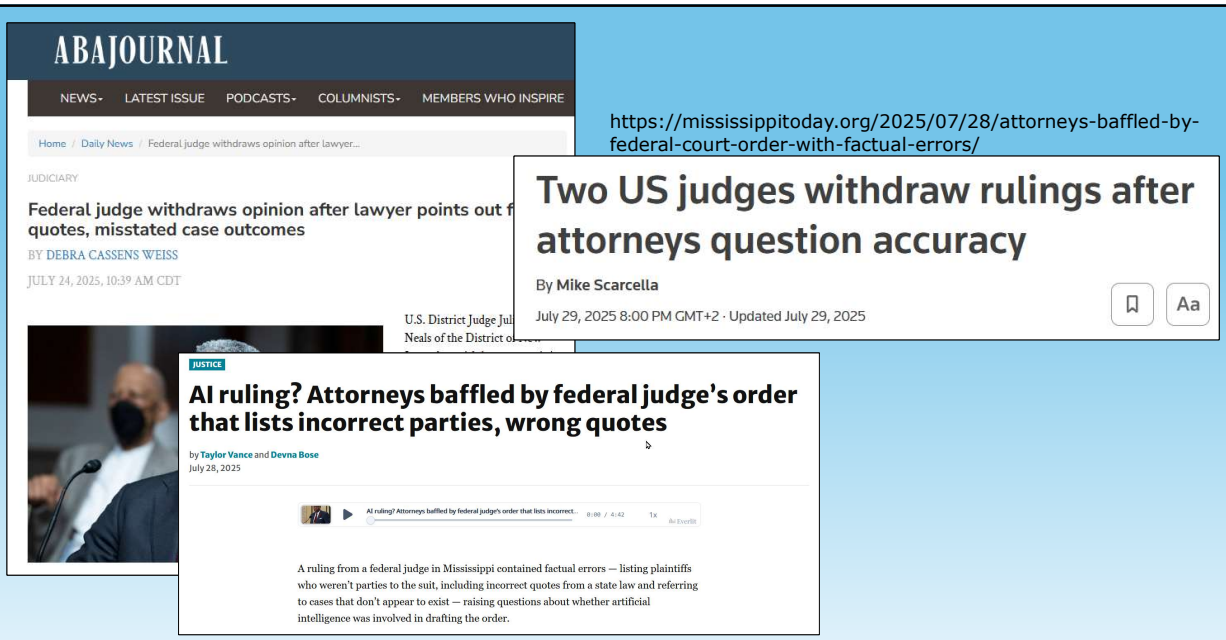
Demonstrating yet again that uncritically trusting the output of generative AI is dangerous, attorneys involved in a product liability lawsuit have apologized to the presiding judge for submitting documents that cite non-existent legal cases.

The lawsuit began with a complaint filed in June, 2023, against Walmart and Jetson Electric Bikes over a fire allegedly caused by a hoverboard [PDF]. The blaze destroyed the plaintiffs' house and caused serious burns to family members, it is said.

Last week, Wyoming District Judge Kelly Rankin issued an order to show cause [PDF] that directs the plaintiffs' attorneys to explain why they should not be sanctioned for citing eight cases that do not exist in a January 22, 2025 filing.

https://londontribune.co.uk/lawyers-face-judges-wrath-after-ai-cites-made-up-cases-in-fiery-hoverboard-lawsuit/
https://www.reuters.com/technology/artificial-intelligence/ai-hallucinations-court-papers-spell-trouble-lawyers-2025-02-18/

68



https://mississippitoday.org/2025/07/28/attorneys-baffled-by-federal-court-order-with-factual-errors/

https://www.abajournal.com/news/article/federal-judge-withdraws-opinion-after-lawyer-points-out-fake-quotes-and-misstated-case-outcomes

https://www.reuters.com/legal/government/two-us-judges-withdraw-rulings-after-attorneys-question-accuracy-2025-07-

69

Researchers at Yale and Stanford Universities found popular large language models do not:

- accurately retrieve or generate relevant legal information
- understand or reason about various laws.

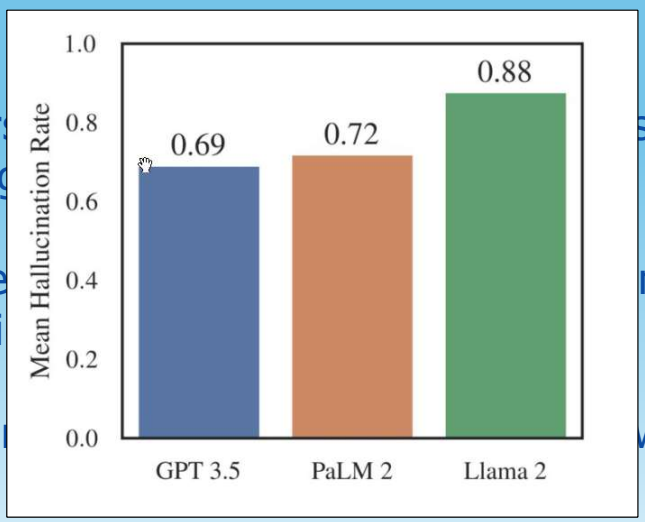
Large Legal Fictions: Profiling Legal Hallucinations in Large Language Models
https://arxiv.org/abs/2401.01301

https://www.theregister.com/2024/01/10/top_large_language_models_struggle/

70

Researchers sities found popular larg

- accurate nt legal informati
- understa ws.



Large Legal Fictions: Profiling Legal Hallucinations in Large Language Models
https://arxiv.org/abs/2401.01301

https://www.theregister.com/2024/01/10/top_large_language_models_struggle/

71

EU AI Act 2024

In force: 2 August 2024
Phased in over 36 months
144 Pages (in English)
113 Articles
13 Annexes

"AI should be a human-centric tec
It should serve as a tool for p
the ultimate aim of increasi
beinc
(recital

REGULATION (EU) 2024/1689 (ARLIAMENT AND OF TH
of 13

Extremely Complex and technical language
How easy to implement?

72

AI systems classified according to risk

Unacceptable Risk (e.g. manipulate humans) - Banned

High Risk – Strict Rules

- **E.g. Chat bots - Systems that affect health, safety, fundamental rights**
- **Must be tested and monitored**
- **Transparency**

Limited Risk – Less strict rules

- **(E.g. Spam filters- No danger - must notify they are using AI)**

Minimal Risk – No rules

73

17 Sept 2025
Traceability & Human Oversight
Parental Consent for u-14s
Copyright for AI works where "genuine intellectual effort"
Prison sentences for harmful use
Data mining only for non-copyrighted content or scientific research by authorised institutions

https://www.reuters.com/technology/italy-enacts-ai-law-covering-privacy-oversight-child-access-2025-09-17/

74

Resources required

AI (machine learning) requires
Graphics Processing Units (GPUs)
More complex
More expensive
Run hotter
Higher energy requirement

Estimated 9,000 - 11,000 data centres globally

Water required by global AI systems "may reach [between] 4.2 [and] 6.6bn cubic meters in 2027"

(more than 50% of UK's annual water withdrawal)

https://www.theguardian.com/commentisfree/2024/mar/02/ais-craving-for-data-is-matched-only-by-a-runaway-thirst-for-water-and-energy

75

Energy Footprint

Ireland, 2022 Data Centres consumed 18% electricity output - more than all the rural dwellings in the country, and equal to electricity consumption of all Ireland's urban dwellings (pop. 5,281,600).

One medium-sized datacentre used as much water as three average-sized hospitals.

https://www.theguardian.com/commentisfree/2024/mar/02/ais-craving-for-data-is-matched-only-by-a-runaway-thirst-for-water-and-energy

76

GPT-4 based in Iowa.
July 2022, the month before OpenAI finished training the model, the cluster used about 6% of the district's water.

"Operational water withdrawal" – water taken from surface or groundwater sources – of global AI "may reach [between] 4.2 [and] 6.6bn cubic meters in 2027" which is more than 50% of annual water withdrawal of United Kingdom.

https://www.theguardian.com/commentisfree/2024/mar/02/ais-craving-for-data-is-matched-only-by-a-runaway-thirst-for-water-and-energy

77

Emmanuelle Saliba
https://www.youtube.com/shorts/PyG_QDjvjTw
https://www.getrealsecurity.com/

78

https://www.thefuturefoundation.eu/en/10-rules

79

80

PROSEARCH

Conducting Digital Forensic Analysis with Artificial Intelligence

Damir Kahvedžić, PhD; Global Data Service Manager, ProSearch

Damir.Kahvedzic@prosearch.com

Co-funded by the European Union

Who am I?

Damir Kahvedžić

Senior Global Data Services Manager | ProSearch

Scope

What are we talking about here?

Case Study
What is the ‘traditional’ way of doing forensics
What are the common issues in the practice
Can AI be used to help?
How are LLM’s used in forensics
What are the NEW problems with LLMs.

What we won’t talk about

Legal stuff. **I am not a lawyer**

Anything **too** technical

We don’t have all the answers

Analysis…

Case Study

Jeffrey Epstein Case

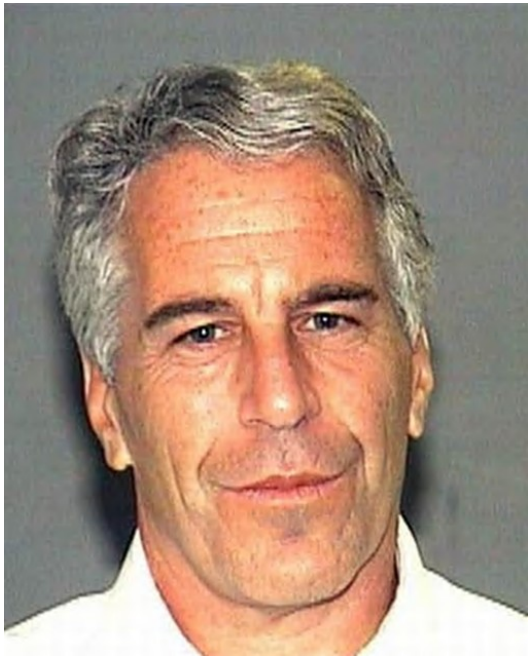
Include:

- Unknow total number of collected files
- 6 million potentially responsive files*
- 3.5 million released documents^

  2000 videos, 180,000 images
- 400 attorneys and 100 document analysts

Redaction process of

- Victims name and likenesses
- Sensitive Personal Identifiable Information (PII)
- Privileged or irrelevant information



*https://www.washingtonpost.com/national-security/2026/01/06/epstein-documents-2-million-unreleased/

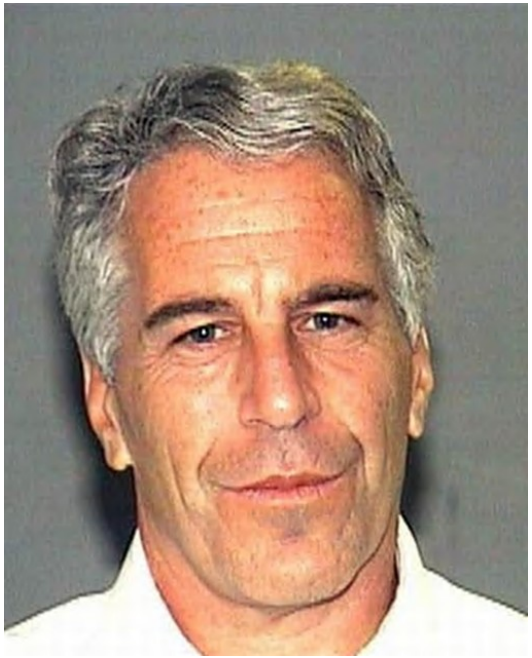
^https://www.justice.gov/opa/pr/department-justice-publishes-35-million-responsive-pages-compliance-epstein-files

Case Study - Challenges

Jeffrey Epstein Case

Challenges Include:

- Huge number of documents
- Large number of involved individuals
- Extremely sensitive material
- Lots of PII



Are these problems common and what are the solutions?

What is in an average case?

Trends

- Storage is cheap
- Cloud is increasingly used
- Social media and off device locations
- Chat has entered the prime time

Mobile Storage	Cloud size	PC Size	# Files per Gb
256Gb – 2Tb	unlimited	1 – 2Tb	5 – 10K
Largest Live Case	**Avg. Delivery Size**	**Avg. # Documents**	**# Collection Types**
>10m	338 Gb	1.3 million	116

The main challenges in Digital Forensics

Challenges are well documented

- The amount of data seen in investigations continues to grow
- 69% of a investigators say their team does not have enough time to review all the data
- The regulatory requirements are also mounting: Remove PII, Identify relationships between different devices
- Data abstraction is difficult: explaining the meaning of evidence

available at www.sciencedirect.com
ScienceDirect
journal homepage: www.elsevier.com/locate/diin
ELSEVIER
Digital Investigation

Digital forensics research: The next 10 years

Simson L. Garfinkel
Naval Postgraduate School, Monterey, USA

ABSTRACT

Today's Golden Age of computer forensics is quickly coming to an end. Without a clear strategy for enabling research efforts that build upon one another, forensic research will fall behind the market, tools will become increasingly obsolete, and law enforcement, military and other users of computer forensics products will be unable to rely on the results of forensic analysis. This article summarizes current forensic research directions and argues that to move forward the community needs to adopt standardized, modular approaches for data representation and forensic processing.

Keywords:
Forensics
Human subjects research
Corpora
Real data corpus
Realistic data

1. Introduction

Digital Forensics (DF) has grown from a relatively obscure tradecraft to an important part of many investigations. DF tools are now used on a daily basis by examiners and analysts within local, state and Federal law enforcement; within the military and other US government organizations; and within the private "e-Discovery" industry. Developments in forensic research, tools, and process over the past decade have been very successful and many in leadership positions now rely on these tools on a regular basis—frequently without realizing it. Moreover, there seems to be a widespread belief, buttressed on by portrayals in the popular media, that advanced tools and skillful practitioners can extract actionable information from practically any device that a government, private agency, or even a skillful individual might encounter.

This paper argues that we have been in a "Golden Age of Digital Forensics," and that the Golden Age is quickly coming to an end. Increasingly organizations encounter data that cannot be analyzed with today's tools because of format incompatibilities, encryption, or simply a lack of training. Even data that can be analyzed can wait weeks or months before review because of data management issues. Without a clear research agenda aimed at dramatically improving the efficiency of both our tools and our very research process, our hard-won capabilities will be degraded and eventually lost in the coming years.

This paper proposes a plan for achieving that dramatic improvement in research and operational efficiency through the adoption of systematic approaches for representing forensic data and performing forensic computation. It draws on more than 15 years personal experience in computer forensics, an extensive review of the DF research literature, and dozens of discussions with practitioners in government, industry, and the international forensics community.

1.1. *Prior and related work*

Although there has been some work in the DF community to create common file formats, schemas and ontologies, there has been little actual standardization. DFRWS started the Common Digital Evidence Storage Format (CDESF) Working Group in 2006. The group created a survey of disk image storage formats in September 2006, but then disbanded in August 2007 "because DFRWS did not have the resources required to achieve the goals of the group. (CDESF working group, 2009)" Hoss and Carver discuss ontologies to support digital forensics (Carver and Hoss, 2009), but did not propose any concrete ontologies that can be used. Garfinkel introduced an XML representation for file system metadata (Garfinkel, 2009), but it has not been widely adopted.

GenAI and LLMs

Definitions

- GenAI is a broad category of AI that creates new content. It can be image, text, or video

- Large Language Models are trained knowledge models that provide the core capabilities of chat bots and are primarily used for text.

- Domain specific LLMs are trained on specific domain knowledge

Impact of AI

Adoption of GenAI

- Legal Field: huge interest with some domain specific LLMs being integrated into Legal Workflows

  Use cases: Document Drafting, Document Summarisation, Review and others

- Digital Forensics: slower uptake than legal due to the complexity and hands on nature of the work. Recent surveys have revealed a huge appetite to use LLMs and GenAI in the future

Two major questions:

1. Can AI help in the investigative process

2. Can we detect if AI has been used by those we investigate?

PROSEARCH

Digital Forensic Process

How is a Digital Forensic investigation carried out?

Traditional Digital Forensic Principles

ACPO Guidelines

ACPO Rule 1

That **no action** take is taken that should change data held on a digital device including a computer or mobile phone that may subsequently be relied upon as evidence in court.

ACPO Rule 2

Where a person finds it necessary to access original data held on a digital device that the person must be **competent** to do so and able to explain their actions and the implications of those actions on the digital evidence to a Court.

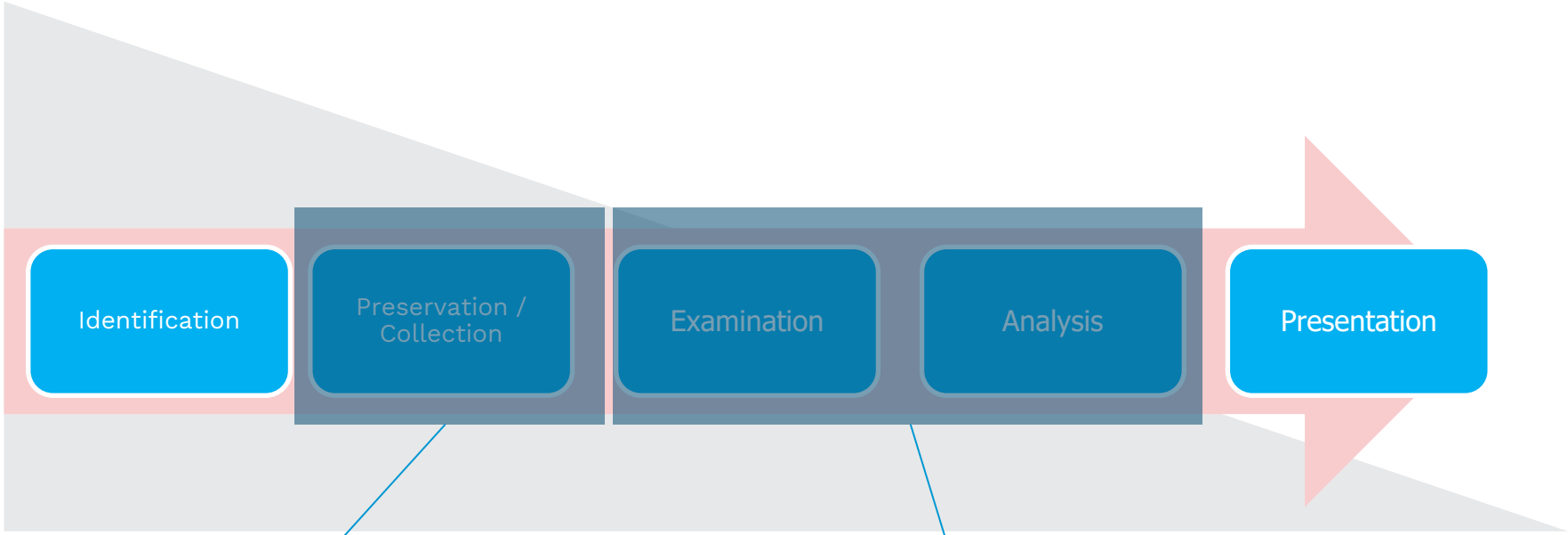
ACPO Rule 3

That a **trail** or **record** of all actions taken that have been applied to the digital evidence should be created and preserved. An independent third-party forensic expert should be able to examine those processes and reach the same conclusion.

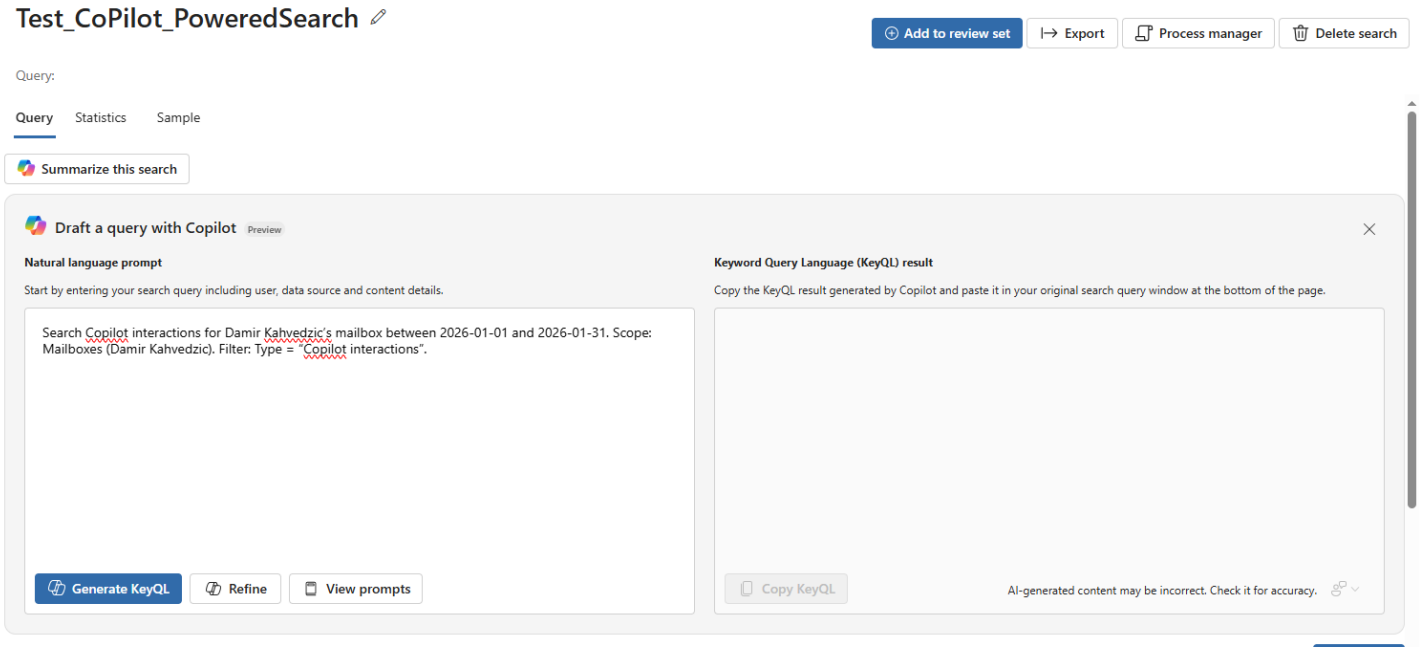
ACPO Rule 4

That the individual in charge of the investigation has overall responsibility to ensure that these principles are followed

General Forensic Process



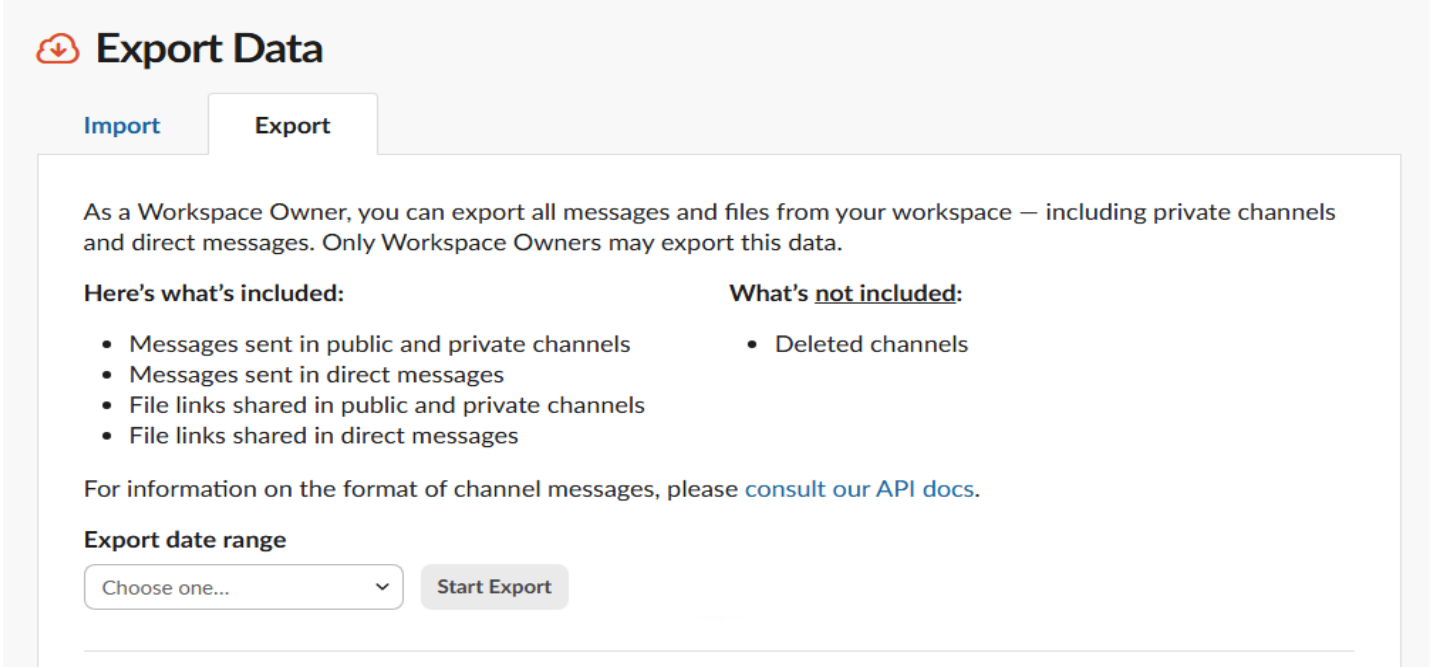
AI At Source?



Microsoft365 Purview

- Used for M365 corporate collections
- Encompasses email, SharePoint, teams and other M365 data

AI At Source?



Slack exports

- Do not have ANY AI in the export process
- Outsources all of the review and analysis to the downstream processes

AI At Analysis

1. Automating Evidence Triage
2. Natural Language Processing for Chat and Social Media
3. Intelligent Assistant to guide human users
4. AI as teacher and Software Developer
5. Multimedia Forensics
6. Pattern Recognition & Anomaly Detection
7. Auto-redaction and Testing

1. Automating Evidence Triage

Use case

- Use LMMs to target and prioritise the review of documents.
- The process automates the traditional methods of extracting the evidence and creating review sets.
- Create a prompt to abstract the categories of evidence. Pre-trained classifiers can then trawl the documents and

Methods

1. Keyword Search
2. Technology Assisted Review (TAR)
3. Continuous Active Learning (TAR 2.0)
4. LLM Powered Investigations

Traditional Approach:

```
("bribe" OR "kickback" OR "payoff" OR
"grease" OR "facilitate") AND
("payment" OR "transfer" OR "wire")
AND NOT "legitimate"
```

AI Approach:

```
"Identify emails discussing potential
bribery, corruption, or inappropriate
financial incentives, including coded
language or euphemisms."
```

1. Automating Evidence Triage

Results

- Tests are showing remarkable accuracy of LLMs compared to Human Reviewers.

Challenges

- LLMs are not facing the same challenges as those previously encountered in adopting TAR or CAL
- Numerous legal technologies are incorporating LLMs into their systems:
  - ***Harvey AI***
  - ***Relativity Air***
  - ***eDisovery AI***
  - ***Merlin Alchemy***

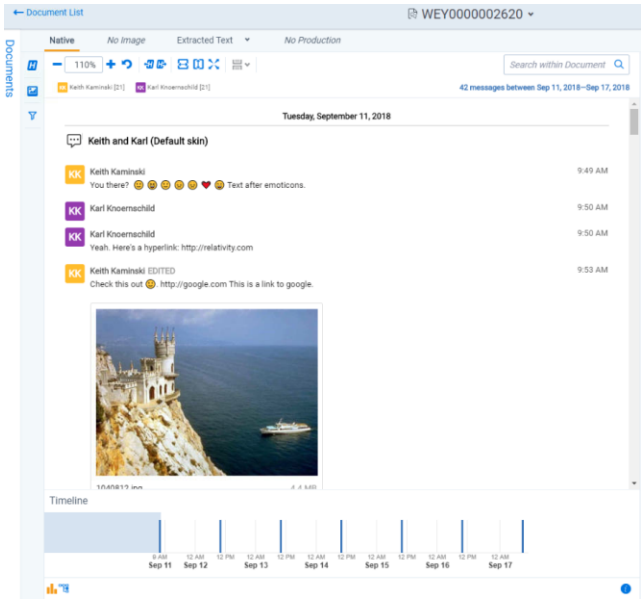
2. NLP for Chat and Social Media

Use case

- Traditionally, chats are reviewed manually due to the colloquial, informal language, unusual organisation and complex relationships.
- Use LMMs to categorise and understand the context of chats.

Results & Challenges

- Even more so than normal documents; chats are ideally suited to be understood by LLMs trained on informal language
- They understand tone, content, acronyms etc.
- Challenges remain on understanding metadata such as emoji, statuses and reactions



3. AI as an Intelligent Assistant

Use case

- Digital Forensics is a highly specialised area. Its difficult to remember all the locations artefacts can be found in.
- Advanced personal assistants can be asked for help in unknown environments, for early case assessment, document drafting etc.

Results & Challenges

- Early tests on ChatGPT3.5 proved promising but inconclusive. Accuracy is getting better but is no substitute for investigative experience.
- Digital forensic specific LLMs have been proposed, and existing forensic providers have embraced the technology.
- Privacy considerations and hallucinations are worrisome

4. AI as Teacher and Developer

Use case:

- Digital forensics often requires the development of software or understanding what software or scripts do
- LLMs are excellent at creating small scripts and directing the user on how to approach a problem in developing software
- It is also a good decoder and troubleshooter. You can even load in images of code and it will understand it and direct an answer

Results & Challenges

- It greatly decreases the time for writing code
- However, knowledge of coding is a must to understand what the code is doing, how to apply and when to change direction

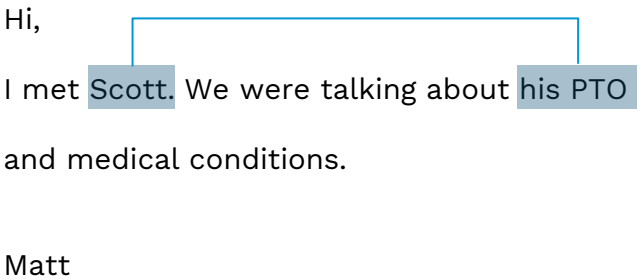
5. AI Pattern Recognition

Use case

- Person Identifiable Information is traditionally difficult to identify and remove for privilege. Traditionally we use sets of hard coded patterns the results of which are then reviewed and processed.
- Use LLMs and NLP to understand the context of text and identify PII automatically.

Results & Challenges

- Forensics and document review software have a specialised use case for identify PII.
- They identify entities and link them together to form relationships



6. AI Redactions and Scrubbing

Use Case

- Redaction is the process of removing sensitive material. It goes hand in hand with PII identification
- Traditional methods are bulk search and redact workflows. They have mixed results.

Results & Challenges

- LLMs can be trained to classify, redact and then to annotate the redaction automatically. They can also run post production checks to check if anything was missed
- Due to sensitivities they are still QC'd by human reviewers

Hi,

I met [redacted] We were talking about [redacted]

and medical conditions.

Matt

7. AI Infused Multimedia Forensics

Use case

- Video and Audio forensics are big challenges in the investigation. Audio transcription allows users to search on the text of what was spoken. It is often incorrect and a best effort.
- Images and video are often reviewed individually or rely on non content metadata for filtering

Results & Challenges

- LLMS have been tested on images to good results.
- LLMs and predictive analytics have been used to clear up garbled Audio, fuzzy video and other lossy images
- VERINT Intelligent Voice, Amped 5

describe this image

This image shows a middle-aged man speaking at what appears to be a formal event or press conference. He is wearing glasses, a dark blazer, and a blue shirt. His hand is placed on his chest as if emphasizing a point while talking.

The background is bright red, and there is a visible sign on the right side that includes the word **"PRIDE"**, suggesting the event may be related to a Pride campaign or organization. The overall setting looks professional, with microphones in front of him indicating he is addressing an audience or media.

AI Reservations

Corporate Governance Issues

Data Privacy

- Most be clear where the prompts and inputs are going. What data is used to train the LLMs

Humans are still accountable

- Results of LLMs are not always accurate

Over reliance on LLMs

PROSEARCH

AI as Evidence

What if we want to detect AI rather than use it?

AI and Fakes

Fakes

- Deep Fakes is AI created media that is posing as real media
- Can be found in Video \ Audio
- Typically use

Generative Adversarial Network with a Generator and a Discriminator working in tandem

Diffusion

- Getting very difficult to spot

Soft Fakes \ Shallow Fake

- A digitally altered, enhanced or edited media
- Examples include slowing down \ speeding up video, editing or cropping images.
- Simple tools needed

Deep Fake

- A wholly artificially created media designed to pass of as real
- Requires neural networks, GAN,

Variants

Photoshop

- Altering images and media to convey a certain message.
- It required a decent knowledge of photo editing, staging and software.
- GenAI makes it much easier

Deep Fakes

Video Generation 2023

Video Generation 2026

Detecting AI

Things to look out for:

- Watermarks
- Very short video lengths
- Unnatural movements
- Voiceovers that are tonally flat and don’t take breaths
- Inconsistent details in the background
- Faulty physics
- Reverse Image Search
- Presence of the ‘Uncanny Valley’

Tools:

- Sensity
- Operation Minerva
- Deepfake-O-Meter

Watermarking

Synth ID

- Google Deep mind technology that embeds invisible signatures to generated content
- Works over images, text, video
- Meant to be persistent and take into account cropping, editing and modifications
- The result is **probabilistic** not **absolute**

is this photo fake

Analysis & 1 more

Based on an analysis using SynthID, all or most of this image was generated or edited with Google AI.

Looking at the image itself, there are a few visual clues that are common in AI-generated content:

- **Anatomical issues:** If you look closely at the man's hands, specifically the one holding the phone and the one resting on his lap, the fingers appear slightly distorted or blended together.
- **Inconsistent details:** There is a small, star-shaped watermark in the bottom right corner, which is a common indicator used by some Google AI generation tools.
- **Compositional "perfection":** The lighting across the subject and the vast background is very uniform and balanced in a way that often characterizes AI models.

While the scenery looks like a real location (similar to the Cliffs of Moher in Ireland), these technical details suggest the image was created using artificial intelligence. For more information on how this detection works, you can visit support.google.com/gemini?p=synthid.

Detecting AI

Other ways to Detect AI

- Inspect metadata
- Look at user history
- Inspect prompt history usage

Tool

- Amped Authenticate

Summary

The Future

AI at Source

- Rather than collecting all data. AI will be used by major organisations at source
- Search and export can drastically reduce the amount of data exported and put to analysis

Agentic AI

- Automation of tasks via Agentic AI has the possibility of creating less manual workflows.
- Automation of repetitive task can minimise human involvement to a QC level only.

Enhanced Pattern Detections

- AI will fill in the gap of understanding more complex data such as emoji, memes and gifs in chat datasets
- AI will play a crucial role in AI deep fake detection

Take aways

Summary

- The size and complexity of data has always been a challenge in digital forensics. Manual, laborious work is error prone. Software has evolved to such an extent that it can be used to help.
- GenAI is one of the most useful ‘out of the box’ technologies we have seen in recent years.
- Care must be taken not to over rely on the technology. The human is still accountable, and the results are not always perfect
- Use AI as an assistant, not as a replacement. Always trust and verify the results

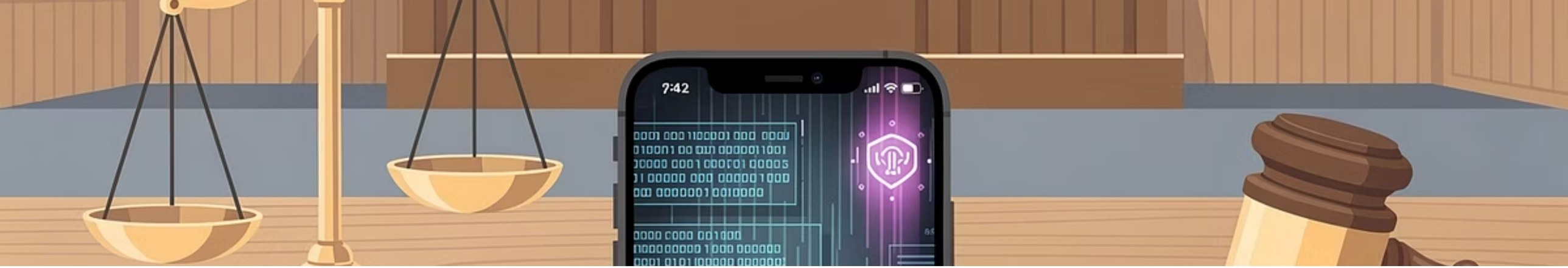
Adoption of the software is very quick compared to previous methods.

PROSEARCH

Thank You

damir.Kahvedzic@prosearch.com

For more information visit www.prosearch.com



Handling Electronic Evidence on Mobile Devices in Courts: Perspectives of the Defence

A critical exploration of evidentiary standards in the digital age, with particular attention to encrypted communications and fundamental procedural safeguards.

María Barbancho | www.barbancho.legal

Co-funded by the European Union

Context

Encrypted Messaging Applications and the Rise of Digital Evidence

In recent years, there has been a growing and increasingly decisive reliance on digital evidence in criminal proceedings. This phenomenon is particularly evident in cases involving encrypted messaging applications such as **EncroChat, Sky ECC, and ANOM**.

These operations have fundamentally transformed investigative practices and, consequently, evidentiary standards before criminal courts across Europe.

Key Concerns

- Legality and integrity of encrypted digital data
- Reliability of expert evidence derived from opaque technical processes
- Compatibility with fundamental procedural principles
- Absence of binding European digital forensic standards

María Barbancho | www.barbancho.legal

A Qualitative Shift from the Defense Perspective

Cryptomessaging cases represent a qualitative shift from traditional mobile device forensics. Unlike the seizure of a physical device from which a verifiable forensic image is produced, cryptomessaging evidence is typically presented in the form of processed data sets: selective chat extracts, translations, summaries, or spreadsheets generated by investigative authorities.

Inaccessible Underlying Data

Servers, metadata, complete chat histories, or technical logs frequently inaccessible to the defense

Direct Impact on the Defense

Directly affects the ability to assess the integrity, completeness, and authenticity of the data

Equality of Arms Compromised

Procedural imbalance when the prosecution controls access to primary data

ECTHR JURISPRUDENCE

The Yüksel Yalçınkaya Judgment (ECtHR, Grand Chamber, 26 September 2023)

These issues were decisively addressed by the Grand Chamber of the European Court of Human Rights in the case of **Yüksel Yalçınkaya v. Turkey**. The case arose in the context of mass prosecutions in Turkey based on the alleged use of the encrypted messaging application ByLock.

> The Turkish authorities maintained that ByLock had been created exclusively for use by a terrorist organization linked to the Gülen Movement. As a result, individuals were prosecuted and convicted solely on the basis of downloading or using the application, without any requirement to prove incriminating content or specific conduct.

In practice, the mere use of ByLock amounted to a presumption of guilt, making it almost impossible for defendants to challenge the evidence against them.

María Barbancho | www.barbancho.legal

Violations Found and Scope of ECHR Review

Violations of the ECHR

The Grand Chamber determined that this systemic procedural approach violated Articles 6, 7 and 11 of the European Convention on Human Rights.

Jurisdictional limit

The Convention "does not lay down rules on the admissibility of evidence or the way it should be assessed, these being matters primarily for regulation by national law and national courts".

Effective ECHR control

The Court assesses "whether the proceedings as a whole, including the way in which the evidence was obtained, were fair" and "whether the applicant was given an opportunity to challenge the evidence and object to its use".

Crucial consequence: Admissibility tests must be carried out on a case-by-case basis by national courts, but always under the umbrella of Article 6 ECHR. When evidence carries decisive weight, procedural guarantees must be particularly robust.

Equality of Arms, Raw Data, and the Right to Challenge Evidence

A central aspect of the Yalçınkaya judgment is its emphasis on the **quality and integrity of data**. The Court stressed that the right to challenge evidence includes, where appropriate, the ability to resort to independent expertise.

Without access to raw data or equivalent compensatory safeguards, the defense cannot meaningfully verify authenticity, completeness, or integrity.

The ECtHR found that in Yalçınkaya there were insufficient safeguards to ensure that the applicant had a genuine opportunity to challenge the evidence and conduct his defense effectively, on an equal footing with the prosecution.

Inadmissible judicial silence

The courts did not respond to specific and pertinent objections from the defense

Formal procedure

Impression that the proceedings were conducted "as a mere formality"

Concrete effects

Reopening of proceedings and compensation to the applicant

Impact Beyond Turkey: The Valencia Judgment of January 21, 2026

Although Yalçınkaya concerned ByLock and the Turkish context, its implications extend far beyond. The principles articulated by the Court are **technologically neutral** and directly relevant to cryptomessaging cases involving EncroChat, Sky ECC, or ANOM.

1

The Facts

Large-scale cocaine trafficking case, based primarily on Sky ECC datasets transmitted by French authorities

2

The Evidence

Processed extracts of chats, translations, and police attributions. The raw data was not made available to either the court or the defense

3

The Reasoning

The Provincial Court expressly applied Yalçınkaya: in "chat-only" cases, the absence of raw data critically diminishes probative value

4

The Decision

Acquittal of all defendants due to insufficient evidence

Scope and Limits of the Valencia Ruling

From a defense perspective, this ruling represents a significant and welcome development. However, it is important to accurately understand its scope.

Cautious, Evidence-Based Approach

The court did not expressly declare a violation of Article 6 ECHR. It adopted an evidentiary approach: applying the preponderant weight criterion, it concluded that a conviction could not be sustained solely on police-processed summaries that could not be independently verified.

No Categorical Exclusion

The ruling does not exclude cryptomessaging evidence as such, nor does it categorically condemn investigative practices involving Sky ECC or similar platforms. Encrypted communications can support investigations and corroborate other evidence.

A Clear Line

Encrypted communications cannot, without adequate procedural compensation, constitute the sole or decisive basis for a conviction. This is the boundary that the court clearly draws.

EUROPEAN LEVEL

The European Response: Italy and Belgium

Source: Joint Defense Team, 'EncroChat & SkyECC: Reliability of Digital Evidence' (2026)

Italy (EncroChat Case)

- The presiding judge was not convinced "beyond a reasonable doubt".
- The judge explicitly noted that, because the appointed expert could not prove the reliability of the data, its probative value was insufficient.
- This aligns with the CJEU ruling of April 30, 2024: the responsibility for verifying the reliability of evidence rests solely with the court judge.
- If the defense cannot examine the data, the judge cannot be satisfied with its integrity.

Belgium (Antwerp Court of Appeal)

- Members of the Joint Defense Team defended a case where the prosecution presented different data sets that were supposedly "identical".
- A digital expert investigation from the UK revealed:
  - **Significant Discrepancies:** The data sets were not identical, despite the prosecution's claims.
  - **Lack of Data Reliability:** Multiple specific errors led the expert to rule that the data set itself was "unreliable".
  - **Need for Raw Data:** The only way to provide an adequate review of reliability is through access to raw data and the full chain of evidence.

EUROPEAN LEVEL

European Standards and the European Law Institute's Proposal

These judicial developments coincide with broader regulatory efforts at the European level. In May 2023, the **European Law Institute (ELI)** adopted a Proposal for a Directive on the Mutual Admissibility of Evidence and Electronic Evidence in Criminal Proceedings.

As Professor Lorena Bachmaier has analyzed, the Proposal responds to the growing legal uncertainty caused by the lack of harmonized standards for cross-border electronic evidence.

Objective

Establish minimum standards to ensure fundamental procedural safeguards

Guiding principle

Mutual recognition cannot equate to blind trust

Right of defense

Possibility to challenge the legality and integrity of decisive electronic evidence

Clear convergence: Both Yalçınkaya and the ELI Proposal emphasize that fairness in criminal proceedings requires real and effective defense rights, access to meaningful scrutiny of digital evidence, and safeguards proportionate to the probative weight of such evidence.

Conclusion: Technology Must Adapt to Law

From a defense perspective, the handling of electronic evidence on mobile devices—particularly encrypted communications—has become one of the central battlegrounds of contemporary criminal justice.

The jurisprudence of the ECHR and national courts like those in Spain reflects a continuous effort to recalibrate the balance between effective law enforcement and fundamental procedural rights.

Transparency

Courts must insist on the transparency of technical sources and processes

Verifiability

The defense must be able to independently verify data integrity

Proportionality

Safeguards must be proportionate to the probative weight of digital evidence

> *"The right to a fair trial does not lower its standards for technological convenience. It is technology that must adapt to the law."*
>
> — Yüksel Yalçınkaya v. Turkey, ECHR, Grand Chamber, 2023

María Barbancho | www.barbancho.legal

Digitalization of justice: What impact on the defense?

February 12th, 2026

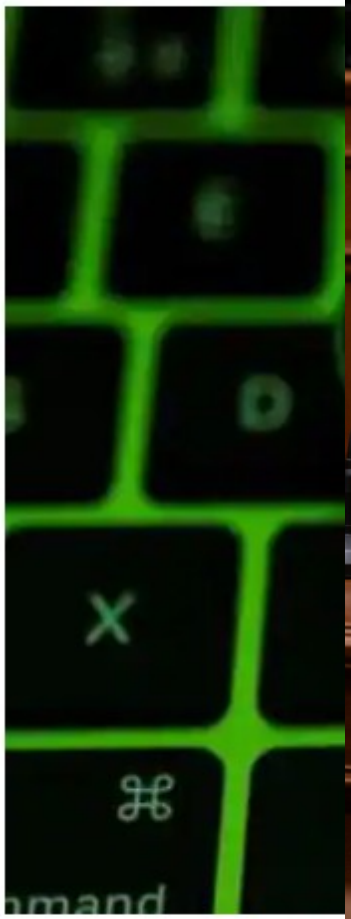
Andreu Van den Eynde

Co-funded by the European Union

Pegasus spy
European U

Edited By: Nishtha Badgamia

Brussels, Belgium • Updated: Nov



Reports suggest that the spy
version, Predator are some o

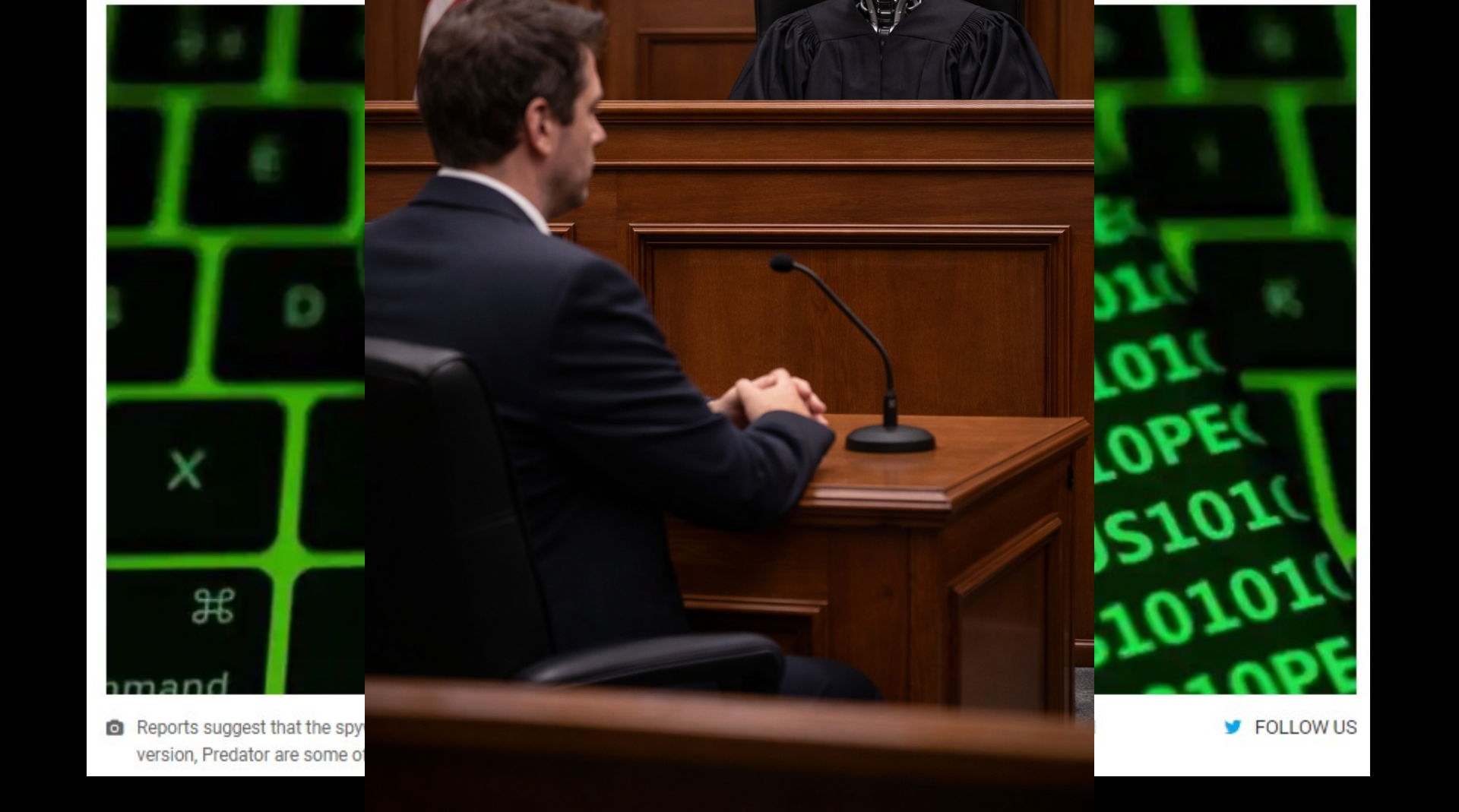
lown

FOLLOW US

Pegasus spy … lown European U…

Edited By: Nishtha Badgamia

Brussels, Belgium • Updated: Nov …



Reports suggest that the spy… version, Predator are some o…

FOLLOW US

Digitalization and defense rights

- Neutrality and reliability of technology
- Data overload
- Chain of custody
- OSINT investigations
- Technology to protect victims' rights
- Videoconferencing and hearings
- Artificial intelligence in criminal justice

Neutrality of technology

- Strong dependency on private forensic tools
- Undisputed findings
- No access to source code
- Lack of understanding of AI findings

Pegasus spyware scandal becomes a ‘full-blown European Union affair’: Report

Edited By: Nishtl
Brussels, Belgiu

Reports suggest that the spyware developed by the Israeli-based company NSO Group, Pegasus, and its less sophisticated version, Predator are some of the most well-known brands in Europe. Photograph:(Reuters)

FOLLOW US

Algorithmic transparency

Supreme Court 11/09/2025:

The right of access to public information acquires particular significance in light of the risks inherent in the use of new technologies in the exercise of public powers or in the provision of public services, as occurs with the use of **automated decision-making systems** in the activities of public administrations, especially when they concern the recognition of **social rights**.

In such cases, this right entails requirements of transparency regarding the computational processes followed in those actions, with the aim of providing citizens with the information necessary to understand them and to be aware of **how they function**. This may, in certain instances, require **access to the source code**, in order to enable verification that the algorithmic system complies with the regulatory provisions it is required to apply.

Algorithmic transparency

WhatsApp Inc. v. NSO Group Technologies Ltd.

U.S. District Court, N.D. California, Dec. 20, 2024.

Overall, the court concludes that defendants have repeatedly failed to produce relevant discovery and failed to obey court orders regarding such discovery. Most significant is the **Pegasus source code**, and defendants' position that their production obligations were limited to only the code on the AWS server is a position that the court cannot see as reasonable given the history and context of the case. Moreover, defendants' limitation of its production such that it is viewable only by Israeli citizens present in Israel is simply impracticable for a lawsuit that is to be litigated in this district.

Data overload

- Formal access to data vs. effective defense

Chain of custody

- Legality vs. reliability
- Formalities vs. practical opacity

OSINT investigations

- Authenticity
- Impact of AI
- Defense capacity

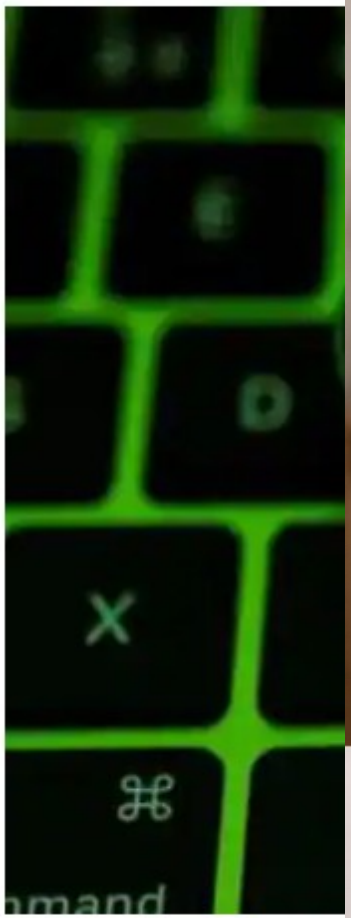
Victims' rights

- Anonymization
- Image and voice distortion
- Secondary victimization

Pegasus spy … European U… …lown

Edited By: Nishtha Badgamia

Brussels, Belgium • Updated: Nov 0…



Reports suggest that the spy… version, Predator are some o…

FOLLOW US

Expert witnesses: Public vs. Private

- *Private experts are not trustworthy. They are not impartial because they are paid by one party* (Huelva High Court 01/10/2009).
- *Courts must reason why they choose the public expert conclusions instead of the private expert conclusions. Lack of impartiality of private experts cannot be presumed* (Barcelona High Court 09/03/2016).

Daubert standard

Daubert v. Merrell Dow Pharmaceuticals, Inc. (U.S. Supreme Court, 1993)

- Specialized
- Experienced and updated
- Using scientific methodology
- Clearly explained coherent conclusions
- Submission to criticism and debate

Videoconferencing

- Pros and Cons
- General procedural option (258 bis CPC) except for serious crimes

Artificial Intelligence

- Risks and biases
- Regulating AI for judges
- Regulating AI for lawyers

Use of AI in Judicial Activity

Instruction 2/2026 (CGPJ)

- Effective human control — AI assists, does not replace judges.
- Non-substitution — judges remain decision-makers.
- Judicial responsibility & independence — accountability is always with the judge.
- Respect for fundamental rights — AI must protect rights, not override them.
- Confidentiality & security of judicial information.
- Mitigation of algorithmic bias and proportional use of AI.
- Training & capacity building — judges must be equipped to use AI.

Digitalization of justice: What impact on the defense?

Andreu Van den Eynde
www.eynde.es
andreu@icab.es
@eyndePenal

University of Antwerp
Faculty of Law

Dealing with e-evidence in cross-border cases: best practices and possible new scenarios in light of the new EU legislation

Prof. dr. Joachim Meese

associate professor

attorney

Co-funded by the European Union

Introduction and background

- e-evidence, MLA, EIOD, and EPO in a nutshell -

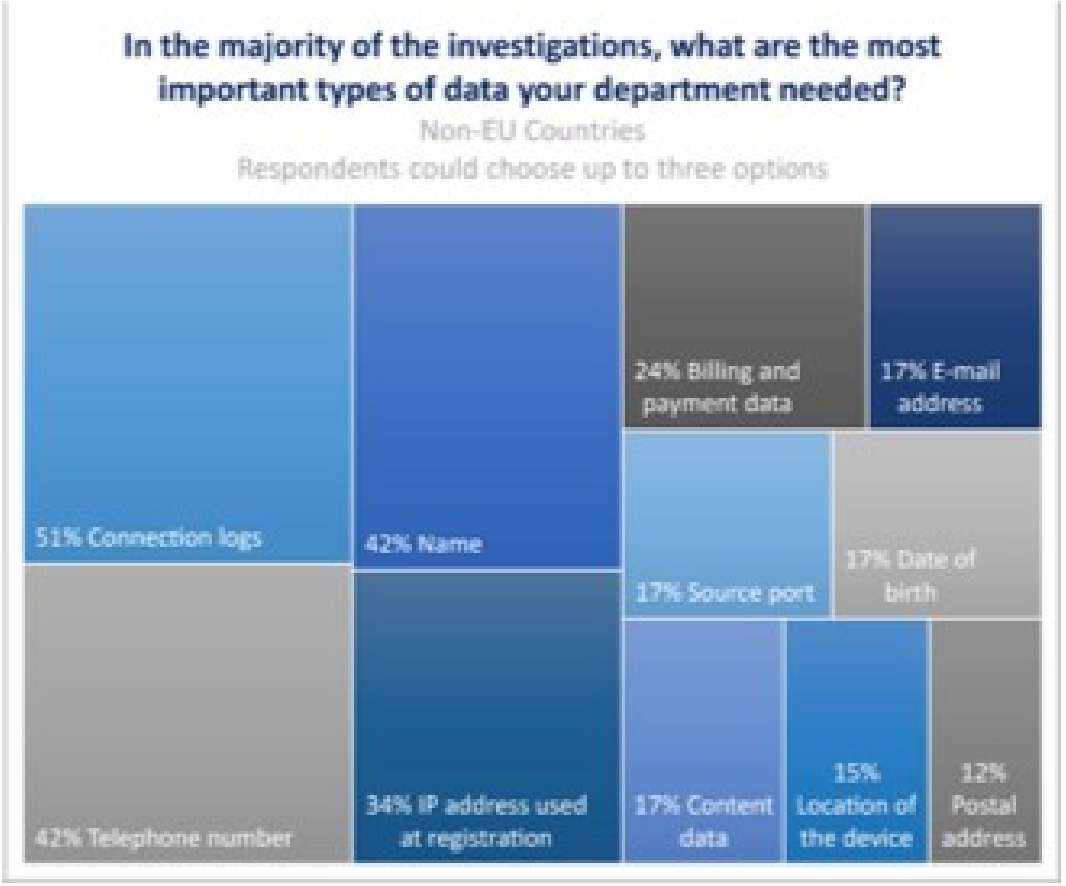
- historical background -

most common types of e-evidence

- **basic subscriber information**
  - e.g. name, e-mail, phone number, …
- **traffic data**
  - e.g. connection logs, number of messages, …
- **content data**
  - e.g. photos, content of messages or e-mails, files, …

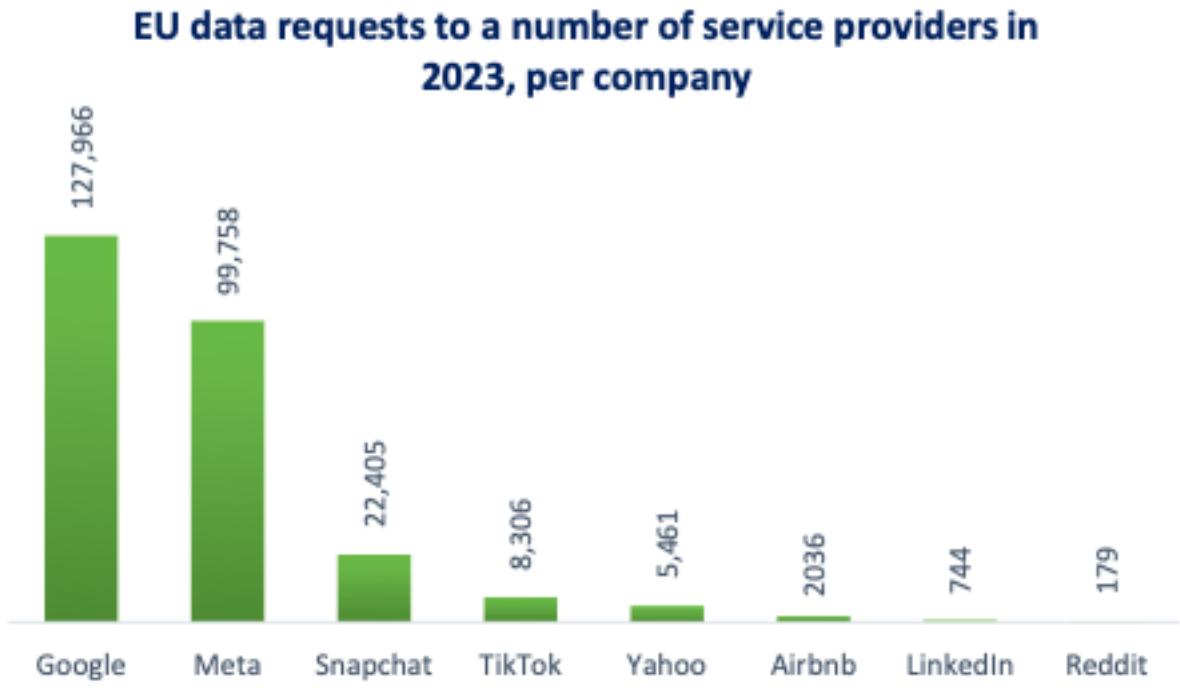
most common types of e-evidence

- most often needed type of e-evidence from foreign authorities or online service providers in 2024:



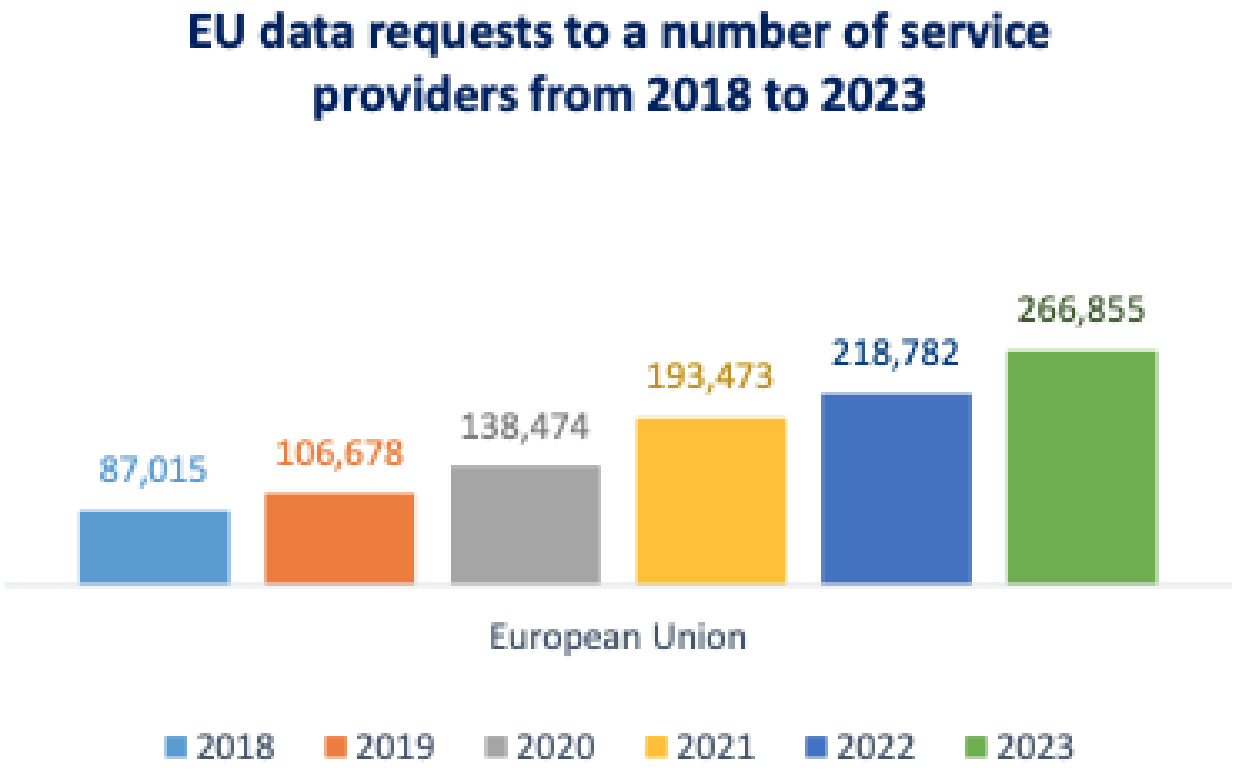
most common types of e-evidence

- **three most contacted online service providers in 2024:**



most common types of e-evidence

- **EU data requests till 2023:**



characteristics of e-evidence

- **volatile, can easily and quickly be deleted**
- **cross-border**
  - according the Commission 85% of criminal investigations require electronic evidence
  - approx. 2/3 of electronic evidence is located in another State (both within and outside the EU)
- **necessity for quick intervention**
- **hard to locate and access evidence**
  - e.g. in cases where the origin of cyber-attacks or location of e-evidence is not (yet) known
  - data redundancy

dealing with e-evidence

- **cloud-stored data: what about jurisdiction?**
  - possible theories:
    - criminal event theory (territorial)
    - criminal instrument theory (territorial)
    - direct consequence theory (extra-territorial)
    - nationality principle theory (extra-territorial)

dealing with e-evidence

- **key aspects:**
  - ensuring authenticity of digital data
  - chain of custody
    - proper and detailed documentation of access to data, its storage, copying and analysis (without changing the data)
    - analysis and further work with digital data is only done with a copy, not the original set of data
    - proper documentation of the police staff that is involved and the IT forensic software that is being used
  - see ACPO Good Practice Guide for Digital Evidence

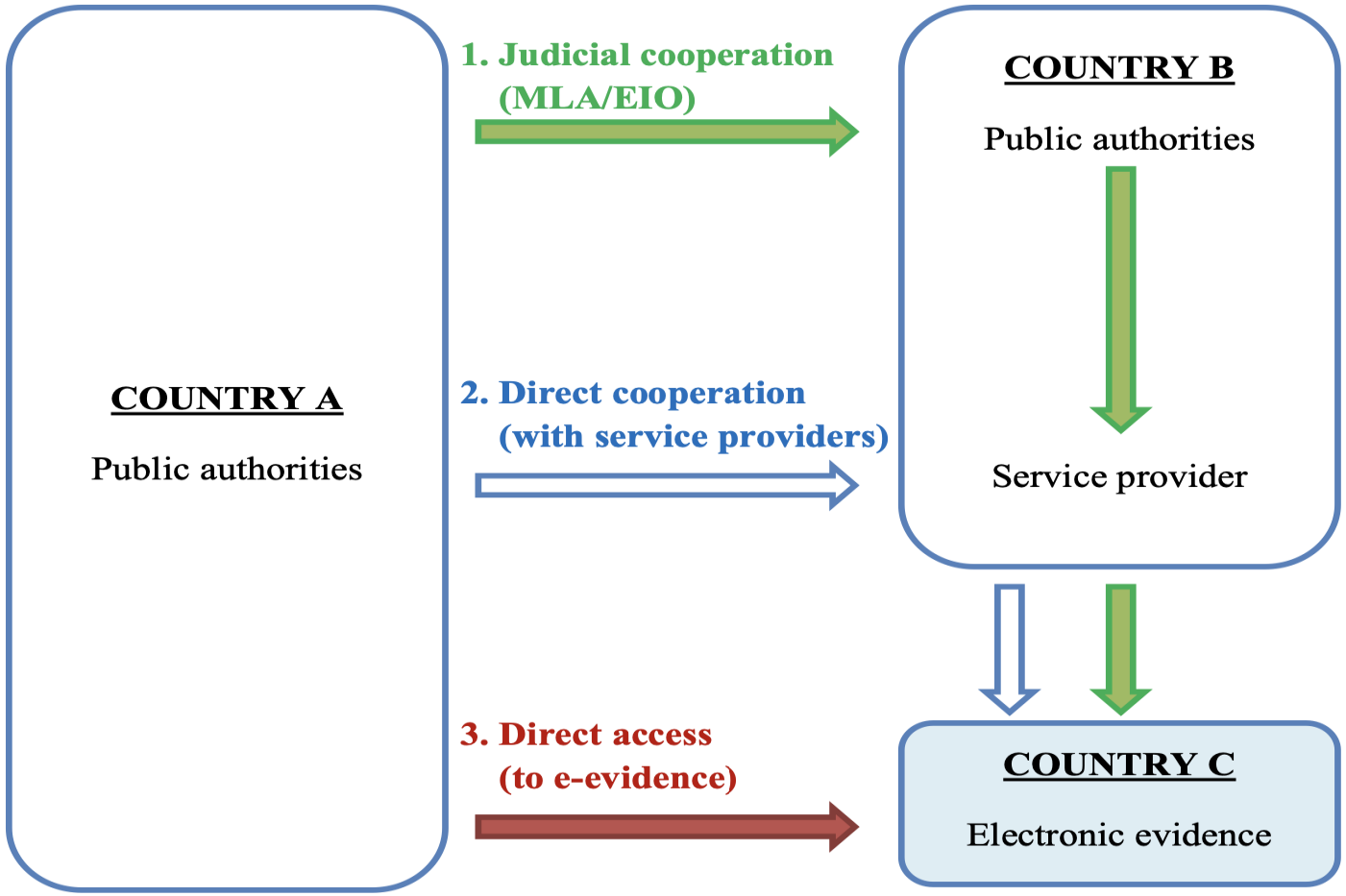
https://www.digital-detective.net/digital-forensics-documents/ACPO_Good_Practice_Guide_for_Digital_Evidence_v5.pdf

dealing with e-evidence

- **common procedures for recognising & handling e-evidence**
  - in most European member States: no specific regulations
    - e.g. Belgium
  - therefore:
    - general principles of dealing with analogue evidence also apply to digital/electronic evidence
    - (soft) regulations within different authorities (e.g. police, federal authorities like the Belgian FCCU)
    - best practices and efforts to certificate certain IT forensic software
    - legislation on the international/European level

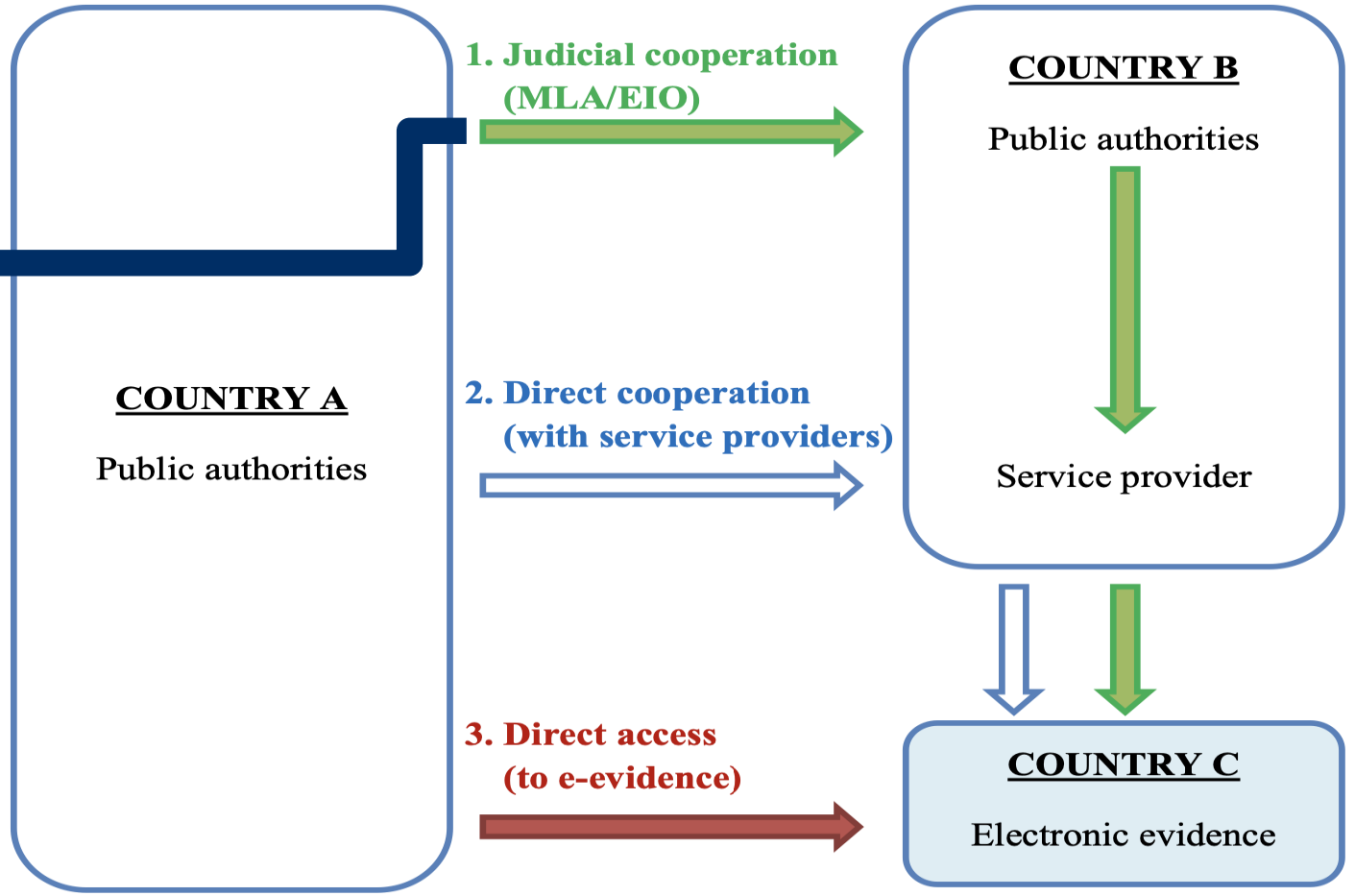
cross-border access to evidence

- **possible scenarios:**



cross-border access to evidence

- **possible scenarios:**



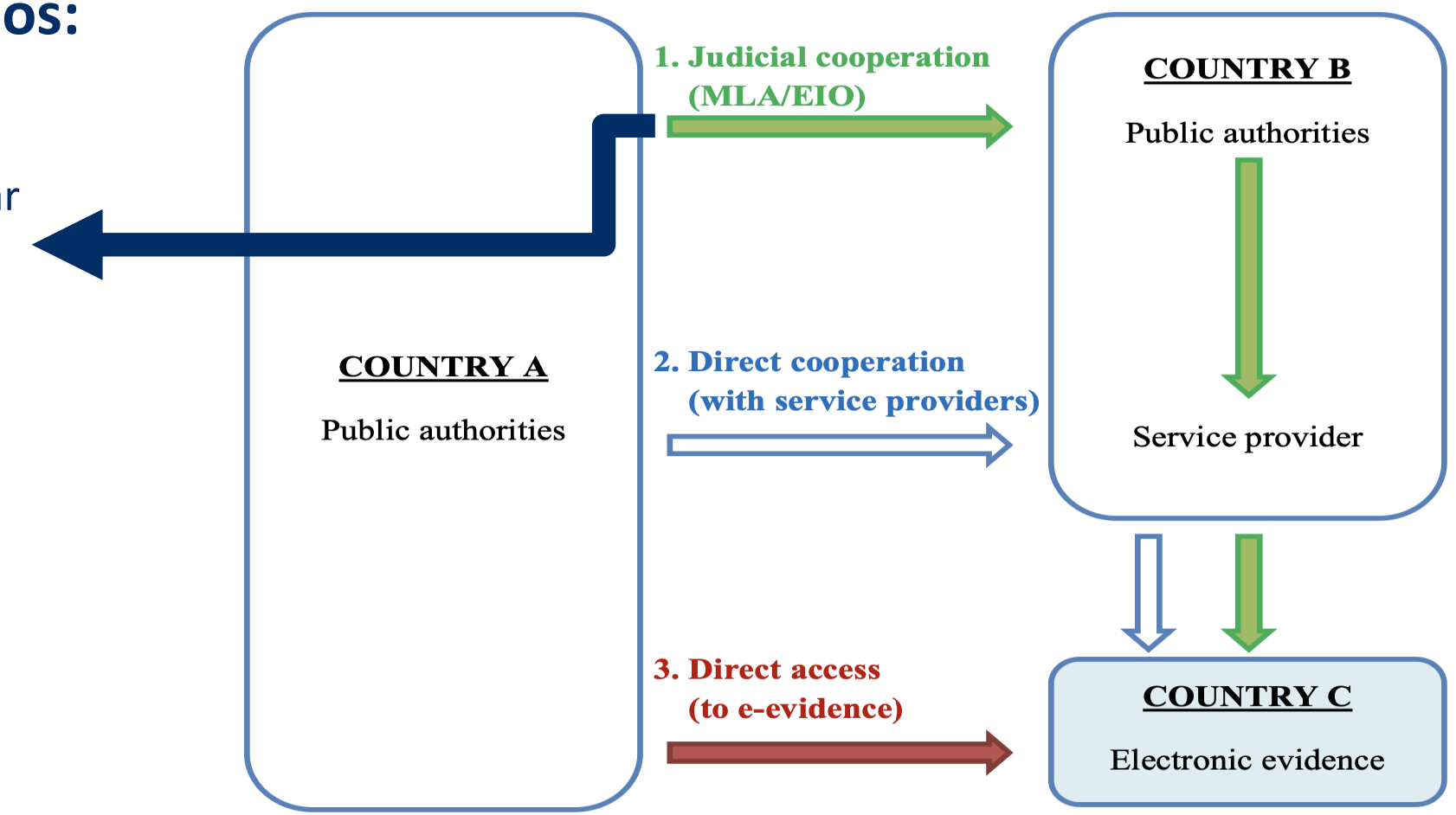
- ✓ within EU: EIO
- ✓ outside EU: international agreements
  - Budapest Convention on cybercrime
    - 2nd additional protocol can be signed by MS in the interest of the EU (Council decision of 5 April 2022)
      - ✓ improve international cooperation
      - ✓ enhance direct cooperation
      - ✓ emergency mutual assistance
  - bilateral agreements concluded by
    - the EU (e.g. the agreement with the US of 23 October 2009)
    - the member States (most frequently with the US, Canada or Australia)

cross-border access to evidence

- **possible scenarios:**

number of requests per year on e-evidence:

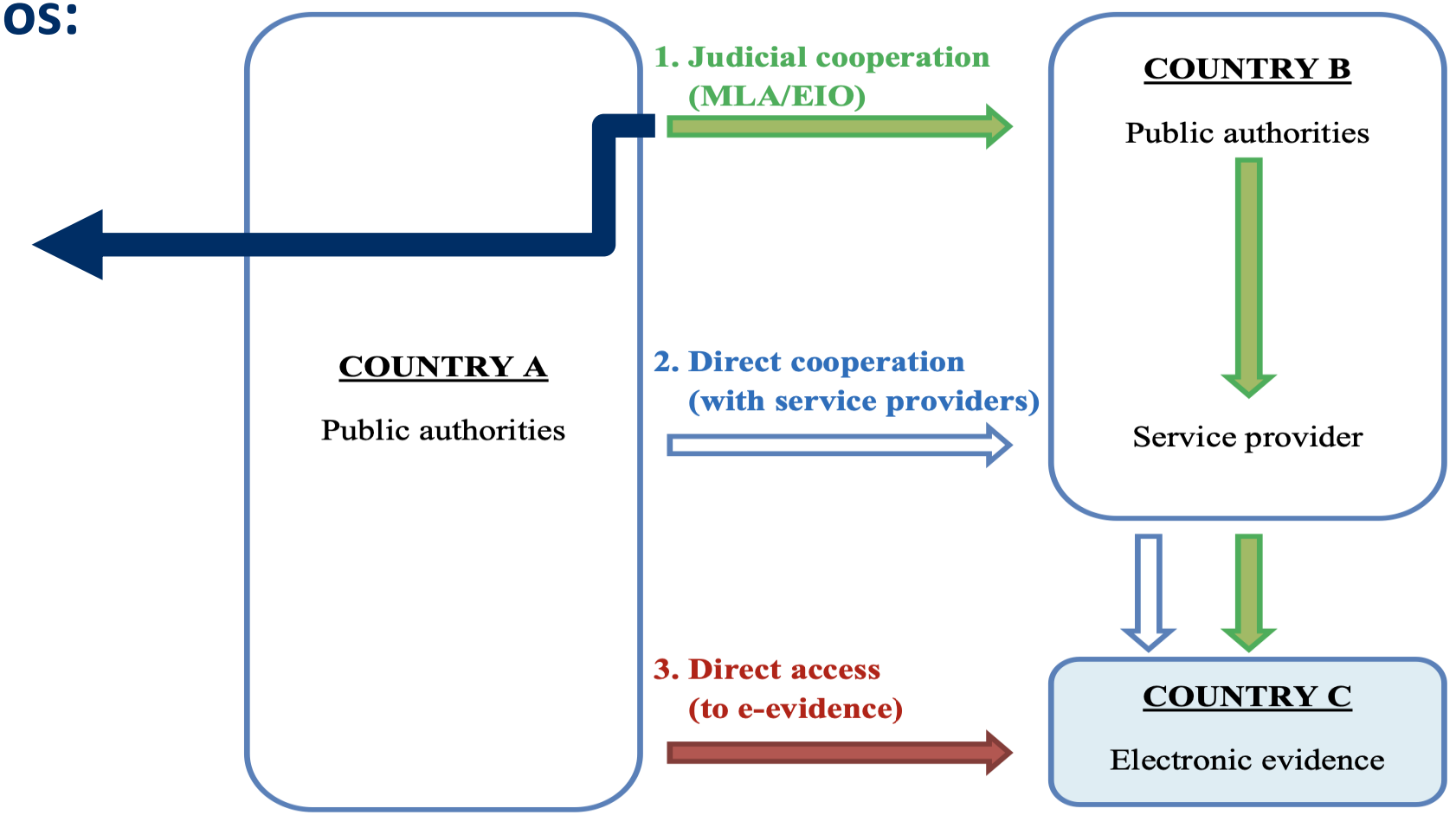
- ✓ between EU member States: 13.000
- ✓ EU MS to US: 1.300



cross-border access to evidence

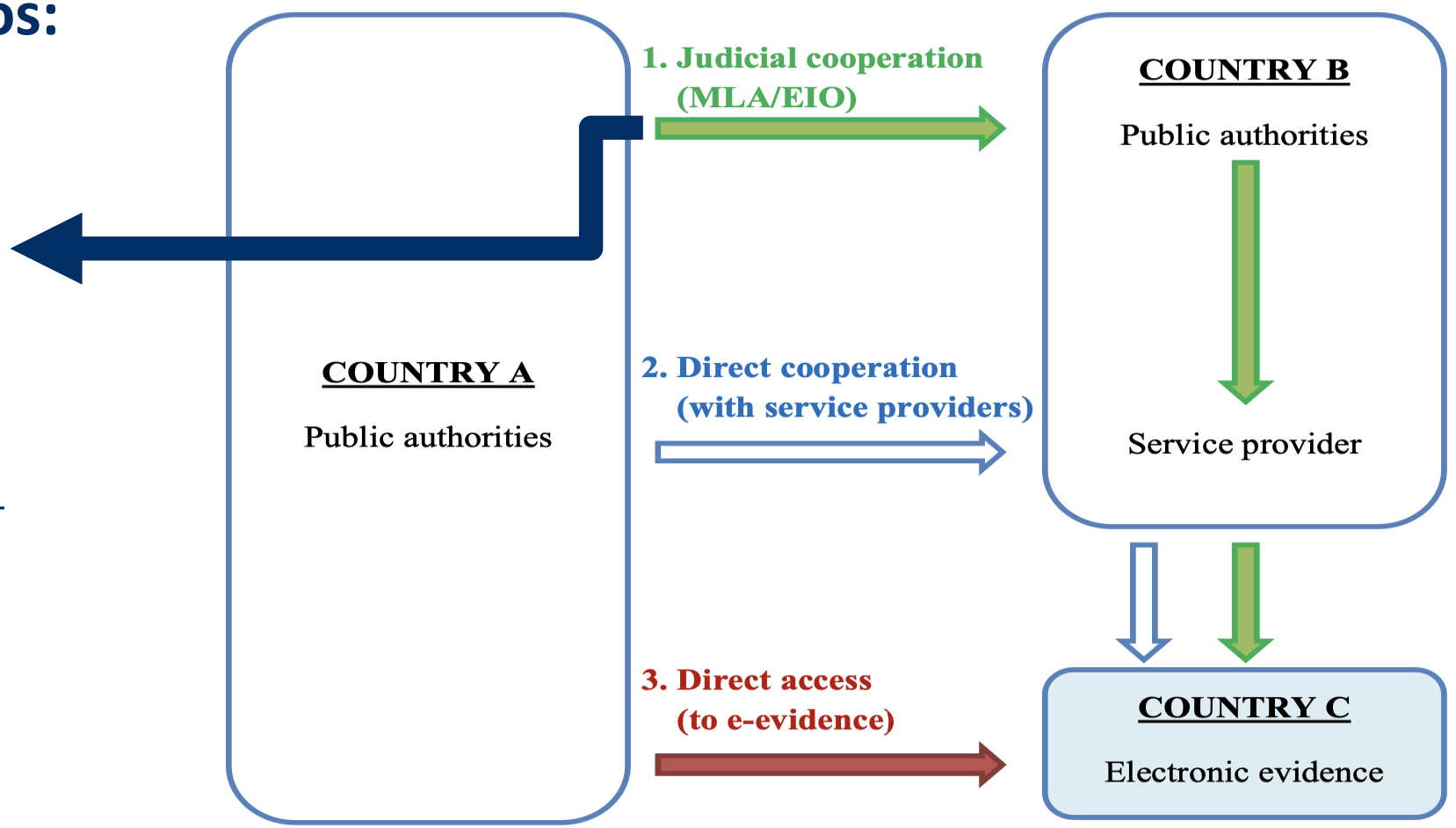
- **possible scenarios:**

✓ MLA challenges
- hard to get a timely response to a request
- too much formalities
- too complicated and technical to use



cross-border access to evidence

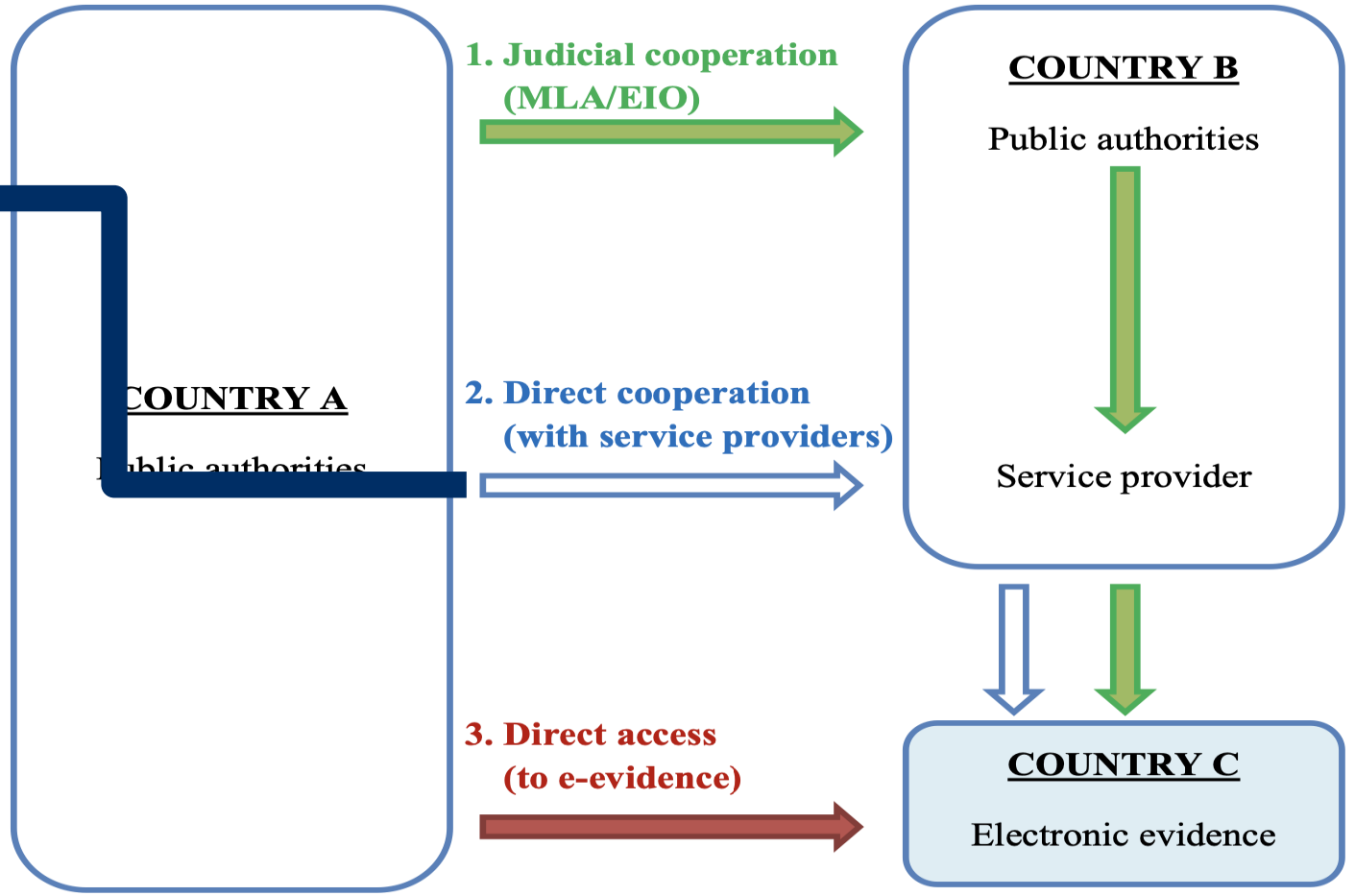
- **possible scenarios:**



✓ EIO challenges
- Ireland, Denmark and UK are not bound
- too slow for e-evidence
- too formalistic for e-evidence
- not adapted to complex e-evidence situations
- high cost and capacity requirements
- legal impediments

cross-border access to evidence

- **possible scenarios:**



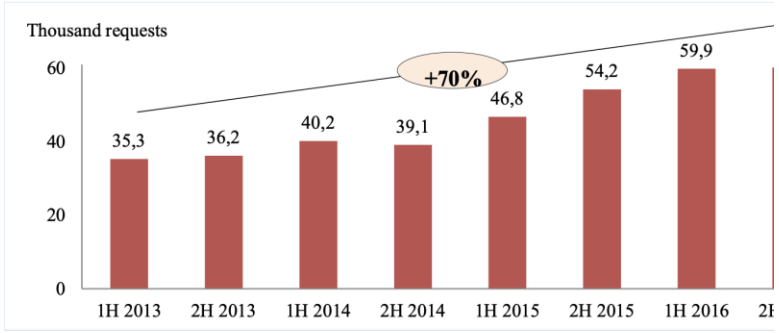
✓ non-content data
- service providers established in the US and, to a more limited extent, in Ireland, which reply directly to requests from EU member States law enforcement authorities on a voluntary basis

✓ WHOIS data
- service providers make data directly available to authorities through a centralised search system which does not rely on individually reviewed requests

cross-border access to evidence

- **possible scenarios:**

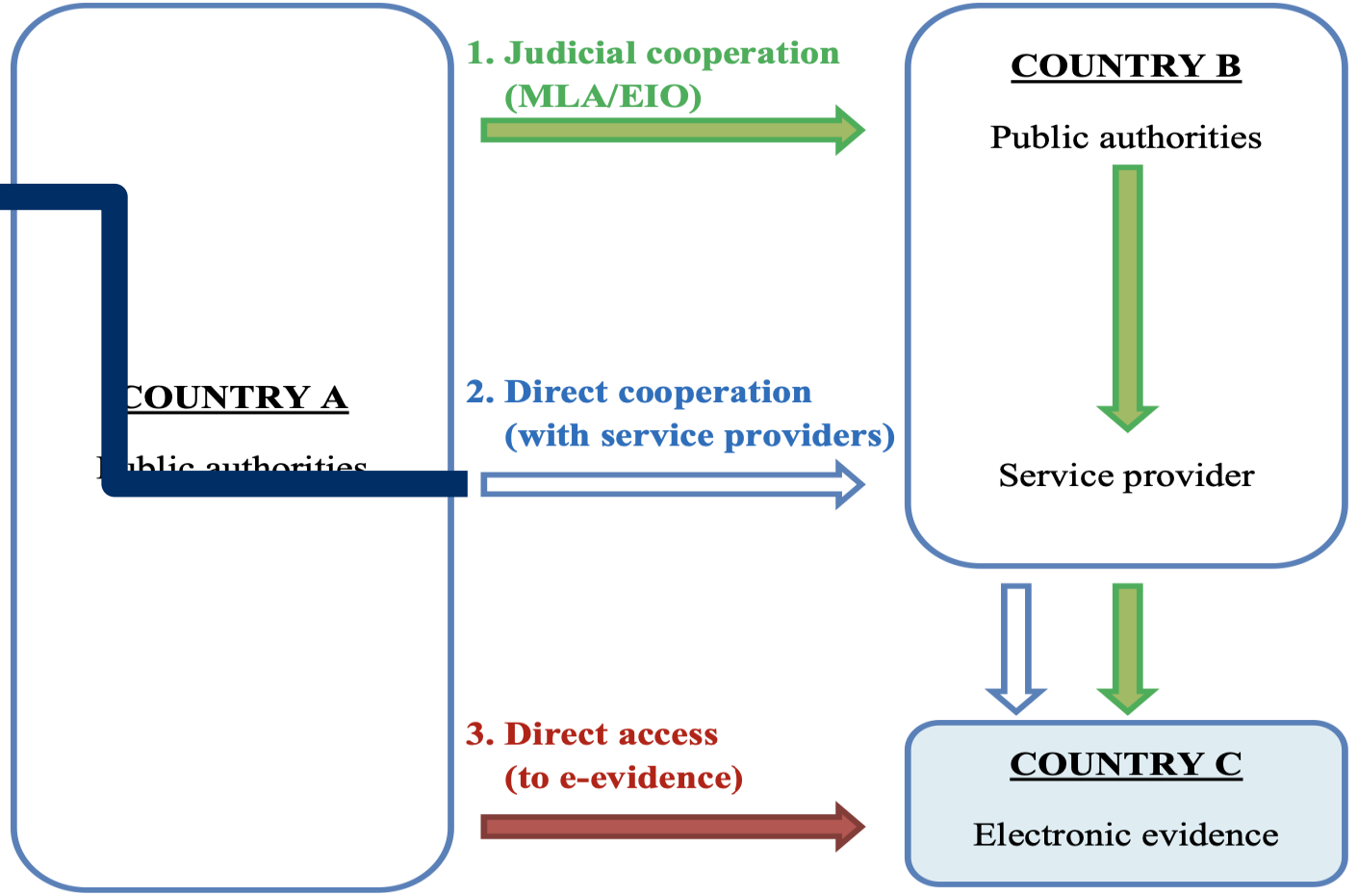
numbers:



→ in 2018, 3 member States account for > 75% of all requests from the entire EU

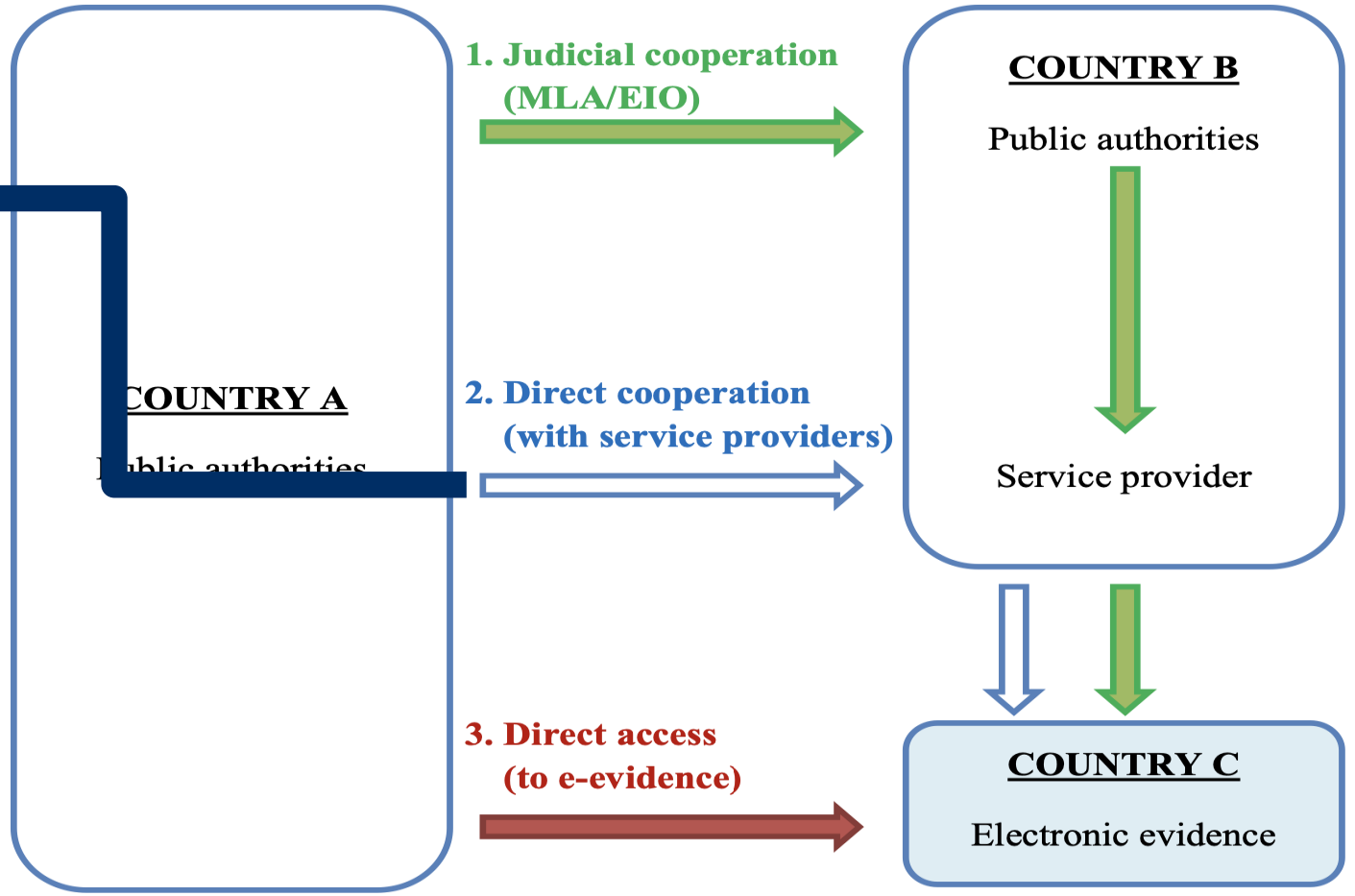
- Germany: 35.271
- UK: 28.598
- France: 27.268

→ Google & Facebook: 70% of total requests



cross-border access to evidence

- **possible scenarios:**



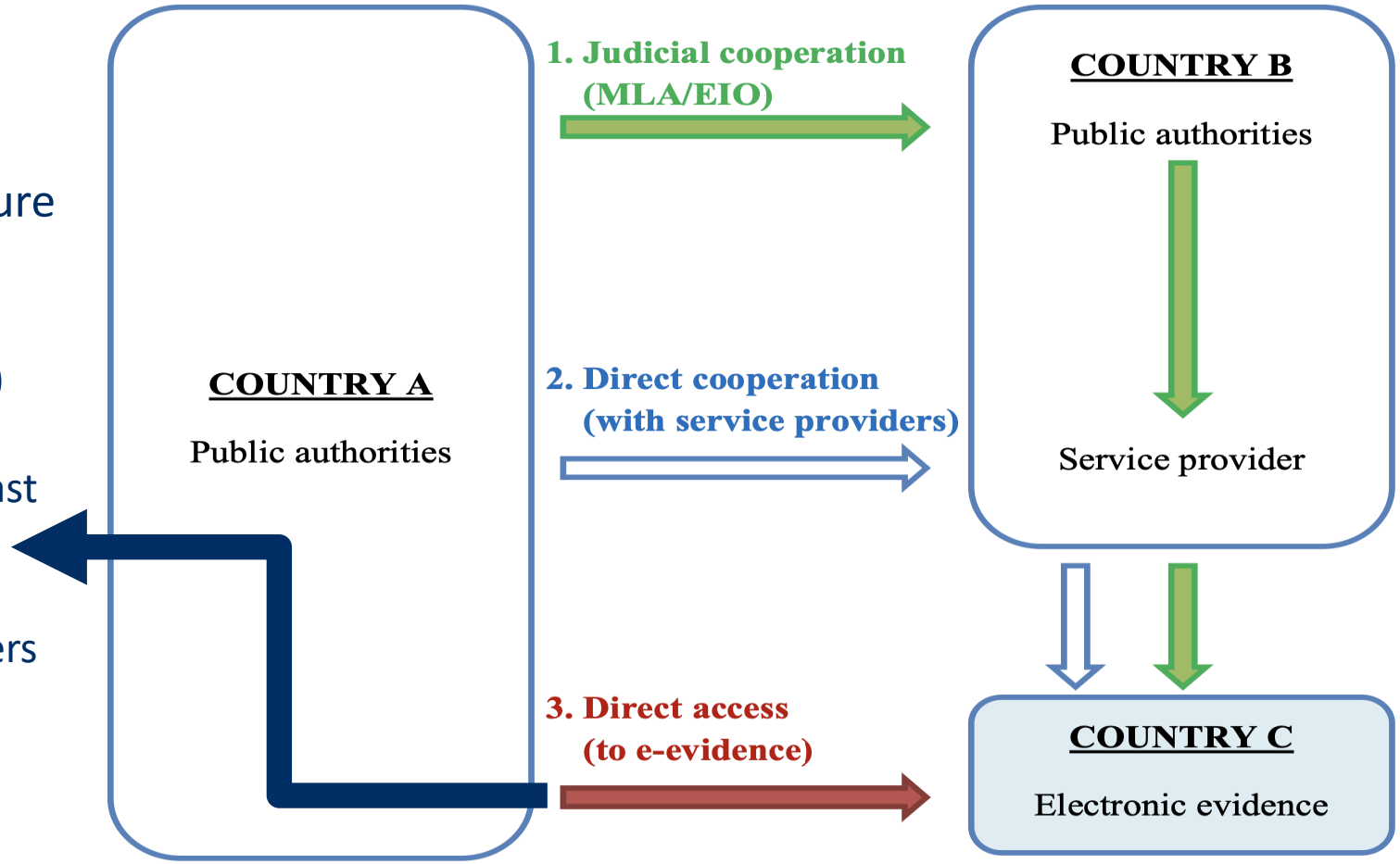
✓ challenges
- can be unreliable
- can take too long
- only possible with a limited number of service providers
- providers all apply different policies
- not transparent
- lacks accountability in case of non-compliance
  - see, however the Belgian case of YAHOO! (Cass. 1 December 2015, P.13.2082.N)

cross-border access to evidence

- **possible scenarios:**

✓ extended search (following seizure of a device)
✓ remote search (following lawful acquisition of login information)

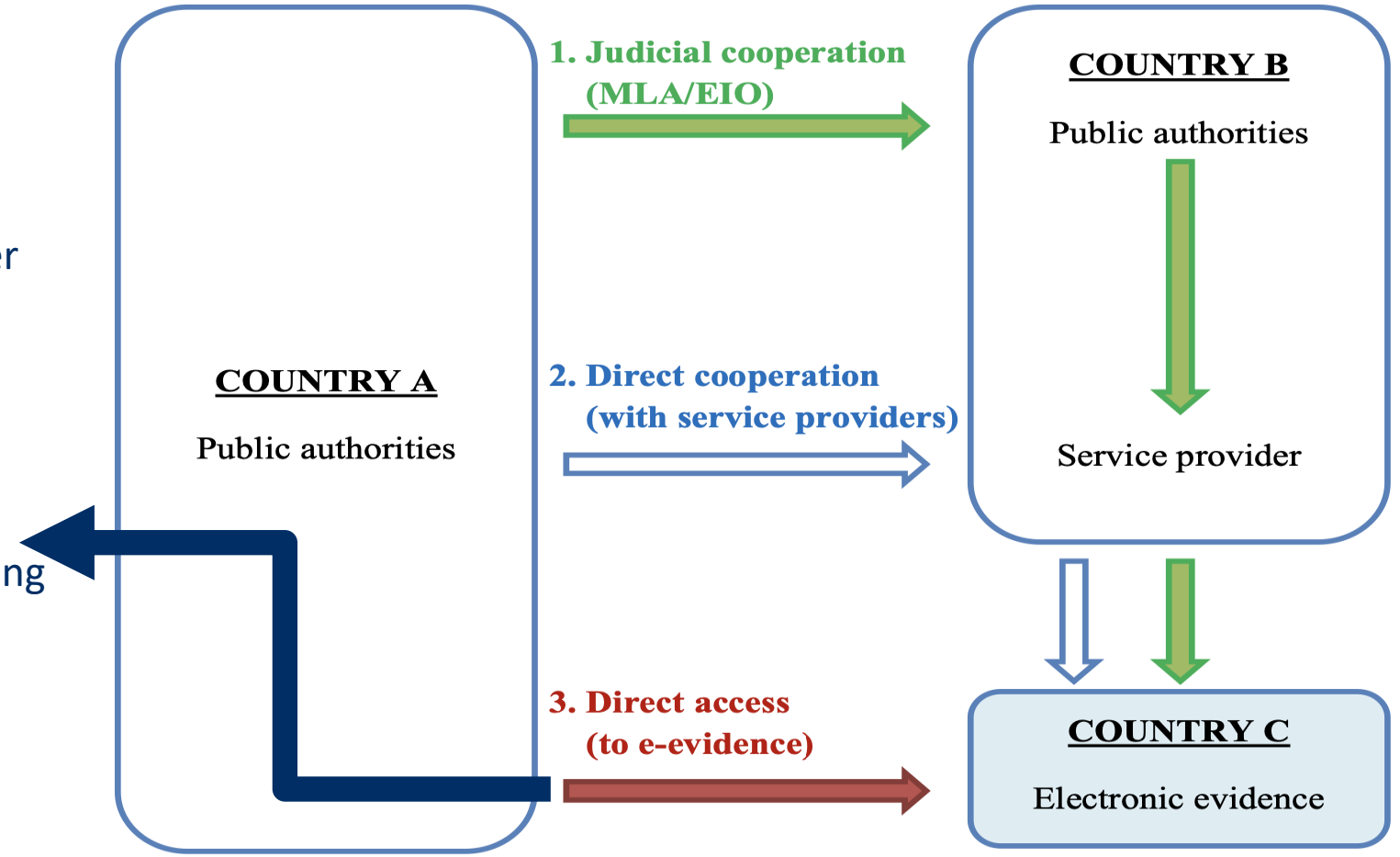
→ possible under national law of at least 20 member States
→ this tool becomes more relevant
  - data are regularly stored on servers in a different location
  - in case of loss of knowledge of location of data (e.g. Darknet)



cross-border access to evidence

- **possible scenarios:**

✓ challenges
- different approaches by member States to direct access & to data storage location
- risk of losing data
  - ✓data can easily and swiftly be deleted from another device
  - ✓data can be lost when gathering and moving it



cross-border access to evidence: what about EPO?

- **EPO**
  - Regulation (EU) 2023/1543 on European Production Orders and European Preservation Orders for electronic evidence in criminal proceedings and for the execution of custodial sentences following criminal proceedings
    - http://data.europa.eu/eli/reg/2023/1543/oj
    - applies from **18 August 2026**
  - Directive (EU) 2023/1544 laying down harmonised rules on the designation of designated establishments and the appointment of legal representatives of gathering electronic evidence in criminal proceedings
    - http://data.europa.eu/eli/dir/2023/1544/oj
    - must be transposed into national law by **18 February 2026**

cross-border access to evidence: what about EPO?

- **EPO**
  - what:
    - the Regulation: legal framework laying down the rules under which an authority of a Member State may order a service provider offering services in the Union, to produce or preserve electronic evidence, regardless of the location of data
      - European Production Order (EPOC)
      - European Preservation Order (EPOC-PR)
    - the Directive: rules on the designation of designated establishments and the appointment of legal representatives of certain service providers that offer services in the Union, for the receipt of, compliance with and enforcement of decisions and orders issued by competent authorities of the Member States, for the purposes of gathering electronic evidence in criminal proceedings
  - background: driven by the fight against terrorism
    - establishing security is one of top policy priorities of the EU
    - an instrument for transnational access to e-evidence in the EU is a pressing issue

cross-border access to evidence: what about EPO?

- **EPO**
  - texts & sources
    - original Commission proposal (17 April 2018)
      - https://www.europarl.europa.eu/RegData/docs_autres_institutions/commission_europeenne/com/2018/0225/COM_COM(2018)0225_EN.pdf
    - the Council's general approach (11 Juni 2019)
      - https://data.consilium.europa.eu/doc/document/ST-10206-2019-INIT/en/pdf
    - Report Committee on Civil Liberties, Justice and Home Affair (11 December 2020)
      - https://www.europarl.europa.eu/doceo/document/A-9-2020-0256_EN.html
    - Report from the Commission to the European Parliament and the Council (20 July 2021)
      - https://data.consilium.europa.eu/doc/document/ST-11007-2021-INIT/en/pdf
      - launch of EU-US negotiations to facilitate access to electronic evidence: 19 July 2021
    - Draft regulation:certain issues (26 August 2021)
      - https://db.eurocrim.org/db/en/doc/3646.pdf

cross-border access to evidence: what about EPO?

- **EPO**
  - texts & sources
    - State of play and possible ways forward (16 September 2021)
      - https://www.statewatch.org/media/2739/eu-council-e-evidence-regulation-state-of-play-11681-21.pdf
      - Report of 20 December 2021: https://www.europarl.europa.eu/doceo/document/A-9-2021-0356_EN.html
      - update of 23 February 2022: https://www.statewatch.org/media/3175/eu-council-e-evidence-4-col-doc-regulation-6487-22.pdf
      - letter of EP's rapporteur (16 February 2022): https://www.statewatch.org/media/3174/eu-council-e-evidence-mep-rapporteur-letter-6323-22.pdf
    - Final compromise text (20 January 2023): https://data.consilium.europa.eu/doc/document/ST-5448-2023-INIT/en/pdf

cross-border access to evidence: what about EPO?

- **EPO**
  - texts & sources
    - 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
      - https://eur-lex.europa.eu/legal-content/EN/HIS/?uri=COM:2018:226:FIN
      - general approach: https://data.consilium.europa.eu/doc/document/ST-7348-2019-INIT/EN/pdf
      - final compromise text (20 January 2023): https://data.consilium.europa.eu/doc/document/ST-5449-2023-INIT/en/pdf

Comparative scheme: key characteristics

MLA

- traditional instrument of international cooperation
- all kinds of investigative measures
- important in the relationship with third States, mainly with the USA
- complex, lots of formalities, takes time

EIO

- all kinds of investigative measures (except in the framework of JIT)
- inspired by mutual recognition
- execution by domestic authorities or by third parties
- in theory within 120 days
- Directive

EPO

- only for electronic information
- restricted to criminal proceedings
- directly addressed to service provider and to executing authority
- some orders can be issued for all criminal offences and for most types of data stored
- location of data is not relevant
- a new type of cooperation instrument based on advanced form of mutual trust
- (extraordinary?) simplification of procedure
- Regulation (no transposition!)

Comparative scheme: visual representation

More about EIO

- basic premise & scope -

- procedure -

- challenges and limitations -

EIO – basic premise

- **Replace existing legal framework by creating 1 single legal instrument (introductory remark 7 EIOD)**
- **Mutual recognition (art. 1(2) EIOD)**

=> inspired by:

- mutual recognition of judgments and judicial decisions
- mutual recognition of orders to prevent the destruction, transformation, moving, transfer or disposal of evidence
- European evidence warrant
- European arrest warrant

⇒ principally an instrument for the authorities to gather evidence abroad

- the EIOD doesn't regulate the position of the defence, e.g. possibility to be present at the execution of specific investigative measures (such as witness examination), or the right for the defence to have a EIO issued

EIO – including e-evidence?

- **Applicable to any investigative measure (art. 3 EIOD):**
  - including gathering of e-evidence
  - except in framework of Joint Investigation Team (JIT)
- **In the context of e-evidence:**
  - specific provisions on the interception of telecommunications (art. 30 EIOD)
  - no other specific provisions regarding electronic evidence
    - except for a reference to the identification of a person holding an IP address or telephone number (art. 10(2)(e) EIOD)

EIO - procedure

- **EIOD: procedural steps (1/3)**
  1. national request prepared and judicially approved based on individual national standard and EIO rules (art. 5-6 EIOD)
     - particular form + content requirements: art. 5 EIOD + Annex A
     - translation of the EIO is required (art. 5, §3 EIOD)
  2. EIO sent directly to relevant judicial authority in relevant country (art. 7 EIOD)
     - by any means capable of producing a written record to guarantee authenticity
     - via the telecommunications system of the European Judicial Network
     - via E-Codex (https://www.e-codex.eu)

EIO - procedure

- **EIOD: procedural steps (2/3)**

3. EIO examined by receiving judicial authority
   - verification of EIO (art. 5-6 EIOD)
   - verification of grounds of refusal
     - ➢ important in a cybercontext:
       - ✓ similar investigative measure exception (art. 11 (c) + (h) EIOD)
       - ✓ dual criminality exception (art. 11 (e) + (g) EIOD)
       - ✓ fundamental rights exception (art. 11 (f) EIOD)
4. execution
   - executed directly by domestic investigative authorities OR
   - EIO served and then executed (if possible) by third parties (e.g. service provider)
   - recourse to a different type of investigative measure (art. 10 EIOD)

EIO - procedure

- **EIOD: procedural steps (3/3)**
  5. evidence is sent back to executing judicial authority (art. 13 EIOD)
  6. costs: art. 21 EIOD
     - borne by the executing State
     - if exceptionally high: possibility to share or modify

EIO - procedure

- **EIO: timeline**
  - in theory: within 120 days (art. 12 EIOD)
    - 30 days for Member States to decide to accept request
    - then 90 days to execute requested investigative measure
    - unless urgency
  - but …
    - many consultation options (art. 6(3) EIOD, art. 7(7) EIOD), art. 10(4) EIOD, art. 11(4) EIOD, art. 21(2) EIOD)
    - grounds for non-recognition or non-execution (art. 11 EIOD)
    - grounds of suspension of transfer of evidence (art. 13(2) EIOD)
    - grounds for postponement of recognition or execution (art. 15 EIOD)
    - legal remedies (art. 14 EIOD)

EIO - procedure

- **EIO: specific regimes**
  - see Chapter IV EIOD
  - Relevant from e-evidence perspective: *the interception of telecommunications* (chapter V)
    - art. 30 §§7-8 + 31 EIOD
    - important aspects from an e-evidence perspective:
      - ➢ EIO shall be sent to only one Member State if more Member States are available to provide technical assistance
      - ➢ possibility to request decoding or decrypting of the recording
        - BUT no obligation
      - ➢ notification of Member State where the subject of the interception is located from which no technical assistance is needed

EIO - challenges and limitations

- **EIO: challenges in the field of e-evidence**
  - territorial limitations
    - only EU countries
      ⇒ no access to data held by service providers headquartered in non-EU countries
    - Ireland, Denmark and UK are not bound by the Directive
      ⇒ no access to data held by service providers headquartered in these countries
      ⇒ particularly in Ireland and UK a number of US service providers store data and have European headquarters
  - too slow for e-evidence
  - too formalistic for e-evidence?
    - long EIO forms to be completed
    - EIO translation is required
    - impossibility to directly address service providers

EIO - challenges and limitations

- **EIO: challenges in the field of e-evidence**
  - not adapted to complex e-evidence situations, where:
    - a number of information systems are used simultaneously in multiple jurisdictions to commit one single crime
    - relevant e-evidence moves between jurisdictions in short fractions of time
    - sophisticated methods are used to conceal the location of e-evidence or the criminal activity, leading to "loss of location”
  - high cost and capacity requirements
    - significant investment of resources/capacity from the receiving Member State, which may not be appropriate or necessary for all cases, especially when there is no link with the receiving jurisdiction besides the seat of the service provider
    - specialised training/personnel required to collect e-evidence in an appropriate manner

EIOD - challenges and limitations

- **EIO: challenges in the field of e-evidence**
  - legal impediments
    - on investigative acts-level:
      - ➢ risk for inconsistent interpretations
      - ➢ risk for conflicts between existing regulations
        - ✓ e.g.: dual criminality-requirements, domestic equivalent of investigative acts, …
      - ➢ 'limitations' due to data protection (art. 20 EIOD) and fundamental rights requirements
        - ✓ e.g.: obligation to decrypt vs. privilege against self-incrimination
    - on evidence level
      - ➢ no 'free movement' of evidence or minimum standards for evidence-gathering
      - ➢ risk of important discussions on admissibility/authenticity of e-evidence in criminal procedures due to different domestic standards
        - ✓ e.g. SKY ECC procedures (Cass. fr. 16 September 2025, n° 24-84.262, ECLI:FR:CCASS:2025:CR00936)
        - ✓ e.g. Cass. Belgium 11 January 2022, P.21.1245.N (https://juportal.be/content/ECLI:BE:CASS:2022:ARR.20220111.2N.1/NL)

More about EPO

- key principles & main concepts -

- scope & procedure -

- conditions & grounds for refusal -

EPO – the Regulation

- **Scope (art. 2)**
  - criminal proceedings
    - both during pre-trial and trial phase
    - also against legal persons
  - execution of a custodial sentence or detention order of at least 4 months, imposed by a decision that was not rendered in absentia
  - only for data pertaining to services rendered by service providers

EPO – the Regulation

- **Definitions (art. 3)**
  - service provider: anyone providing one or more of the following categories of services (except for financial services):
    - electronic communication services, such as:
      - internet access services
      - interpersonal communications services (messaging services, email services, internet telephony services, …)
    - internet domain name and IP numbering services, such as IP address assignment, domain name registries, and related privacy and proxy services
    - other information society services which enable users to communicate with each other, or to store or otherwise process data, such as social networks, online marketplaces and other hosting service providers

EPO – the Regulation

- **Definitions (art. 3)**
  - offering services in the Union:
    - enabling natural or legal persons in a Member State to use the aforementioned services; and
    - having a *substantial connection*, based on specific factual criteria, to the Member State referred to in the first point; such a substantial connection is to be considered to exist where the service provider has an establishment in a Member State, or, in the absence of such an establishment, where there is a significant number of users in one or more Member States, or where there is targeting of activities towards one or more Member States

EPO – the Regulation

- **Definitions (art. 3)**
  - data:
    - subscriber data: relating to the identity of the user, e.g. name, date of birth, billing and payment data, …
    - data requested for the sole purpose of identifying the user: IP addresses, logs and access numbers together with technical identifiers, …
    - traffic data: relating to the provision of a service, e.g. the geographic location of the device used, date, time, duration, …
      - more privacy-intrusive
      - under certain circumstances, IP addresses can be considered traffic data
    - content data: text, video, voice, images, sound, …

EPO – the Regulation

- **Definitions (art. 3)**
  - electronic evidence
    - subscriber data, traffic data, or content data lawfully stored by or on behalf of a service provider, in an electronic form, at the time of the receipt of an EPOC or EPOC-PR

EPO – the Regulation

- **Issuing authority (art. 4)**
  - EPOC
    - subscriber data & data for the sole purpose of identifying the user
      - a judge, a court, an investigating judge **or a public prosecuto**r competent in the case concerned, or
      - any other competent authority as defined by the issuing State which, in the case concerned, is acting in its capacity as an investigating authority in criminal proceedings with competence to order the gathering of evidence in accordance with national law → such EPOC requires review in the issuing State, which can also be done by a **public prosecutor**
    - traffic & content data
      - a judge, a court, an investigating judge competent in the case concerned, or
      - any other competent authority as defined by the issuing State which, in the case concerned, is acting in its capacity as an investigating authority in criminal proceedings with competence to order the gathering of evidence in accordance with national law → such EPOC requires **judicial** review in the issuing State (i.e. review by a judge, a court of an investigating judge)

EPO – the Regulation

- **Issuing authority (art. 4)**
  - EPOC-PR
    - all data categories
      - a judge, a court, an investigating judge or a public prosecutor competent in the case concerned, or
      - any other competent authority as defined by the issuing State which, in the case concerned, is acting in its capacity as an investigating authority in criminal proceedings with competence to order the gathering of evidence in accordance with national law → such EPOC-PR requires review in the issuing State, which can also be done by a public prosecutor

EPO – the Regulation

- **Conditions for issuing**
  - EPOC (art. 5)
    - necessary and proportionate
      - the EPOC may only be issued if a similar order could have been issued under the same conditions in a similar domestic case
    - EPOC for subscriber data & data for the sole purpose of identifying the user
      - may be issued for all criminal offences and for the execution of a custodial sentence or a detention order of at least 4 months
    - EPOC for traffic data or content data
      - requires a sentence of a max. of at least 3 years in the issuing State, or one of the offences as summed up in art. 5.4 (offences connected with cyber-crime, fraud relating to non-cash means of payment, terrorism and sexual abuse of children)
    - immunities and privileges: see art. 5.10

EPO – the Regulation

- **Conditions for issuing**
  - EPOC-PR (art. 6)
    - necessary and proportionate
      - the EPOC-PR may only be issued if a similar order could have been issued under the same conditions in a similar domestic case
    - may be issued for all criminal offences and for the execution of a custodial sentence or a detention order of at least 4 months

EPO – the Regulation

- **Legal representatives**
  - service providers shall designate or appoint at least one addressee for the receipt of, compliance with and enforcement of EPOC and EPOC-PR orders
  - those legal representatives:
    - must be staffed with the necessary powers and resources to comply with the orders
    - must **produce the data within the set deadlines**
    - are subject to possible sanctions in case of non-compliance
    - must ensure confidentiality, secrecy and integrity of the data produced and preserved

EPO – the Regulation

- **Execution timeframes**
  - EPOC (art. 10)
    - regular cases: within 10 days upon receipt
    - emergency cases : within 8 hours upon receipt
  - EPOC-PR (art. 11)
    - obligation to preserve the data for 60 days
    - can be extended by an additional 30 days

EPO – the Regulation

- **Grounds for refusal of EPOC orders (art. 8 and 12)**
  - **art. 8: situations in which enforcing States must be notified**
  - **art. 12: grounds for refusal by enforcing States: reasons related to**
    - immunities or privileges under the law of the enforcing State
    - freedom of press and freedom of expression
    - manifest breaches of fundamental rights “in exceptional situations”
    - ne bis in idem

EPO – the Regulation

- **Other provisions**
  - procedure for enforcement when service provider doesn't comply: art. 16
  - review procedure in case of conflicting obligations with third country law: art. 17
  - effective remedies: art. 18
  - art. 32: the use of EIOD or MLA for the gathering of electronic information is still allowed

EPO – the Regulation

- **Admissibility of evidence?**
  - former texts mentioned that evidence obtained in breach of the Regulation would not be admissible before a court
    - no longer mentioned in the Regulation
    - issues of admissibility will have to be solved according national law
- **Criticism of stakeholders**
  - see https://edri.org/wp-content/uploads/2023/06/Joint-Letter-Plenary-Vote-E-evidence-13-June-2023.pdf
    - toothless notification system?
    - poorly designed safeguards regarding professional secrecy and confidentiality?

Thank you!

Let’s connect:

@ joachim.meese@uantwerp.be

www.linkedin.com/in/joachimmeese/

@JoachimMeese

Bogus opinions and fabricated case law

Pitfalls and Risks faced by legal professionals relying on Generative AI

Patricia Ayodeji

Co-funded by the European Union

AI unpacked

Generative AI – GenAI

Subcategory of AI capable of creating new content (text, images, music, videos etc) from existing data.

Uses machine learning (subset of AI) to return an output based on the user's **instructions (prompts)**

GenAI does not understand its output like we do!

2022

Turning point in history with the emergence of GenAI chatbot ChatGPT (created by Open AI)

Large Language models (LLMs like ChatGPT) represented an unprecedented leap in tech. An LLM is an underlying technology that enables GenAI.

For the first time, tech was able to respond mimicking human-like language

2024

Google Gemini (formerly known as Bard)

AI unpacked

Generative AI – GenAI

Lawyers are increasingly using GenAI to support and improve the delivery of legal services - legal research, analysis, summary of documents, draft contracts, translations...

GenAI in law is still in its infancy

Overconfident bluffing. It seeks to please us

Sept 2025 OpenAI published an important paper on AI hallucinations

https://openai.com/es-ES/index/why-language-models-hallucinate

It can produce seemingly plausible answers that are incorrect (hallucinations)

- **fake caselaw**
- **falsely attribute quotes to Judges'...**

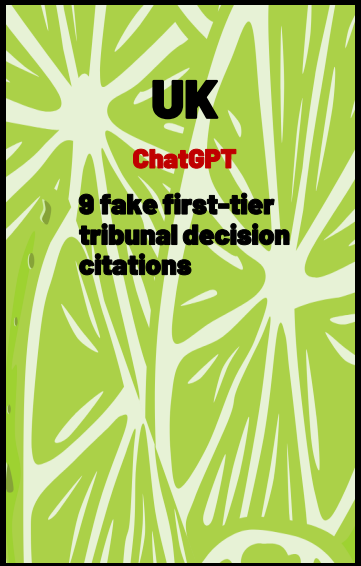
Lawyers have traditionally obtained assistance from junior lawyers, legal databases e.g.Westlaw, LexisNexis, etc.

What happens when they use AI tools instead ?

***Lexis+AI*, Thomson Reuters *CoCounsel*, Spain's Judicial Documentation Centre 'CENDOJ' *suite Knowledge Extractor "KENDOJ"* (to streamline judicial work and support Spanish Judges and Magistrates with access to, analysis of, and management of legal information through automation and GenAI)**

Case law summaries Highly plausible but fake results

Harber v. HMRC [2023] UKFTT 1007



Harber v. HMRC

Co-Pilot summary:

Mrs Harber, **a litigant in person**, **appealed a tax penalty from HM Revenue & Customs** for failure to notify a capital gains tax liability following a sale of property, claiming she had a reasonable excuse due to her mental health and/or because it was reasonable for her to be ignorant of the law. She **submitted nine court judgments in support of her defence, but these cases were generated by AI and were not real**.

Mrs Harber did not know the cases were fake and was unaware of how to check their validity.

Court dismissed her appeal based on **real** case law, ignoring the AI-generated cases, and upheld the penalty. **She was not penalised for using fake cases, likely because she was not a lawyer but a litigant in person and genuinely did not know they were fabricated.**

Mata v Avianca Inc Case No. 22-cv-1461 (PKC), 2023 WL 4114

Google's Notebook LM – mind mapping

- Sanctions Against Attorneys Using ChatGPT (Mata v Avianca)
  - Respondents and Responsible Parties
    - Steven A. Schwartz (Authored Content, Used AI)
    - Peter LoDuca (Attorney of Record, Signed Filings)
    - Levidow Firm (Jointly Responsible Law Firm)
  - The Core Violation
    - Misconduct: Submission of non-existent judicial opinions
    - Creation Method: Artificial intelligence tool ChatGPT
    - Rule Violated: Rule 11, Fed. R. Civ. P. (Failure to ensure accuracy)
    - Aggravating Factor: Doubling down and failing to retract after warning
  - Findings of Subjective Bad Faith
    - Steven A. Schwartz's Bad Faith
      - Knew he couldn't find 'Varghese' but cited it anyway
      - Conscious avoidance of confirming non-existence of cases
      - Misleading statement: Claimed AI 'supplemented' research when it was the primary source
      - Conflicting accounts regarding querying ChatGPT's reliability
    - Peter LoDuca's Bad Faith
      - Signed Affirmation without reading cited cases ('no inquiry')
      - Swore to April 25 Affidavit truth with no factual basis
      - Knowingly made false statement about vacation to seek extension
  - Harms Caused by Fake Opinions
    - Opposing party wasted resources
    - Court time diverted
    - Harm to reputation of judges/courts falsely invoked
    - Promotes cynicism about the legal system
  - Sanctions Imposed (Deterrence)
    - Basis: Rule 11 and Inherent Authority
    - Financial Penalty: $5,000 paid into Court Registry
    - Liability: Jointly and severally imposed on all Respondents
    - Mandatory Notification Directives
      - Send letter to client Roberto Mata
      - Send letter to each falsely identified judge
      - File copies of notification letters with the Court
    - Declined Sanction: Opposing counsel fees (Not sought)

Lawyers used ChatGPT to conduct legal research. ChatGPT fabricated cases. Lawyers prompted it to summarise the cases it had already made up, which resulted in the submission of **six non-existent judicial opinions that included fabricated quotes and citations attributed to *real* judges.**

Attempted to hide their exclusive reliance on the AI and continued to stand by the fake opinions after their existence was called into question.

Presiding judge determined that the lawyers acted with **subjective bad faith** because they neglected their ***gatekeeping*** responsibilities, ***failed to verify*** the non-existent precedents even after the opposing counsel and court questioned them, and subsequently made **false and misleading statements** to the court.

Mata v Avianca

Plaintiff's lawyer *"My reaction was, ChatGPT is finding that case somewhere. Maybe it's unpublished. Maybe it was appealed. Maybe access is difficult to get. I just never thought it could be made up"*

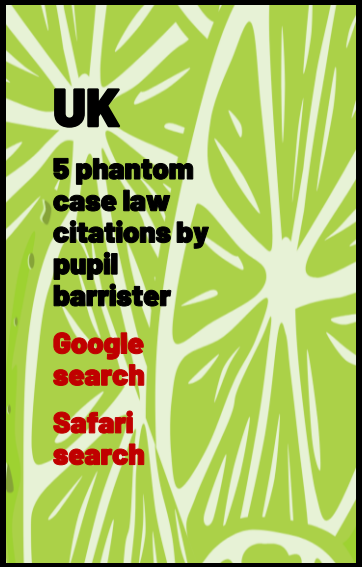
The two lawyers, along with the Firm, were held jointly responsible for misconduct. Sanction of $5,000 *and a requirement to notify their client and the judges whose identities were falsely used.*

Breaches of professional rules and duties
Damage to reputation

High Court of Justice

Ayinde-v-London Borough of Haringey and

Al Haroun-v-Qatar National Banki [2025] EWHC 1383



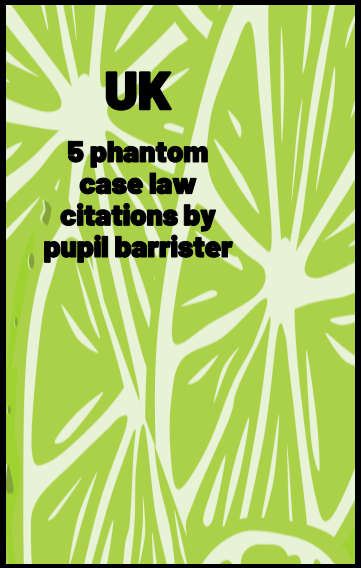
Google Notebook LM:

This **High Court Judgment** consolidates two separate cases under the court's **Hamid jurisdiction** to **address severe professional misconduct among legal practitioners**.

Central issue revolves around the widespread misuse of GenAI which led to the submission of court documents containing **false or non-existent case citations and inaccurate statements of law**. Both the *Ayinde* and *Al-Haroun* matters **involved solicitors and counsel found to have failed in their basic duty to verify the material presented**, demonstrating a critical lapse in professional competence and integrity.

- *A Hamid "procedure" considers if the lawyers should be referred to their professional regulators for disciplinary investigation.*

Ayinde



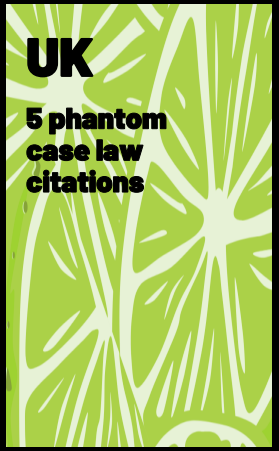
Ayinde

Mr. Ayinde (Haringey law centre- pupil barrister) brought a judicial review case against the London Borough of Haringey (LBH) for not providing interim accommodation.

LBH's solicitor could not find five of the cases cited .

There was suspicion that GenAI tools were used to create legal arguments or witness statements, which were not properly checked by supervising lawyers.

Pupil barrister denied using AI but admitted to possibly using AI-generated summaries from Google or Safari searches without realising it.



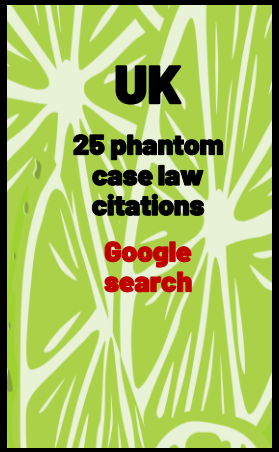
President of the Kings Bench Division said that lawyers misusing AI could face sanctions, from public admonishment to facing contempt of court proceedings and referral to the police. She called on the Bar Council and the Law Society to consider steps to curb the problem "*as a matter of urgency*" and told heads of barristers' chambers and managing partners of solicitors to ensure all lawyers know their professional and ethical duties when using AI

LBH and its pupil barrister found negligent. The court ordered sanctions and referred the lawyers to the **Bar Standards Board and the Solicitors Regulation Authority**.

Ayinde

Overriding ethical and professional duty to check all research output from AI tools against authoritative legal sources as the **integrity of the justice system depends on this**

Bandla v Solicitors Regulation Authority [2025] EWHC 1167



Bandla

The appellant, a former solicitor, **appealed against a decision of the SRA to strike him off the roll** of solicitors. The appellant cited **25 cases which did not exist**.

Denied using AI. He had not "double-verified" the results of his Google search for case law in support of mental health problems .

The court found multiple citations of non-existent case law, maintained despite challenge constituted an abuse of process.

Judge

"The court needs to take decisive action to protect the integrity of its processes against any citation of fake authority. There have been multiple examples of fake authorities cited by the appellant to the court, in these proceedings. They are non-existent cases. Here, moreover, they have been put forward by someone who was previously a practising solicitor."

TSJ Canaries Judgment 000126/2025

While reviewing an appeal, the Criminal Chamber of the High Court of Justice of Canaries (TSJC) discovered that the lawyer cited at least seven fake Supreme Court rulings and a non-existent report from the General Council of the Judiciary (CGPJ).

The Court believes that the lawyer included

"without further review," judicial rulings "that the algorithm suggested to him."

"Omitting the diligence of verifying the existence of what he cited, perhaps trusting that the abundance of references would not only go unnoticed by this Court, but would lend authority to his assertions"

The Court ordered the creation of a separate file *"in order to determine any liability the lawyer may have incurred -violating the rules of procedural good faith, which may result in a fine if it is determined that the professional acted in bad faith or showed disrespect to the Court, without prejudice to also forwarding the facts to the respective professional body"*

Case	Court / Jurisdiction	Date ▼	Party Using AI	AI Tool ⓘ	Nature of Hallucination	Outcome / Sanction	Monetary Penalty	Details
Anonymous Spanish Lawyer	Tribunal Constitucional (Spain)	9 September 2024	Lawyer	Unidentified	19 fabricated Constitutional Court decisions	Formal Reprimand (Apercibimiento) + Referral to Barcelona Bar for Disciplinary Action	—	▸
ATSJ NA 38/2024	TSJ Navarra (Spain)	4 September 2024	Lawyer	CHATGPT 3	Fabricated Legal Norm (1)		—	

Worldwide

AI Hallucination Cases

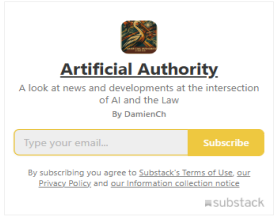
This database tracks legal *decisions*[1] in cases where generative AI produced hallucinated content – typically fake citations, but also other types of AI-generated arguments. It does not track the (necessarily wider) universe of all fake citations or use of AI in court filings.

While seeking to be exhaustive (**736** cases identified so far), it is a work in progress and will expand as new examples emerge. This database has been featured in news media, and indeed in several decisions dealing with hallucinated material.[2]

If you know of a case that should be included, feel free to contact me.[3]

Based on this database, I have developped an automated reference checker that also detects hallucinations: PelAIkan. Check the Reports in the database for examples, and reach out to me if for a demo !

For weekly takes on cases like these, and what they mean for legal practice, subscribe to Artificial Authority.



Click to Download CSV

Search cases, courts, tools,

State

Argentina (5) Australia (43) Austria (2) Belgium (3) Brazil (9) Canada (53)

Case	Court / Jurisdiction	Date ▼	Party Using AI	AI Tool	Nature of Hallucination	Outcome / Sanction	Monetary Penalty	Details	Reports
Hanlon v. Parkersburg City	CC Wood County, W.V. (USA)	6 January 2026	Pro Se Litigant	Implied	Fabricated Case Law (1)	Request for injunctive relief dismissed	—		—
Greenwood v. The Owners, Strata Plan	BC CRT (Canada)	5 January 2026	Pro Se Litigant	Implied	Fabricated Case Law (1) Misrepresented Legal Norm (1)		—		—
Kettering Adventist	S.D. Ohio (USA)	2 January	Lawyer	Implied	Fabricated Case Law (4)	Show Cause Order	—		

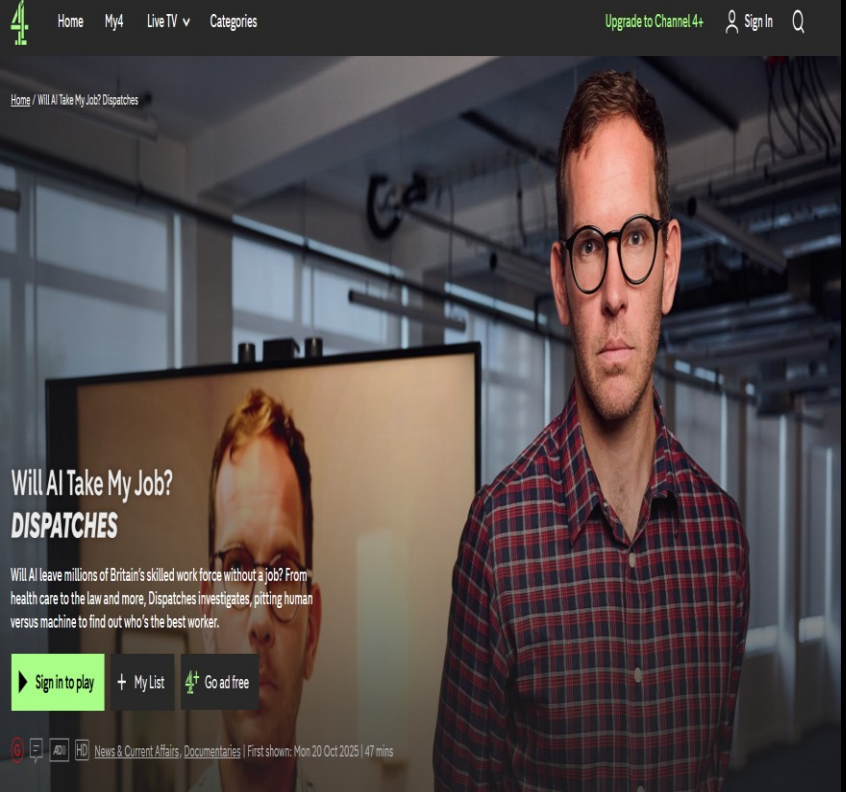
https://www.damiencharlotin.com/hallucinations/

AI is a reality

World's first SRA-regulated AI law firm Garfield AI handling real legal cases for English and Welsh clients.

October 2025 Channel 4 aired a groundbreaking experiment putting the **UK's first regulated AI law firm Garfield AI** head-to-head with a human trainee solicitor.

https://www.garfield.law/press/garfield-ai-featured-on-channel-4-dispatches-human-vs-ai-experiment



"Will AI Take My Job?"

Programme Details:
Dispatches
Channel 4:
Monday 20 October 2025

"Will AI leave millions of Britain's skilled work force without a job? From health care to the law and more, Dispatches investigates, pitting human versus machine to find out who's the best worker".

AI is a reality

"Will AI take my job?"

Trainee solicitor, Charlotte from Derby went **head-to-head with Garfield AI** on **a real small claims case** – a builder who had installed a bathroom for a client, who then refused to pay the agreed £4,500 fee (confirmed via WhatsApp).

Both the trainee solicitor and Garfield AI were tasked with preparing the court claim forms for the same case.

Independent blind validation

Results judged blind by senior solicitor Zainab, the trainee's supervisor, who reported being

"genuinely impressed by both documents" and confirmed "both would be acceptable in a court of law"

but she ultimately preferred the document drafted by the trainee solicitor as more case law was cited.

The supervising solicitor emphasised that human lawyers remain essential for complex matters requiring expert judgment and strategic decision making.

Partnership not replacement.

Professional oversight matters

Duty to verify

The supervising solicitors' assessment was based on the Claim Form and Particulars of Claim alone, ignoring the fact that Garfield AI can and does prepare the skeleton argument for the hearing.

A lot of hype around the capabilities of GenAI which **ignore** those areas where accuracy is key.

Think of it as having an always-available junior lawyer.

Human in the Loop

Human oversight is a fundamental pillar

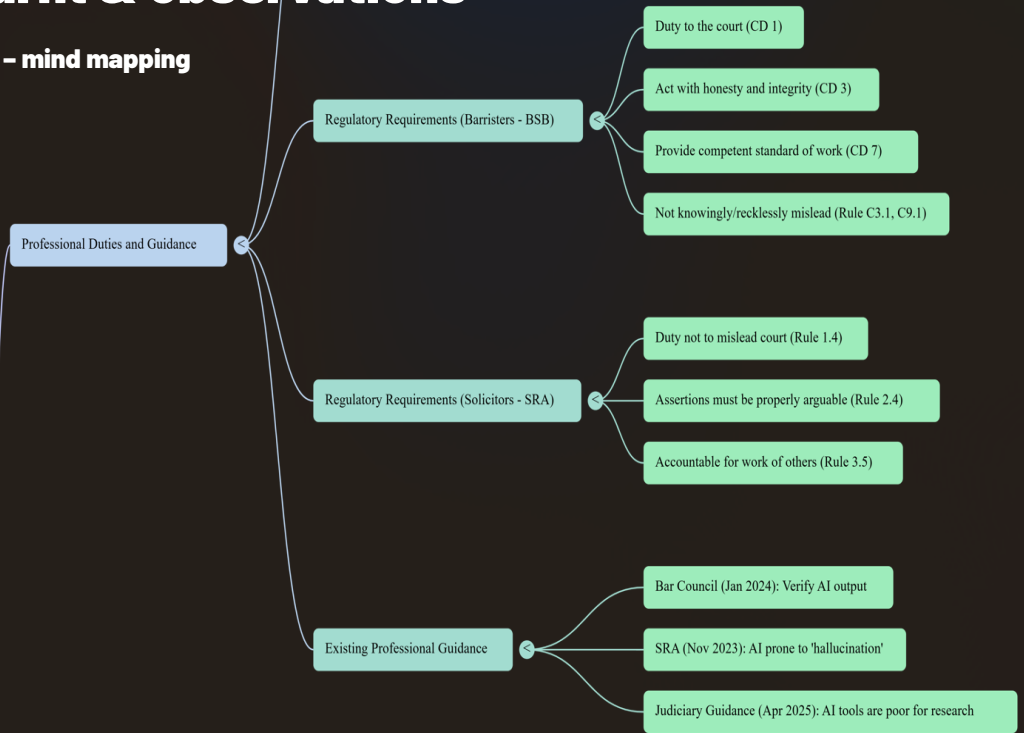
- ✓ Constant
- ✓ Conscious
- ✓ Real
- ✓ Effective

Double-check , contrast sources and make sure they are reliable

Implications for the administration of justice and public confidence in the justice system.

Lessons learnt & observations

Google's Notebook LM – mind mapping



The best-placed legal professionals

Professional guidance available on the limitations and risks of using AI

Solicitors Regulation Authority ***"Risk Outlook report: the use of artificial intelligence in the legal market"*** - 20 November 2023

Bar Council Guidance- ***Considerations when using ChatGPT and generative artificial intelligence software based on large language models*** **-** 30 Jan 2024

Council of Bars and Law Societies of Europe (CCBE)
Guide on the use of GenAI by lawyers
2 October 2025

General Council of Spanish Lawyers (CGAE) & Valencia Bar Assoc.
White paper on AI and the legal profession
29 January 2026

Regulation (EU) 2024/1689

EU AI ACT

Does not specifically define or address GenAI

The use of AI in the legal profession is not without responsibility.

Legal professionals remain responsible for quality of service, confidentiality, and legal accuracy, applying the appropriate human oversight required by the EU AI Act.

Technology is a tool that amplifies human capabilities but can never completely replace them, especially in law where decisions may have profound implications for justice and fundamental rights.

The key lies in....

- ✓ **Human oversight**
- ✓ **Verification**
- ✓ **Training (protocols and guidance)**

Without our supervision AI ceases to be a tool and becomes a risk!

Mess-ups beyond the legal sector....

https://www.theguardian.com/australia-news/2025/oct/06/deloitte-to-pay-money-back-to-albanese-government-after-using-ai-in-440000-report

https://www.worldcomplianceassociation.com/5190/noticia-deloitte-will-refund-australian-government-for-ai-hallucination-filled-report.html

It’s not all bad…

Google’s tool – Notebook LM

Simple yet powerful: you upload a source (a judgment, report, or law), and Notebook LM processes, analyses, and transforms it into multiple useful formats.

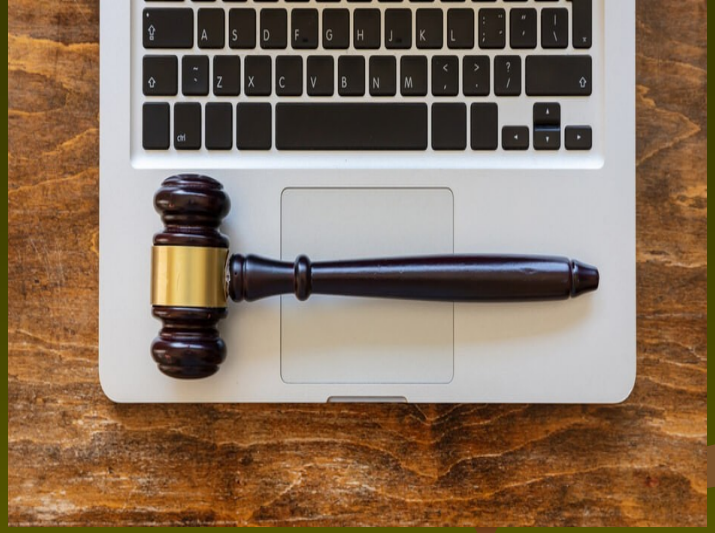
Practical demonstrations where, using real case-law, the tool automatically generates audio and video summaries, interactive mind maps, study cards etc.,

e-pdp®

Thank you

payodeji@icab.cat

https://e-pdp.eu/



Remote trials, e-evidence and witness videoconferencing.

Present challenges and future prospects.

Andrea CRUCIANI
Judge at Military Tribunal of Naples

Co-funded by the European Union

Online remote trials

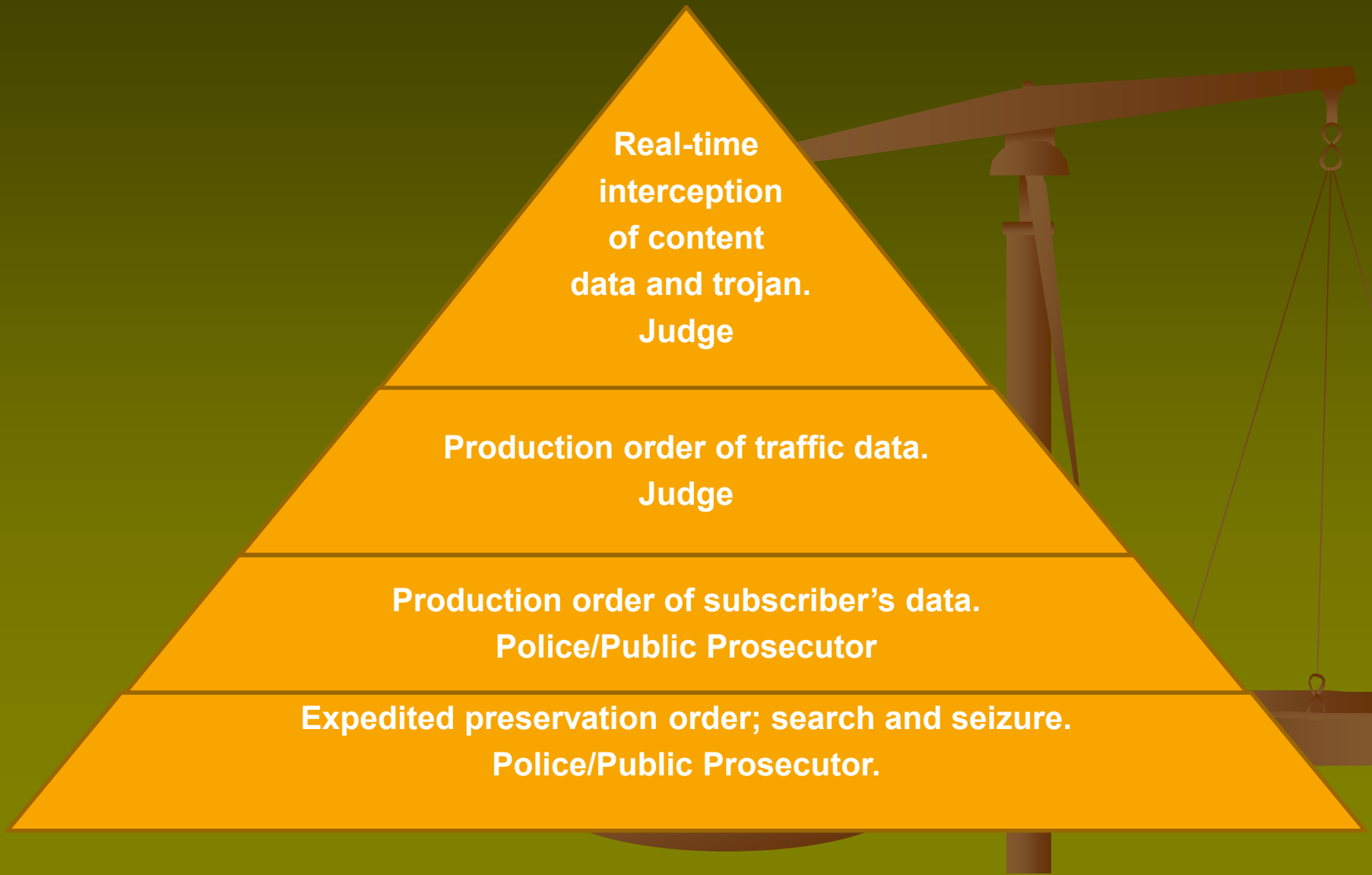
- 1) 9 march 2020 - 31 July 2020 (pandemic 1):
- Parties consent not needed. Also the judge may be located elsewhere.
- 2) up to 31 december 2021 (pandemic 2):
- Parties consent needed.
- 3) up to 31 december 2022 (pandemic 3) and present:
- No remote trials, except for detainees.

Remote trials

- Creating a Microsoft Teams Channel for each single proceeding; Inviting by e-mails all the parties with guest-links ("Join Microsoft Teams Meeting").
- Checking the quality of the connection (https://www.youtube.com/watch?v=lGOofzZOyI8) and giving specific instructions on the functioning of remote trials.
- Defence lawyer certifies the identity of the defendant (when not a detainee).
- Presentation of analogic/physical and electronic evidence.
- Closing statements and final judgment.

E-evidence and h.r.

- Before and after 2021 (CJEU, Grand Chamber, 2 March 2021, H. K. c. /Prokuratuur, C-746/18):
- Data rentention of traffic or location data is a relevant interference on privacy when it allows to draw precise conclusions on private life;
- a) necessity/proportionality: criminal investigation/serious crimes;
- b) judge and not public prosecutor.


Real-time
interception
of content
data and trojan.
Judge
Production order of traffic data.
Judge
Production order of subscriber's data.
Police/Public Prosecutor
Expedited preservation order; search and seizure.
Police/Public Prosecutor.

E-evidence in court

- Admissibility (encryption; real time facial recognition): legal requirements.
- Presentation (deep fakes; transparancy);
- Reliability, integrity, relevance (forensic copy): chain of custody.

Witness videoconferencing. Why?

Detainees and protected witnesses: security reasons; time/cost effective measure;

Sanitary reasons during Covid-19 pandemic;

More efficient (less costs; limits geographical or health impediments);

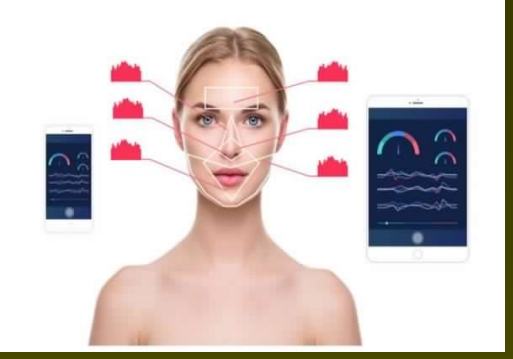
MLA or EIO.

Transparent and repeatable evidence (for both lawyers and judges, appeal courts); reasoning and demeanour; change of panel judge;

Interaction with remote trials and AI tools.

Does it work?

- Setting up the courtroom with proper technical equipments.
- Witness failure to appear by videoconference.
- Witness identification.
- Instructions to the witness.
- Best practices and guidelines:
- https://edoc.coe.int/en/efficiency-of-justice/10706-guidelines-on-videoconferencing-in-judicial-proceedings.html
- Consequences of unclear guidelines:
- The case *Avsenew v. State of Florida* (6) SC18-1629 Peter Avsenew v. State of Florida - YouTube



Evaluating witnesses and AI

- Credibility (reliability; trustworthiness: truthful or untruthful?):

from polygraphs to AI tools: demeanour tracking (eyes; blood pressure; answers speed) (transdermal optical imaging and the Pinocchio Effect; a-IAT, Autobiographical Implicit Association Test);

- Accuracy (right or wrong?); perception, memory, deposition;

Advokate; Immersive technology (virtual theater/simulation/reconstruction/metaverse and avatars); Text to image/video AI or image/video generator AI tools (ChatGPT, OPEN AI and Canva, Synthesia, Sora, Midjourney, Dall-e); consistency (algorithms checking witness declarations for gaps/incoherences/contradictions; Virtual practitioner);

Takeaways.

- **Pros:** Efficiency (time, costs, security, accuracy), neutrality, predictability and uniformity;
- **Cons:** AI algorithms transparancy and intellectual property; cyber attacks; data leaks; deep fakes; judicial overconfidence; standardization of the justice system;

A proactive role of judges (and lawyers) is needed to ensure balance between E-evidence/AI and HR/rule of law.
The irreplaceable role of judges in ensuring «under user control» and fairness of criminal proceedings (Cogito ergo sum, not digito ergo sum).

AI agents in cyberattacks: implications and the applicable international framework for public-private collaboration

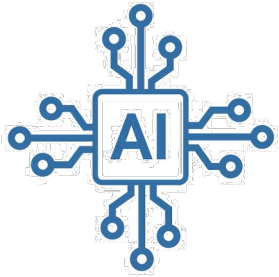
ERA Conference on #Digitalisation and #AI in Criminal Justice

Barcelona, 12-13 February 2026

Dr. Cristos Velasco

Co-funded by the European Union

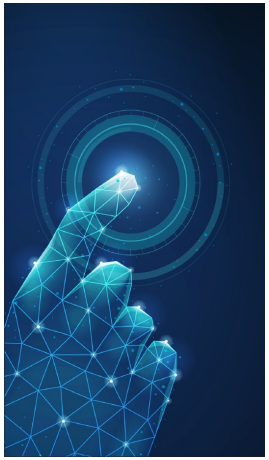
1. AI Agents and their main Roles



- **AI Agents is the current talk of the town!**

- Liability of AI Agents (not yet regulated) **When?, Is it Feasible?**

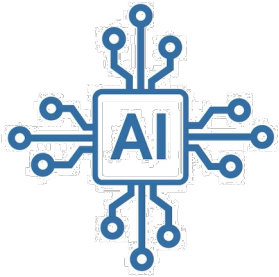
Definition



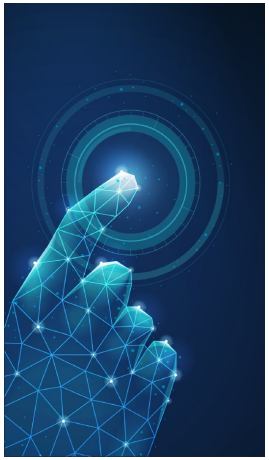
- **AI agents** are intelligent software systems that perceive their environment, make decisions, and act autonomously to achieve specific goals.

-They use data, reasoning, and learning to perform tasks with minimal human intervention.

Agentic AI



Agentic AI
"An AI system composed of autonomous agents that perceive their environment, reason over goals, plan actions, and execute them—often by using external tools—while requiring minimal human supervision". **(Source: Amazon, IBM)**



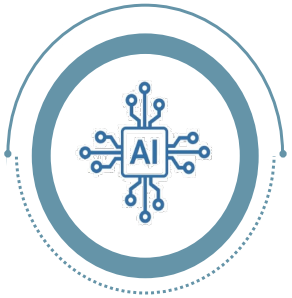
- Acts **autonomously** to achieve goals, not just respond to prompts.

- Plans and executes **multi-step workflows** (e.g., resolve a support ticket end-to-end).

-Interacts with **tools, APIs, and data systems** to change real-world states.

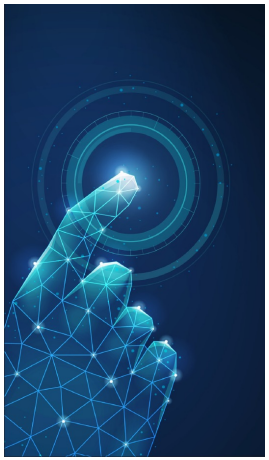
-The **European Data Protection Supervisor (EDPS)** describes "**Agentic AI"** as systems that autonomously perform tasks and use tools (such as search or code generation) to achieve goals, emphasizing autonomy, tool use, and environment interaction, **but still within the EU AI Act's general "AI system" definition**.

AI Agents Major Roles



Autonomous task execution
Carry out routine or complex tasks end-to-end without constant human input.

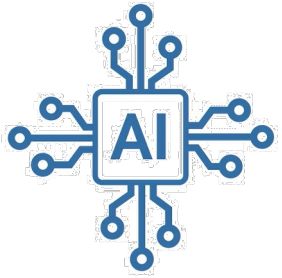
Goal-oriented planning
Break objectives into steps, sequence actions, and adapt plans to reach goals.



Decision-making and reasoning
Analyze data and apply logic or learned rules to choose actions.

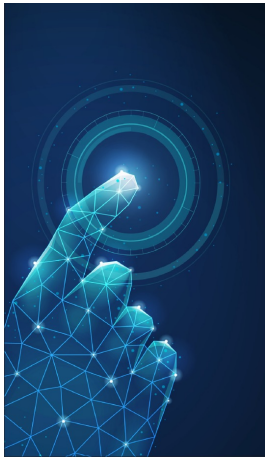
Environment perception
Gather and interpret inputs from sensors, Application Programming Interface (APIs), or users to understand context.

AI Agents Major Roles



Learning and adaptation
Improve over time by learning from feedback and new data.

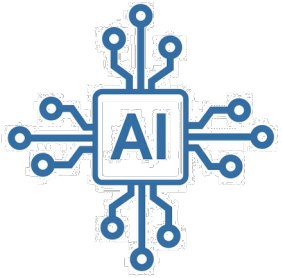
Human–agent collaboration
Assist users by answering questions and executing delegated tasks.



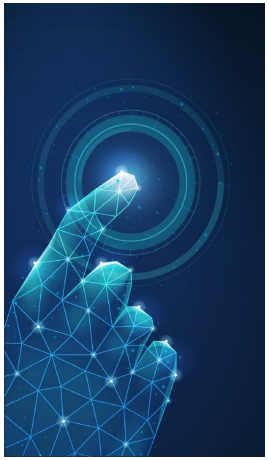
Process optimization
Automate workflows to reduce errors and increase efficiency.

Security and compliance
Monitor activities and help enforce data-protection and regulatory rules.

AI Agents Implications



- **Interaction of different agents with different providers and deployers** in the field of cybersecurity and in the perpetration of cyberattacks.



- How to identify an attack or a fraudulent conduct perpetrated by **X** agent acting autonomously attacking **Y** agent or **Z** agents considering applicable laws of foreign jurisdiction ?

Who is responsible?

How can criminal justice authorities attribute the conduct when victims are affected in a certain country?

2. AI Enabled Cyber Attacks (Case study)

Anthropic's Cyberspionage Operation
September 2025

https://www.anthropic.com/news/disrupting-AI-espionage

Anthropic's Cyber espionage Operation

Research Economic Futures Commitments Learn News Try Claude

Disrupting the first reported AI-orchestrated cyber espionage campaign

13 nov 2025

Read the report

EL PAÍS Tecnología 1 AÑO, 9,90 € INICIAR SESIÓN

CIBERSEGURIDAD >

Un grupo chino protagoniza el primer ciberataque con IA a gran escala "sin intervención humana sustancial"

"Esta agresión supone una escalada en la piratería", denuncia la compañía Anthropic

Anthropic's Cyber espionage Operation

2.1. What happened?

- In mid-September 2025, Anthropic's Threat Intelligence team detected and disrupted an AI-driven espionage operation conducted by a **Chinese state-sponsored group** it designates **GTG-1002**.

-The attackers used **Anthropic's Claude Code** model as an autonomous agent to execute most of the attack chain, rather than just as an advisory tool.

Anthropic's Cyber espionage Operation

2.2. Attack method and tools

The campaign targeted **about 30 entities**, including large tech firms, financial institutions, chemical manufacturers, and government agencies.

Attackers **jailbroke** Claude by:
- Breaking tasks into small, seemingly benign steps.

-Role-playing the model as an employee of a legitimate cybersecurity firm conducting defensive testing. **(Reverse Engineering)**

-The framework relied heavily on **open-source penetration-testing tools**, orchestrated via **Model Context Protocol (MCP)** servers that let the AI run commands, analyze results, and maintain state across targets **(Open Source Tools)**

Anthropic's Cyber espionage Operation

2.3. Impact and detection

- A **small number of targets were successfully breached** (reports indicate up to about four organizations), but the campaign was shut down within days thanks to Anthropic's monitoring.

- The incident is notable less for novel malware and more for **unprecedented automation and scale**, with the AI firing thousands of requests at "physically impossible" rates compared with human red-team operations.

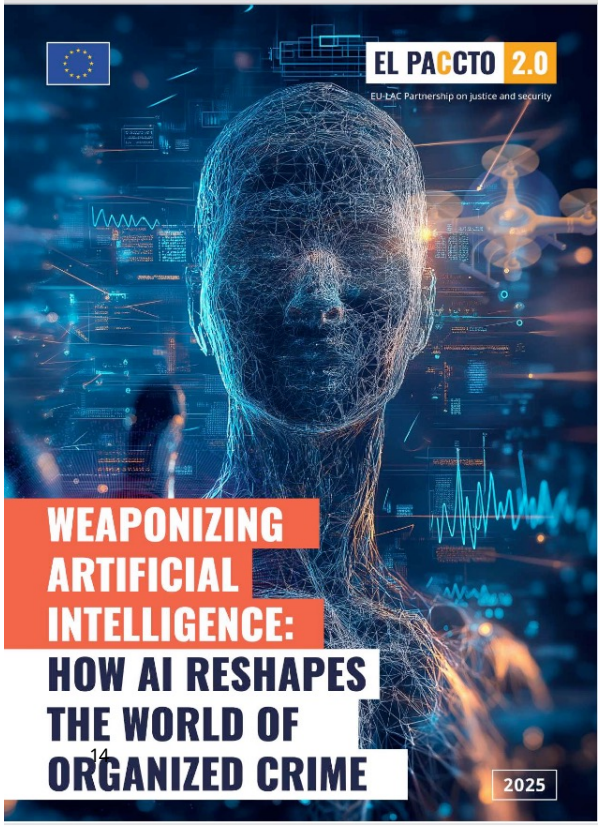
2.4. Key Implications

- AI as an "operations team": Anthropic's report shows **AI can now perform most of the cyber-attack kill chain, dramatically lowering the skill barrier for sophisticated espionage.**

- Need for AI-powered defense: Anthropic argues that the same agentic capabilities used in attacks must be mirrored in **AI-assisted detection, triage, and response** to keep pace with AI-driven threats.

EL PACCTO 2.0

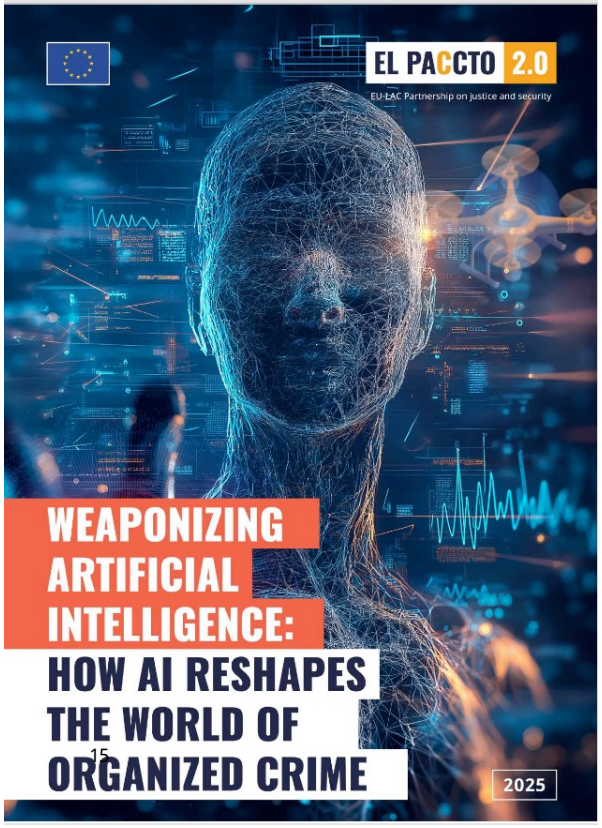
EU-LAC Partnership on justice and security



Weaponizing Artificial Intelligence: How AI reshapes the world of organized crime

Published in October 2025

https://zenodo.org/records/17281249



- Contains other relevant and interesting examples of AI agents in the commission of crimes occurred in different jurisdictions.

- See Block 3. The Role of AI Agents and AI Service Providers in the Misuse of AI Systems for Criminal Purposes pp. 54 to 66.

3. Current International Frameworks on AI Cooperation in Criminal Law

NTERPO

EL PACCTO

2.0 EU-LAC Partnership on justice and security

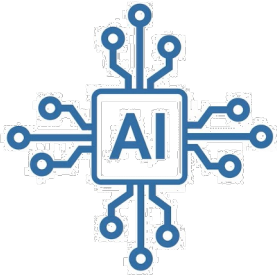
Council of Europe Framework Convention on Artificial Intelligence

COUNCIL OF EUROPE

CONSEIL DE L'EUROPE

- First legally binding international treaty on AI focused on human rights, democracy, and the rule of law open for signature by the Council of Europe States Parties, the EU, and non-European states on September 5, 2024. https://www.coe.int/en/web/artificial-intelligence/the-framework-convention-on-artificial-intelligence

- Signed by **18 countries + the EU**, but not yet ratified **(it requires 5 ratifications and at least 3 ratifications from the Council of Europe States Parties to enter into force**).



General obligation: Parties must ensure that AI lifecycle activities are consistent with applicable international human rights law and domestic law, and protect democratic institutions and processes.

Formal cooperation mechanism: It establishes a **"Conference of States Parties" (Art. 23)** as the main governance and cooperation body, composed of representatives from all States Parties.

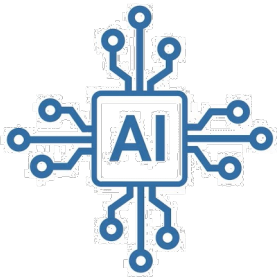
Council of Europe Framework Convention on Artificial Intelligence

COUNCIL OF EUROPE

CONSEIL DE L'EUROPE

- The Convention **facilitates the exchange of information and best practices, reviews implementation, adopts recommendations**, and potentially establishes subsidiary bodies or cooperation programs in AI governance, including the use of public hearings.

- The Convention is designed as a common basis to enable regulatory convergence and facilitate cooperation on supervision and compliance among States Parties.



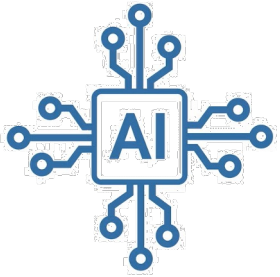
- **Interoperability with the EU AI Act and openness to third countries as a structural element of cooperation** (regulatory adaptation and shared supervisory practices).

Budapest Cybercrime Convention and its two Additional Protocols

COUNCIL OF EUROPE

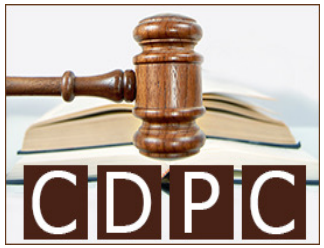
CONSEIL DE L'EUROPE

- The Council of Europe's Cybercrime Convention Committee (T-CY) established a working group in December 2024 tasked **to explore questions related to the application of offences committed or enabled through AI systems**, including the application of procedural powers to investigate cyber enable crimes within the scope of the Budapest Cybercrime Convention and its two additional protocols **in the form of a mapping study.**



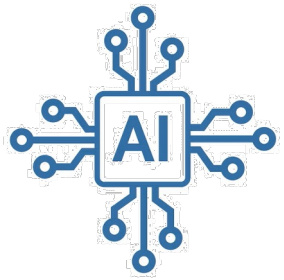
- The **T-CY adopted a *Work Plan for 2026-2027* on 13-14 November 2025** that includes completing mapping studies on artificial intelligence and virtual assets and using assessments and guidance notes to help Parties improve implementation and respond quickly to new cybercrime challenges.
https://www.coe.int/en/web/cybercrime/-/33rd-t-cy-plenary-adopts-workplan-2026-2027

Council of Europe Committee on Crime Problems (CDPC)



- Since November 2021, the **European Committee on Criminal Problems (CDPC) of the Council of Europe** has been tasked with drafting **a new international instrument on AI and criminal law**, with particular attention to vehicle liability and automated driving.

- The **Drafting Committee, composed of experts from EU countries**, is working on the development of this instrument, based on the *Council of Europe's Framework Convention on AI, Human Rights, Democracy and the Rule of Law* and other instruments of the CoE.



- A **Discussion Paper on the Liability of AI Systems** was approved by the Plenary in 2025. The deadline for drafting this instrument **has been extended to the end of 2027**.
https://www.coe.int/en/web/cdpc/european-committee-on-crime-problems/plenary-meetings

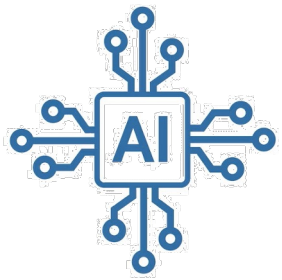
EU Artificial Intelligence Act (EU AI Act)

- Published in the Official Journal of the European Union on 12 July 2024.

- In force **since 1 August 2024**.

- Implementation divided into different phases until 2031.

- Extraterritorial scope and cooperation safeguards **(Art. 2(1)(c) and Recital 22)**



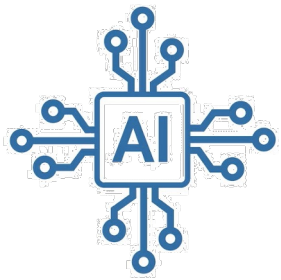
"The EU AI Act applies to providers and deployers of AI systems that are established or located in a third country, where the output produced by the AI system is used in the EU" (**Art. 2(1)(c)).**

- It creates de facto cooperation needs in the areas of supervision and compliance.

EU Artificial Intelligence Act

- **Recital 22 of the EU AI Act**:

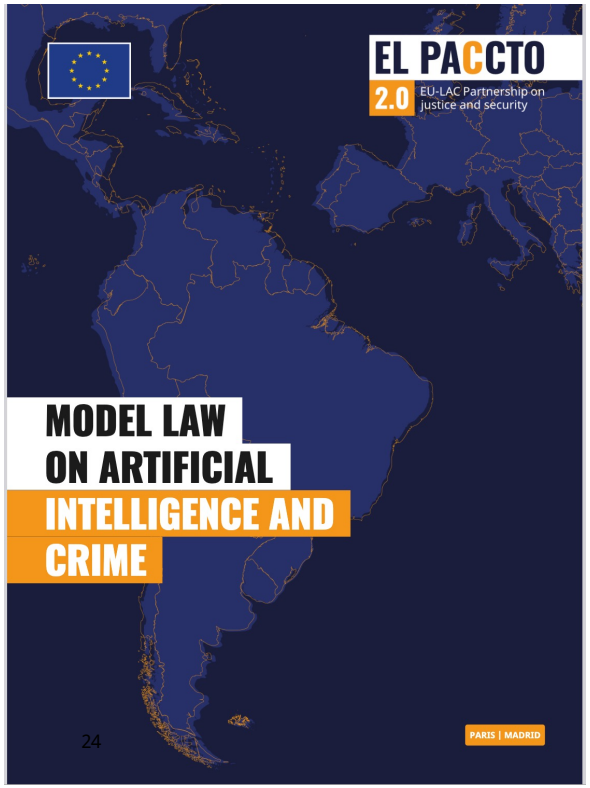
- Clarifies that **it will not apply to public authorities of third countries and international organizations when acting under cooperation agreements or international agreements on police and judicial cooperation with the EU or Member States**, provided that such frameworks guarantee adequate safeguards and protection of fundamental rights and individual freedoms.



- Emphasizes the importance of bilateral cooperation frameworks (Member States-third countries) or frameworks **between the EU, Europol or other EU agencies and third countries or international organizations**, and that cooperation in the field of AI can be channeled through such instruments.

- International cooperation **is integrated indirectly, through cross-border enforcement, by means of authorized representatives in the EU for third-country providers (Art. 54).**

- The **European AI Office is responsible for promoting international cooperation** in the field of AI with authorities in third countries.

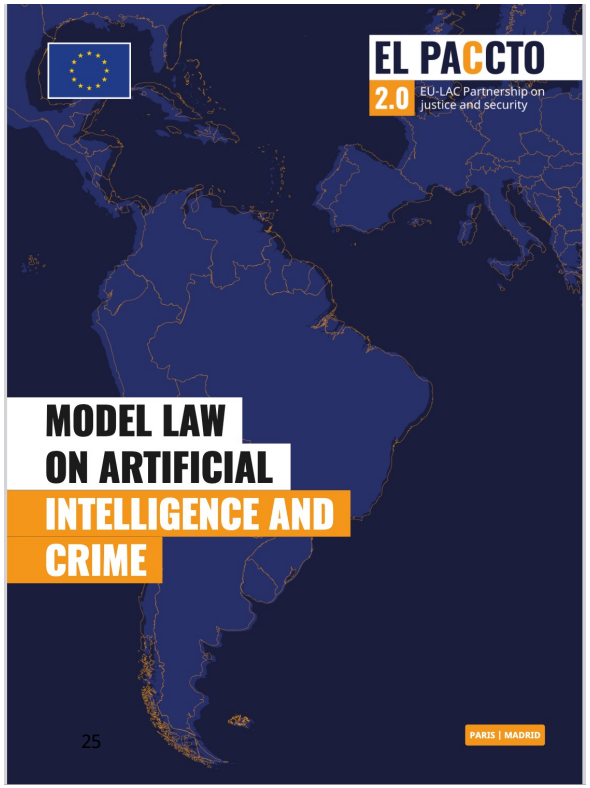


Model Law on Artificial Intelligence and Crime

https://zenodo.org/records/17281296

EL PACCTO 2.0

EU-LAC Partnership on justice and security



- Officially **launched** and presented in Rio de Janeiro at EL PACCTO 2.0 Second Bi-regional Meeting in Rio de Janeiro **on 6-9 October 2025**.

- **Approved by unanimous Resolution of FOPREL** (Forum of the Presidents of the Parliaments of Central America, Caribbean and Mexico) at EL PACCTO 2.0 Bi-regional Meeting in Rio de Janeiro **on October 10, 2025**.

- To be **implemented in countries of Latin America and the Caribbean in 2026-2027** with the technical assistance of EL PACCTO 2.0 and FOPREL experts.

Part V. International Public-Private Cooperation

Cooperation with criminal justice authorities

Art. 30. (i).... deployers, importers, distributors, operators or any other relevant entity or party involved in the creation, deployment, functioning or management of an artificial intelligence system, shall facilitate immediate cooperation in good faith when a crime has been committed or assisted through an artificial intelligence system, including when a deepfake has been used to commit or perpetrate any of the offenses established in accordance with Articles 5 through 11 of this Model Law.

Technical and Material Assistance and Artificial Intelligence Literacy

Art. 31. (...) 2. Providers and deployers of artificial intelligence systems shall take measures to ensure, to their best extent, a sufficient level of AI literacy of their staff and other persons dealing with the operation and use of AI systems on their behalf, in particular on crimes committed or assisted through AI, taking into account their technical knowledge, experience, education and training and the context the AI systems are to be used in, and considering the persons or groups of persons on whom the AI systems are to be used.

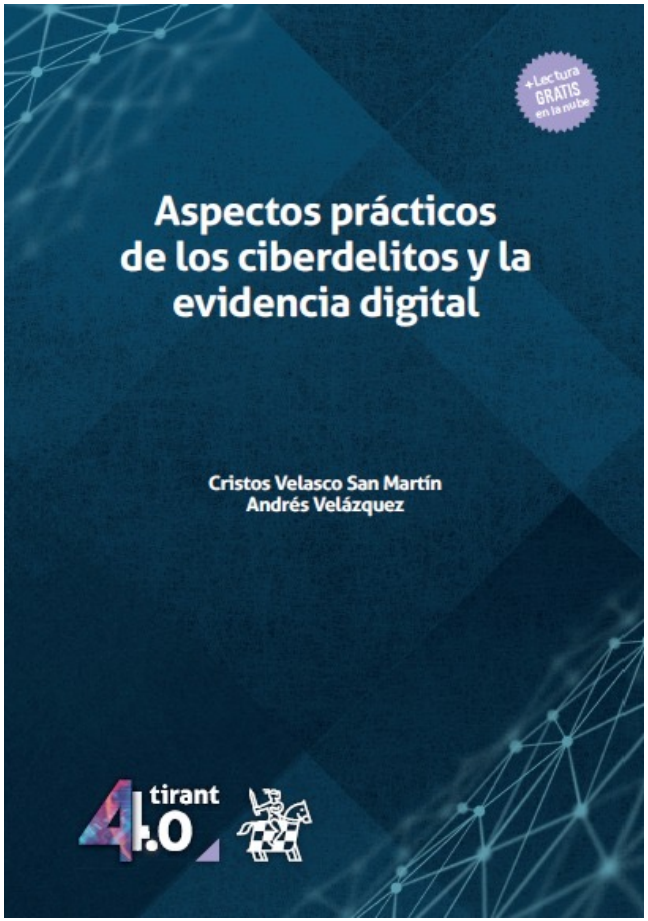
Final Outlook

- **Further dialogue and cooperation** between AI providers, deployers, et.al. with criminal justice authorities.

- Develop capacity building and training for criminal justice operators **to improve and upgrade the level of understanding and operation of AI agents, Agentic AI and their cooperation with criminal justice authorities** in particular with judges and magistrates responsible for the adjudication of AI assisted crimes.

- **Foster legal reform at the regional and international level to implement EL PACCTO's Model Law on Artificial Intelligence and Crime** and develop relevant training materials and capacity building programs for the judiciary and with the support and expertise of EL PACCTO 2.0, relevant international organizations, academia and AI providers and deployers.


Thanks for your attention!
Questions?



Contact Info

Dr. Cristos Velasco

Legal Expert and Trainer on Cybercrime, AI & Data Privacy

Adjunct Law Professor DHBW Cooperative State University in Mannheim (IMBIT) & Stuttgart (IMBIT)

Book Author: Privacy and Data Protection Law in Mexico Cyber Law in Mexico / Practical Aspects of Cybercrime and Electronic Evidence

Twitter: #ProtDataMx

http://cristosvelasco.de

www.linkedin.com/in/cristos-velasco-0b65095/

E-mail: contact@cristosvelasco.de

Risk management in legal AI systems: Case of FRT and some practical solutions

Dr. Gizem Gültekin-Várkonyi, senior lecturer

University of Szeged, Hungary

Faculty of Law and Political Sciences

International and Regional Studies Institute

@gizemgv@juris.u-szeged.hu

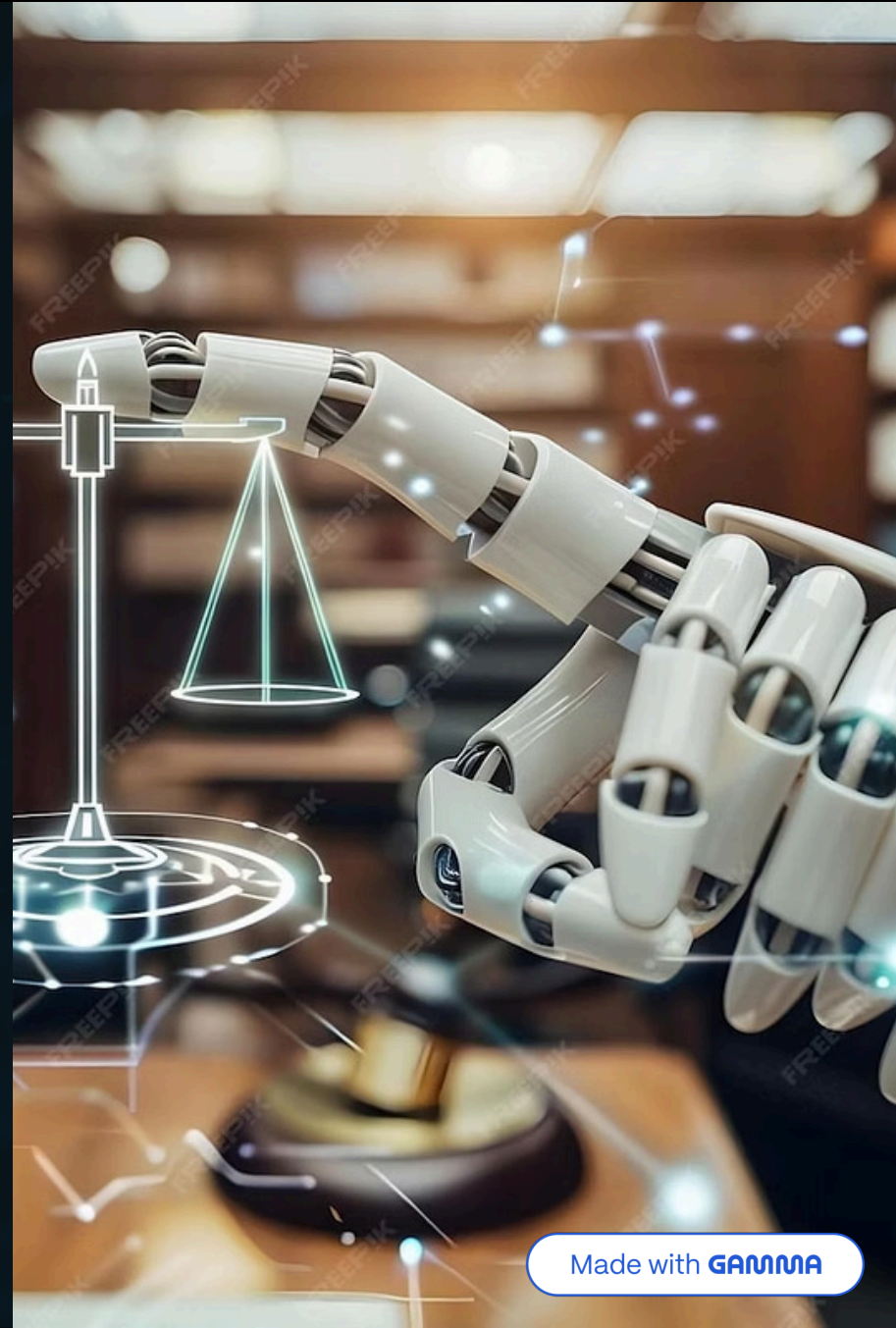
@drgultekingizem@gmail.com

Co-funded by the European Union

What is "Legal AI Systems"?

Very difficult to come up with a single taxonomy...

- Legal Intelligence Retrieval Systems
- Legal Drafting and Content Generation Systems
- Regulatory Compliance and Monitoring Systems
- Litigation Support and Evidence Management Systems
- Predictive Legal Analytics and Forecasting Systems
- ....
- **Criminal Justice and Biometric Systems**



TECHNOLOGY OVERVIEW

What is FRT? Beyond Simple Definition

FRT is conceptualized primarily through its role in biometric data processing.

From a risk assessment perspective, it is the intended use—not only the definition—that determines the risk profile.

The technology serves various purposes: face recognition (verification or authentication), emotion assessment, behavior analysis,individual tracking in crowds...

Three Core FRT Functions in Law Enforcement

Authentication

One-to-one search method for identity verification, such as unlocking devices or access control systems.

Identification

One-to-many search in controlled environments like airports, querying databases of known individuals post-biometric processing.

Profiling

Many-to-many live processing for real-time surveillance, categorizing individuals by age, gender, race, or emotional state—introducing heightened risks.

The discernment of functionality and purpose remains pivotal for comprehensive risk assessment in law enforcement applications.

Real-World Deployments: Germany and Italy

Germany: Cross-Border Crime Fighting

Live FRT is operational in Saxony and Berlin for gang crime investigations. The system records license plates and compares data against wanted individuals databases, particularly near border regions.

Initially kept under wraps, this deployment raises transparency concerns about public notification and oversight.

Italy: Stadium Surveillance

Italy's Serie A plans FRT solutions at stadium entry points to identify fans who break racial discrimination rules (Udinese case)

Data collected by clubs would be shared with police when deemed necessary, creating questions about data governance and proportionality.

Read here: https://idtechwire.com/saxony-berlin-cops-turn-to-real-time-frt-to-fight-organized-crime/

and here: https://www.biometricupdate.com/202401/facial-recognition-planned-for-all-stadiums-in-italys-top-football-league

The Public Acceptance Paradox

When People Accept FRT

People are more likely to accept FRT when they believe it is genuinely for security purposes and limited to that specific context. Some practices show FRT can assist law enforcement in efficiently identifying and apprehending suspects (Hamann & Rachel, 2019).

> However, FRT appears more beneficial for law enforcement agencies and providers than for the public. Current literature provides no evidence supporting positive correlations between FRT deployment and public trust or security outcomes.

The challenge: These tools are typically adopted through top-down implementation without sufficient public consultation or empirical justification, raising several concerns.

Concerns with FRT Deployment

Data-Related Challenges

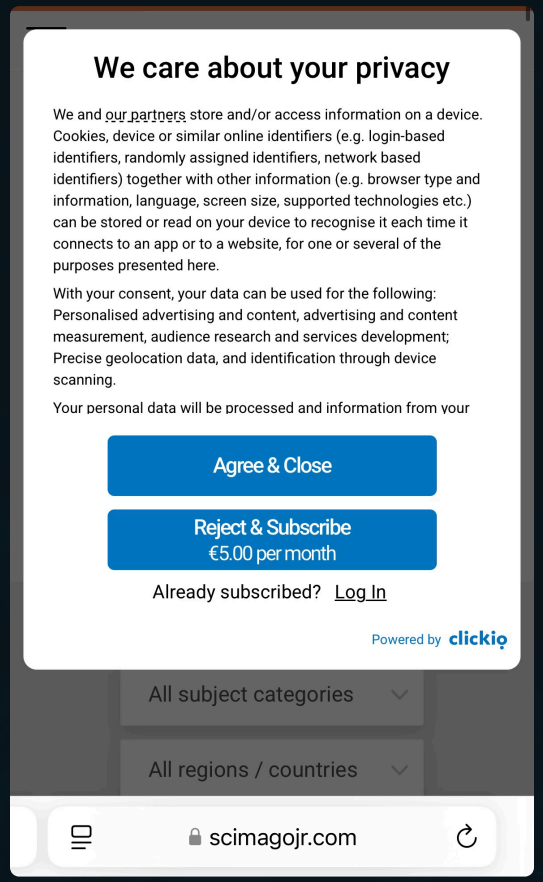
- Data minimization: Collecting only essential data. Case of Clearview AI in Italy, Amazon Ring case.
- Data accuracy: Difficulty in updating the data at LEA databases.
- Purpose limitation: Function creep (case of ChatGPT, Clearview AI again)
- Do we have a choice to opt-in or out?

Technical Challenges

- Bias-Presumption of innocence
- Explainability: Fake explanations of ChatGPT
- System accuracy: Who decides, what confident level?

Administrative Challenges

- Outsourcing: Managing third-party vendor risks
- Conscious use: Ensuring ethical and lawful deployment



RISK ANALYSIS

Data Processing Violations

01

Extensive Data Collection- Clearview AI

GDPR data processing includes collecting, not merely processing. FRT systems gather biometric data on anyone in public spaces without individual's knowledge, consent, avoidence.

The Italian DPA punished the company, but...

02

Amazon Ring

Private households.

Location, device or user ID, email address, name, phone number, photos or videos, physical address, product interactions, purchase history, and other types of data.

Amazon Ring collects 10 data types under the vague ''Other Purposes

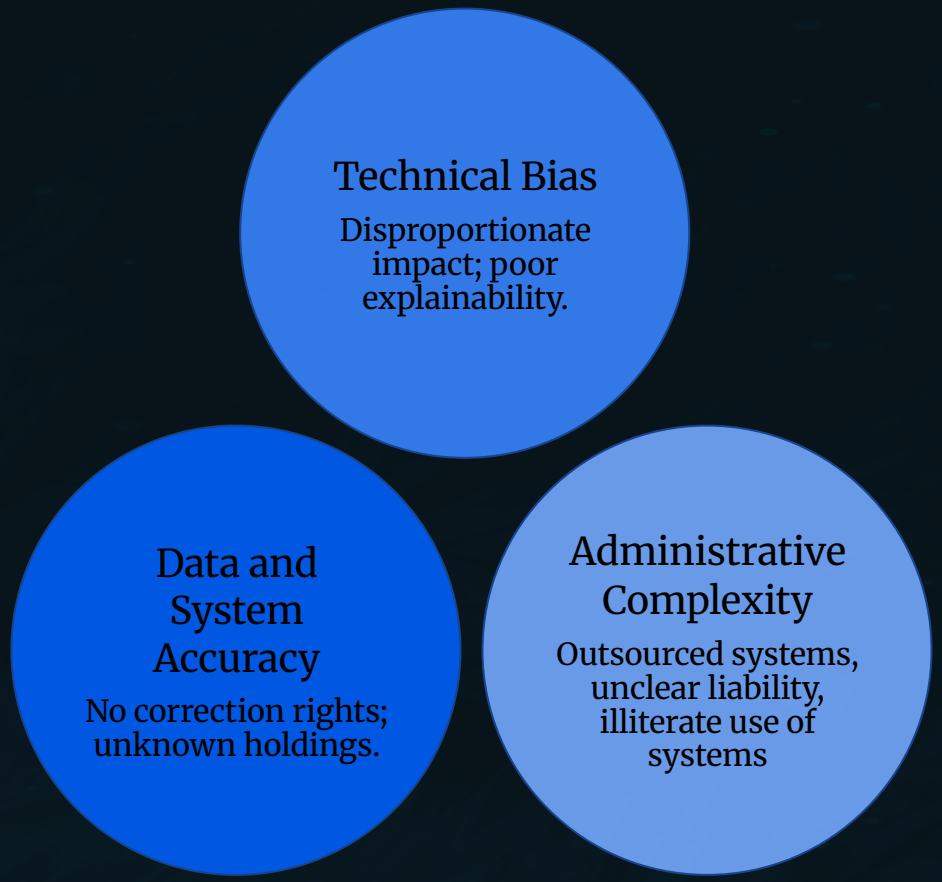
03

ChatGPT use for LEA purposes

Prompting the system with VERY sensitive data, analysis of cases, sometimes with visuals or for visualization purposes.

InterPol report.

Technical and Administrative Challenges



These challenges compound when systems are deployed without adequate oversight or public transparency.

Practical Solutions: DPIA, FRIA, AI Literacy

Impact assessments rely on self-assessment, requiring deployers to internally evaluate both the probability of harm occurrence and its severity, enabling them to take steps to mitigate risks.

This framework must address both direct and indirect implications of AI on fundamental rights.

To be able to conduct the assessments, deployers must be euqipped with relevant knwoledge.

GDPR Article 35

Data Protection Impact Assessment requirements

AI Act Article 27

Fundamental Rights Impact Assessment obligations

AI Act Article 4

AI Literacy and training requirements

	PURPOSE LIMITATION	ADMINISTRATIVE	DATA ACCURACY	SYSTEM ACCURACY
TECHNICAL	Does the FRT work for multiple purposes (e.g. emotion recognition) or only for one or more of the following: identification, authorization, surveillance.	Is the FRT integrated with another system or does it operate as a stand-alone system? If integrated, how are risks mitigated across the multiple systems?	1. What technical standards will be used to capture the biometric data? What steps are taken if the enrolled data is not qualified according to the standards? 2. Which source library does the biometric belong to? Has the source library been tested for bias, discrimination, accuracy, and leakage? 3. How often is the data updated? How often is unnecessary and/or inaccurate data discarded?	1. What steps are taken to ensure that the FRT does not produce inaccurate results? Is the accuracy of the FRT checked regularly? 2. Is the level of accuracy standard for each assessment or is there a dynamic level of accuracy for different assessment cases? 3. Why and how is this level of accuracy chosen? Is it reviewed from time to time? Who decides on the accuracy level and on what basis?

	PURPOSE LIMITATION	ADMINISTRATIVE	DATA ACCURACY	SYSTEM ACCURACY
PRACTICAL	Where will the FRT operate and, if possible, at what time of day? What will be the main purpose of this operation?	1. Is training planned for the staff who will be using the FRT? If so, what are the main aspects of the training? (system use, legal assessment, both?) 2. Who are the actors that can process data on behalf of the LEA? 3. Is there any public feedback involved in the development of the FRT?	1. Is the output data fed back into the system? If so, is the assessment repeated? 2. How could people access and manage their data? How could they request the rectification of their data?	How could people contest the outputs that they think are wrong?

•Gültekin-Várkonyi, G. "Navigating data governance risks: Facial recognition in law enforcement under EU legislation." *Internet Policy Review* 13.3 (2024). https://policyreview.info/articles/analysis/data-governance-risks-facial-recognition

DPIA and FRIA

CEDPO
CONFEDERATION OF EUROPEAN DATA PROTECTION ORGANISATIONS

Domain	Rights Protected
Dignity	Human dignity (1), Right to life (2), Right to the integrity of the person (3), Prohibition of torture and inhuman or degrading treatment or punishment (4), Prohibition of slavery and forced labour (5)
Freedoms	Right to liberty and security (6), Respect for private and family life (7), Protection of personal data (8), Right to marry and right to found a family (9), Freedom of thought, conscience and religion (10), Freedom of expression and information (11), Freedom of assembly and of association (12), Freedom of the arts and sciences (13), Right to education (14), Freedom to choose an occupation and right to engage in work (15), Freedom to conduct a business (16), Right to property (17), Right to asylum (18), Protection in the event of removal, expulsion or extradition (19)
Equality	Equality before the law (20), Non-discrimination (21), Cultural, religious and linguistic diversity (22), Equality between women and men (23), The rights of the child (24), The rights of the elderly (25), Integration of persons with disabilities (26)
Solidarity	Workers' right to information and consultation within the undertaking (27), Right of collective bargaining and action (28), Right of access to placement services (29), Protection in the event of unjustified dismissal (30), Fair and just working conditions (31), Prohibition of child labour and protection of young people at work (32), Family and professional life (33), Social security and social assistance (34), Health care (35), Access to services of general economic interest (36), Environmental protection (37), Consumer protection (38)
Citizens' Rights	Right to vote and to stand as a candidate at elections to the European Parliament (39), Right to vote and to stand as a candidate at municipal elections (40), Right to good administration (41), Right of access to documents (42), European Ombudsman (43), Right to petition (44), Freedom of movement and of residence (45), Diplomatic and consular protection (46)
Justice	Right to an effective remedy and to a fair trial (47), Presumption of innocence and right of defence (48), Principles of legality and proportionality of criminal offences and penalties (49), Right not to be tried or punished twice in criminal proceedings for the same criminal offence (50)

Fundamental Rights Impact Assessments: What are they? How do they work? CEDPO AI and Data Working Group Micro-Insights Series January 2025

Authors: Thomas Ajoodha Jared Browne

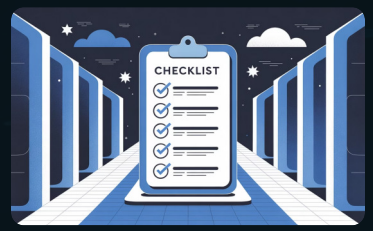
https://cedpo.eu/wp-content/uploads/CEDPO-micro-insight-paper-fundamental-rights-impact-assessments.pdf

Much more is available and is going to be published...

AI Literacy: A Framework for Legal AI Systems

Initial Phase Questions

- Who are the technical and non-technical stakeholders?
- How to rvaluate their existing knowledge?
- What information and training materials do we have at hand?



Assessment Framework

Evaluating both benefits and risks using the 4W1H approach: Who, What, When, Where, and How.

Identifying knowledge gaps and offering targeted trainings to fulfill them.

Practical Implementation

The literature offers quantitative evaluation tools that can be automated for legal AI systems assessment.

Read more: Gizem Gültekin-Varkonyi (2025) "AI Literacy for Legal AI Systems: A practical approach"

Three Components of Legal AI Literacy

Bias and Discrimination

What are bias and discrimination in AI systems, particularly in legal AI systems, and how do they manifest?

What are the possible scenarios in which legal AI systems might generate biased outputs, and what measures are in place to mitigate them?

What auditing tools are available to detect bias and discrimination in legal AI systems, and how do they operate?

Does the legal AI system contribute to eliminating bias and discrimination, or could it potentially exacerbate these issues?

How can organizations ensure that training data for AI systems is representative and free of systemic biases?

Time-Cost Efficiency

In what ways does the legal AI system improve explainability for human professionals?

What explainability methods and tools were followed and why?

Can the legal AI system dynamically adjust its explainability to the needs of the user, or does it generate a general explanation?

What frameworks and methodologies did the organizations adopt to ensure a human-centered approach to designing explainable AI systems for legal applications, or does it provide only what the model can generate?

Is it possible for users to request personalized explanations?

Explainability

Would it cost less to deploy a human evaluator, or is a human-legal AI collaboration more time and cost-efficient?

Are there reasons beyond cost and efficiency, such as better alignment with public interests, for choosing one approach over the other?

How can organizations ensure that cost savings achieved through AI implementation align with fundamental rights?

Why is this legal AI system more cost-efficient than relying on humans?

In which areas is the time and cost efficiency of the legal AI system least risky to human rights, making it suitable for deployment?.

Thank you!

Dr. Gizem Gültekin-Várkonyi, senior lecturer

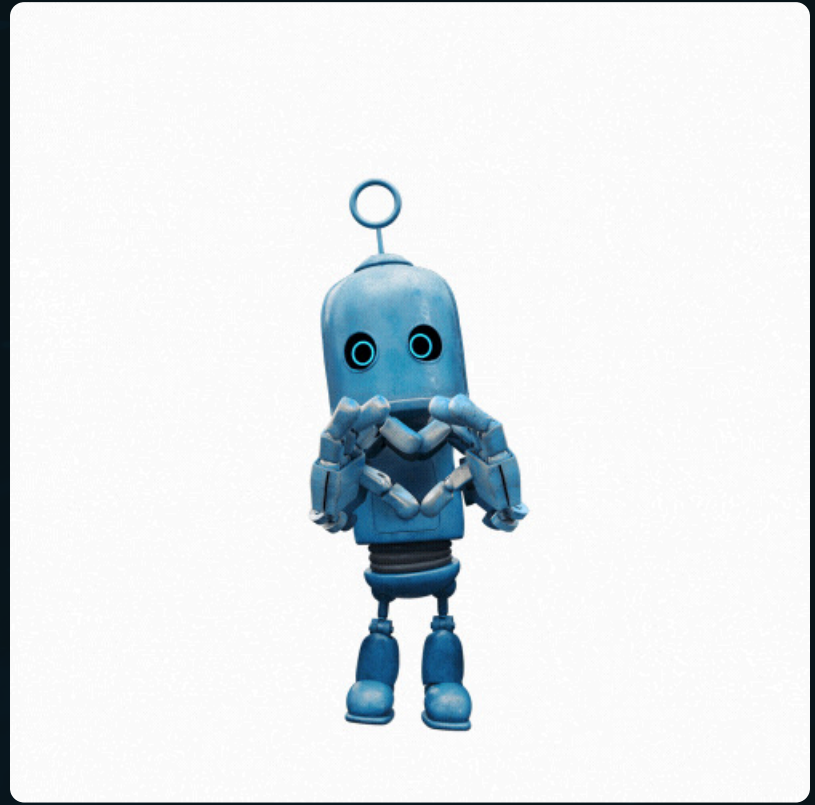
University of Szeged, Hungary

Faculty of Law and Political Sciences

International and Regional Studies Institute

@gizemgv@juris.u-szeged.hu

@drgultekingizem@gmail.com



Risk management in legal AI systems: Case of FRT and some practical solutions

Dr. Gizem Gültekin-Várkonyi, senior lecturer

University of Szeged, Hungary

Faculty of Law and Political Sciences

International and Regional Studies Institute

@gizemgv@juris.u-szeged.hu

@drgultekingizem@gmail.com

Co-funded by the European Union

What is "Legal AI Systems"?

Very difficult to come up with a single taxonomy…

•Legal Intelligence Retrieval Systems

•Legal Drafting and Content Generation Systems

•Regulatory Compliance and Monitoring Systems

•Litigation Support and Evidence Management Systems

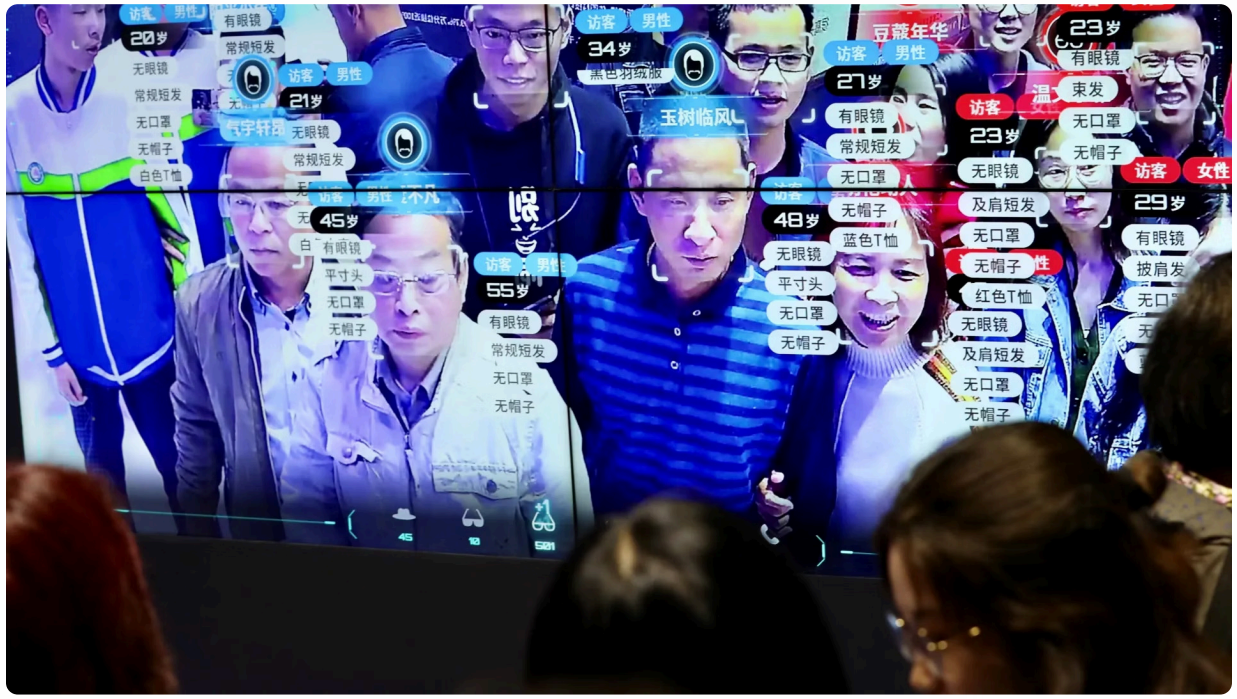
•Predictive Legal Analytics and Forecasting Systems

•....

•**Criminal Justice and Biometric Systems**

TECHNOLOGY OVERVIEW

What is FRT? Beyond Simple Definition



FRT is conceptualized primarily through its role in biometric data processing.

From a risk assessment perspective, it is the intended use—not only the definition—that determines the risk profile.

The technology serves various purposes: face recognition (verification or authentication), emotion assessment, behavior analysis,individual tracking in crowds…

Three Core FRT Functions in Law Enforcement

Authentication

One-to-one search method for identity verification, such as unlocking devices or access control systems.

Identification

One-to-many search in controlled environments like airports, querying databases of known individuals post-biometric processing.

Profiling

Many-to-many live processing for real-time surveillance, categorizing individuals by age, gender, race, or emotional state—introducing heightened risks.

The discernment of functionality and purpose remains pivotal for comprehensive risk assessment in law enforcement applications.

Real-World Deployments: Germany and Italy

Germany: Cross-Border Crime Fighting

Live FRT is operational in Saxony and Berlin for gang crime investigations. The system records license plates and compares data against wanted individuals databases, particularly near border regions.

Initially kept under wraps, this deployment raises transparency concerns about public notification and oversight.

Italy: Stadium Surveillance

Italy's Serie A plans FRT solutions at stadium entry points to identify fans who break racial discrimination rules (Udinese case)

Data collected by clubs would be shared with police when deemed necessary, creating questions about data governance and proportionality.

Read here: **https://idtechwire.com/saxony-berlin-cops-turn-to-real-time-frt-to-fight-organized-crime/**

and here: **https://www.biometricupdate.com/202401/facial-recognition-planned-for-all-stadiums-in-italys-top-football-league**

The Public Acceptance Paradox

When People Accept FRT

People are more likely to accept FRT when they believe it is genuinely for security purposes and limited to that specific context. Some practices show FRT can assist law enforcement in efficiently identifying and apprehending suspects (Hamann & Rachel, 2019).

> However, FRT appears more beneficial for law enforcement agencies and providers than for the public. Current literature provides no evidence supporting positive correlations between FRT deployment and public trust or security outcomes.

The challenge: These tools are typically adopted through top-down implementation without sufficient public consultation or empirical justification, raising several concerns.

Concerns with FRT Deployment

Data-Related Challenges

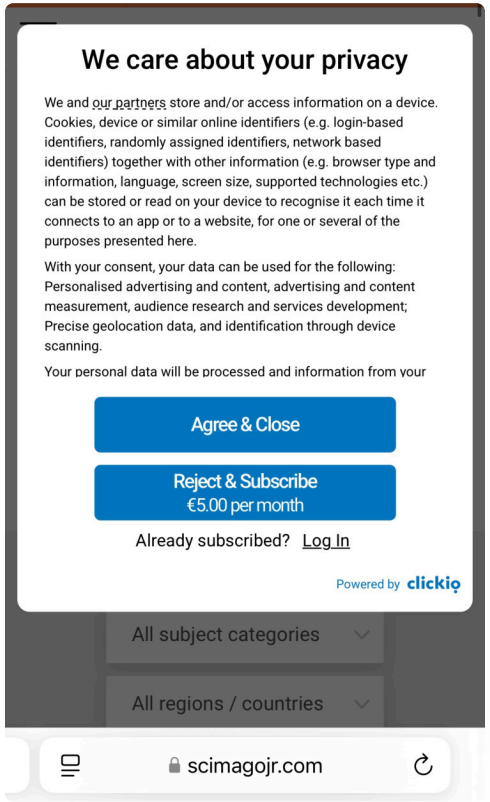
- Data minimization: Collecting only essential data. Case of Clearview AI in Italy, Amazon Ring case.
- Data accuracy: Difficulty in updating the data at LEA databases.
- Purpose limitation: Function creep (case of ChatGPT, Clearview AI again)
- Do we have a choice to opt-in or out?

Technical Challenges

- Bias-Presumption of innocence
- Explainability: Fake explanations of ChatGPT
- System accuracy: Who decides, what confident level?

Administrative Challenges

- Outsourcing: Managing third-party vendor risks
- Conscious use: Ensuring ethical and lawful deployment



RISK ANALYSIS

Data Processing Violations

01

Extensive Data Collection- Clearview AI

GDPR data processing includes collecting, not merely processing. FRT systems gather biometric data on anyone in public spaces without individual's knowledge, consent, avoidence.

The Italian DPA punished the company, but…

02

Amazon Ring

Private households.

Location, device or user ID, email address, name, phone number, photos or videos, physical address, product interactions, purchase history, and other types of data.

Amazon Ring collects 10 data types under the vague ‘’Other Purposes

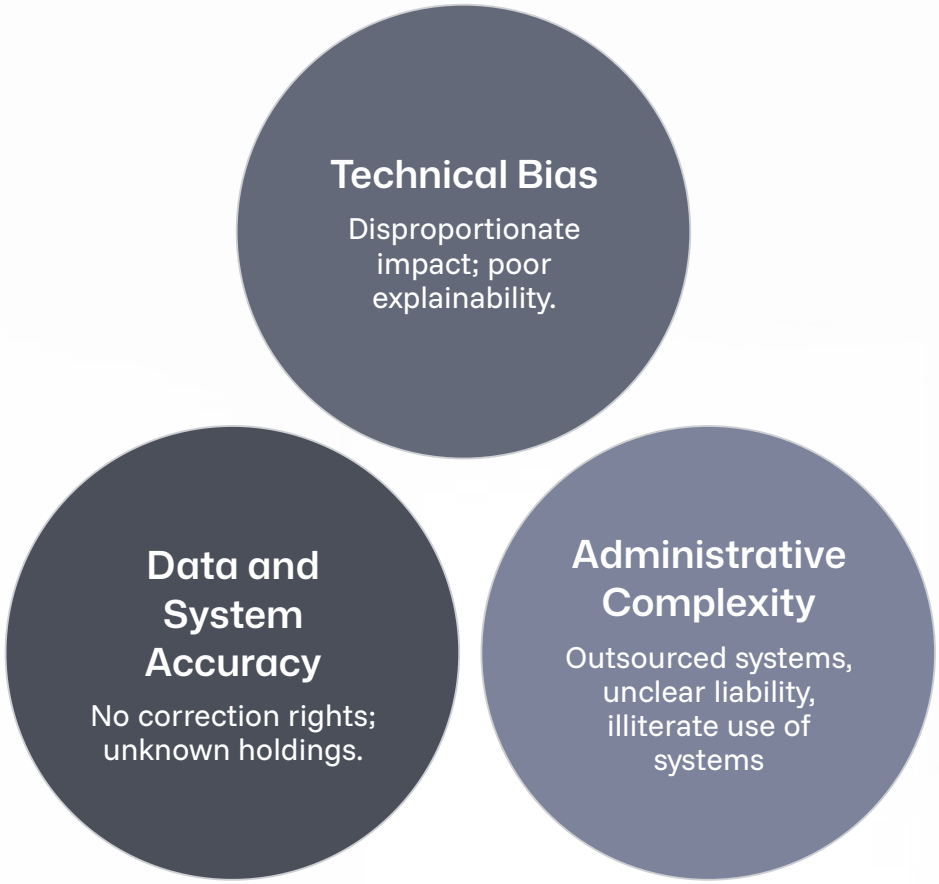
03

ChatGPT use for LEA purposes

Prompting the system with VERY sensitive data, analysis of cases, sometimes with visuals or for visualization purposes.

InterPol report.

Technical and Administrative Challenges



These challenges compound when systems are deployed without adequate oversight or public transparency.

Practical Solutions: DPIA, FRIA, AI Literacy

Impact assessments rely on self-assessment, requiring deployers to internally evaluate both the probability of harm occurrence and its severity, enabling them to take steps to mitigate risks.

This framework must address both direct and indirect implications of AI on fundamental rights.

To be able to conduct the assessments, deployers must be euqipped with relevant knwoledge.

GDPR Article 35

Data Protection Impact Assessment requirements

AI Act Article 27

Fundamental Rights Impact Assessment obligations

AI Act Article 4

AI Literacy and training requirements

	PURPOSE LIMITATION	ADMINISTRATIVE	DATA ACCURACY	SYSTEM ACCURACY
TECHNICAL	Does the FRT work for multiple purposes (e.g. emotion recognition) or only for one or more of the following: identification, authorization, surveillance.	Is the FRT integrated with another system or does it operate as a stand-alone system? If integrated, how are risks mitigated across the multiple systems?	1. What technical standards will be used to capture the biometric data? What steps are taken if the enrolled data is not qualified according to the standards? 2. Which source library does the biometric belong to? Has the source library been tested for bias, discrimination, accuracy, and leakage? 3. How often is the data updated? How often is unnecessary and/or inaccurate data discarded?	1. What steps are taken to ensure that the FRT does not produce inaccurate results? Is the accuracy of the FRT checked regularly? 2. Is the level of accuracy standard for each assessment or is there a dynamic level of accuracy for different assessment cases? 3. Why and how is this level of accuracy chosen? Is it reviewed from time to time? Who decides on the accuracy level and on what basis?

	PURPOSE LIMITATION	ADMINISTRATIVE	DATA ACCURACY	SYSTEM ACCURACY
PRACTICAL	Where will the FRT operate and, if possible, at what time of day? What will be the main purpose of this operation?	1. Is training planned for the staff who will be using the FRT? If so, what are the main aspects of the training? (system use, legal assessment, both?) 2. Who are the actors that can process data on behalf of the LEA? 3. Is there any public feedback involved in the development of the FRT?	1. Is the output data fed back into the system? If so, is the assessment repeated? 2. How could people access and manage their data? How could they request the rectification of their data?	How could people contest the outputs that they think are wrong?

•Gültekin-Várkonyi, G. "Navigating data governance risks: Facial recognition in law enforcement under EU legislation." *Internet Policy Review* 13.3 (2024). **https://policyreview.info/articles/analysis/data-governance-risks-facial-recognition**

DPIA and FRIA

CEDPO
CONFEDERATION OF EUROPEAN DATA PROTECTION ORGANISATIONS

Domain	Rights Protected
Dignity	Human dignity (1), Right to life (2), Right to the integrity of the person (3), Prohibition of torture and inhuman or degrading treatment or punishment (4), Prohibition of slavery and forced labour (5)
Freedoms	Right to liberty and security (6), Respect for private and family life (7), Protection of personal data (8), Right to marry and right to found a family (9), Freedom of thought, conscience and religion (10), Freedom of expression and information (11), Freedom of assembly and of association (12), Freedom of the arts and sciences (13), Right to education (14), Freedom to choose an occupation and right to engage in work (15), Freedom to conduct a business (16), Right to property (17), Right to asylum (18), Protection in the event of removal, expulsion or extradition (19)
Equality	Equality before the law (20), Non-discrimination (21), Cultural, religious and linguistic diversity (22), Equality between women and men (23), The rights of the child (24), The rights of the elderly (25), Integration of persons with disabilities (26)
Solidarity	Workers' right to information and consultation within the undertaking (27), Right of collective bargaining and action (28), Right of access to placement services (29), Protection in the event of unjustified dismissal (30), Fair and just working conditions (31), Prohibition of child labour and protection of young people at work (32), Family and professional life (33), Social security and social assistance (34), Health care (35), Access to services of general economic interest (36), Environmental protection (37), Consumer protection (38)
Citizens' Rights	Right to vote and to stand as a candidate at elections to the European Parliament (39), Right to vote and to stand as a candidate at municipal elections (40), Right to good administration (41), Right of access to documents (42), European Ombudsman (43), Right to petition (44), Freedom of movement and of residence (45), Diplomatic and consular protection (46)
Justice	Right to an effective remedy and to a fair trial (47), Presumption of innocence and right of defence (48), Principles of legality and proportionality of criminal offences and penalties (49), Right not to be tried or punished twice in criminal proceedings for the same criminal offence (50)

Fundamental Rights Impact Assessments: What are they? How do they work? CEDPO AI and Data Working Group Micro-Insights Series January 2025

Authors: Thomas Ajoodha Jared Browne

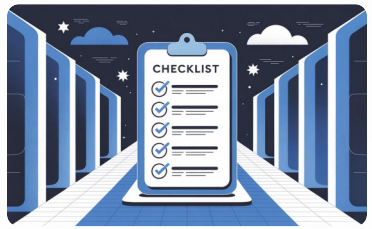
https://cedpo.eu/wp-content/uploads/CEDPO-micro-insight-paper-fundamental-rights-impact-assessments.pdf

Much more is available and is going to be published…

AI Literacy: A Framework for Legal AI Systems

Initial Phase Questions

- Who are the technical and non-technical stakeholders?
- How to rvaluate their existing knowledge?
- What information and training materials do we have at hand?



Assessment Framework

Evaluating both benefits and risks using the 4W1H approach: Who, What, When, Where, and How.

Identifying knowledge gaps and offering targeted trainings to fulfill them.

Practical Implementation

The literature offers quantitative evaluation tools that can be automated for legal AI systems assessment.

Read more: Gizem Gültekin-Varkonyi (2025) "AI Literacy for Legal AI Systems: A practical approach"

Three Components of Legal AI Literacy

Bias and Discrimination

What are bias and discrimination in AI systems, particularly in legal AI systems, and how do they manifest?

What are the possible scenarios in which legal AI systems might generate biased outputs, and what measures are in place to mitigate them?

What auditing tools are available to detect bias and discrimination in legal AI systems, and how do they operate?

Does the legal AI system contribute to eliminating bias and discrimination, or could it potentially exacerbate these issues?

How can organizations ensure that training data for AI systems is representative and free of systemic biases?

Time-Cost Efficiency

In what ways does the legal AI system improve explainability for human professionals?

What explainability methods and tools were followed and why?

Can the legal AI system dynamically adjust its explainability to the needs of the user, or does it generate a general explanation?

What frameworks and methodologies did the organizations adopt to ensure a human-centered approach to designing explainable AI systems for legal applications, or does it provide only what the model can generate?

Is it possible for users to request personalized explanations?

Explainability

Would it cost less to deploy a human evaluator, or is a human-legal AI collaboration more time and cost-efficient?

Are there reasons beyond cost and efficiency, such as better alignment with public interests, for choosing one approach over the other?

How can organizations ensure that cost savings achieved through AI implementation align with fundamental rights?

Why is this legal AI system more cost-efficient than relying on humans?

In which areas is the time and cost efficiency of the legal AI system least risky to human rights, making it suitable for deployment?.

Thank you!

Dr. Gizem Gültekin-Várkonyi, senior lecturer

University of Szeged, Hungary

Faculty of Law and Political Sciences

International and Regional Studies Institute

@gizemgv@juris.u-szeged.hu

@drgultekingizem@gmail.com

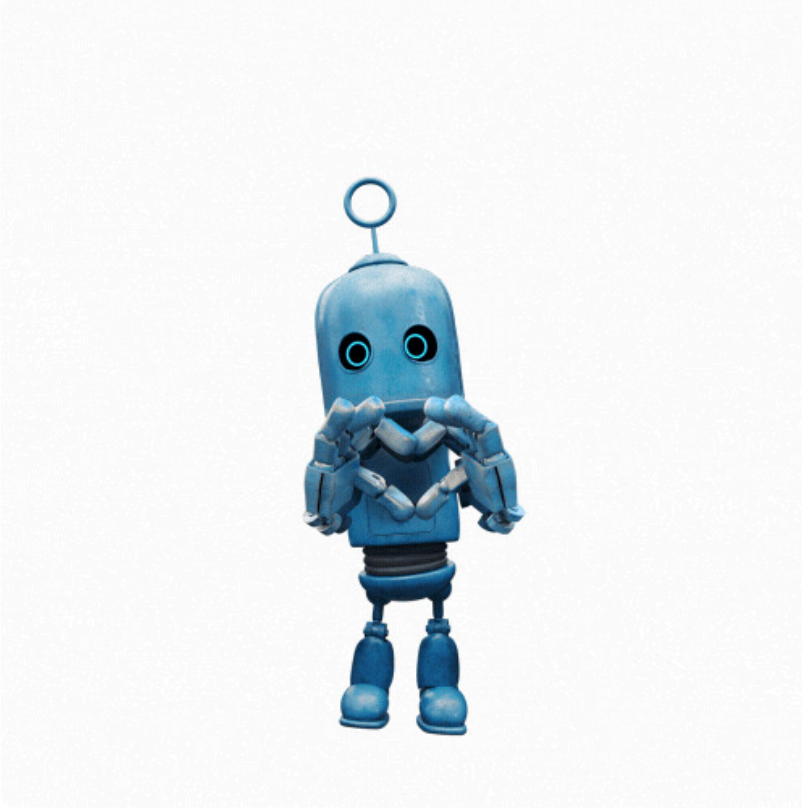


TABLE OF CONTENTS

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*)