# DATA PROTECTION STANDARDS AND THE USE OF AI FOR CRIMINAL INVESTIGATION AND PROSECUTION

LUXEMBOURG, 8 NOVEMBER 2024

VRIJE UNIVERSITEIT BRUSSEL

PAUL DE HERT

paul.de.hert@vub.be

# 4 KEY ISSUES FOR DISCUSSION

1. Short human rights reminder

2. What is data protection law? + Impact of the Law Enforcement Directive ((EU) 2016/680 ) – LED on the use of AI for investigation and prosecution

   - *How does the LED affect the use of AI in law enforcement? Which principles of the LED can be found in the AI Act (AIA)?*

3. Balancing Data Protection and Evidence Law /defense rights

   - *How do data protection laws interact with criminal procedural laws?*

4. The ‘European Courts’ Approach

   - *How do ECtHR and CJEU read criminal procedural laws through a data protection lens?*

1. United Nations High Commissioner for Human Rights *The Right to Privacy in the Digital Age* Report, UN, September 2021, 16p

- The thematic report of the United Nations High Commissioner for Human Rights builds on the 2014 report by the High Commissioner on the right to privacy in the digital age (A/HRC/27/37) and puts the spotlight on Artificial Intelligence (AI), in particular machine-learning technologies.

- The swift increase in the use of AI-empowered techniques, spurred by the imperatives dictated by the on-going global health emergency, has focused the attention to the multifaceted and dynamic impact of AI to the right to privacy and related human rights.

- The right to privacy, as a cornerstone of personal autonomy and self-identity, has become a precondition for the enjoyment of other fundamental rights, both online and offline, and must apply equally and indiscriminately to everyone. Any restrictions to privacy must be legitimately justified.

# The UN High Commissioner for Human Rights on the risks

- AI has become more commonly used for inferring individuals' characteristics or identifying behavioural patterns, which has an impact on privacy and related rights.
- AI also increasingly serves to determine the probability of future preferences or events and, despite inferences' probabilistic nature, potential inaccuracy of data, and data bias. These data are used by decision-makers as evidence in key sectors where people's rights are significantly at stake.
- The outcomes of AI decision-making are not deprived of errors (par. 18). For instance, predictions based on biased data can lead individuals being discriminatorily flagged as prospective terrorists or welfare raiders.
- Ultimately, AI-assisted systems, or those relying on automated decision-making are often opaque, hindering effective accountability for potential human rights violations.

➔The report looks into the following four key sectors in which the use of AI is cause of concern due to its human rights impact, one of them is the criminal law area .

# The UN High Commissioner on AI & criminal law

States are progressively merging AI into law enforcement, national security, criminal justice, and border management. Data that is collected is processed through algorithms to derive computed results indicating or forecasting criminal behaviours and threats which can, for instance, be used to cluster individuals into risky categories or flagging them as possible terrorists and future reoffenders.

➔Privacy and other human rights, including the right to a fair trial, are deeply affected by the collection of data, the enforcement of punishments and other coercive measures through statistical predictions.

➔Often, algorithms trained on biased data target historical minorities which may in turn lead to discrimination.

➔These systems' opacity greatly impairs state accountability.

➔Additionally, the use of remote real-time biometric recognition, including facial emotion recognition, affects privacy and the rights to freedom of expression, association, assembly, and movement, for its recurring erroneous, biased, and discriminatory character.

# The Commissioner’s Human Rights Toolbox for AI (4 layers)

- Suggesting how to tackle AI challenges, the High Commissioner emphasises that only a comprehensive human rights-based approach provides a *toolbox* to find ways to minimise or avoid harm whereas making the best of technology for all.

**1st layer:** Developments and deployments of AI should be surrounded by a framework of human rights principles, including equality, non-discrimination, participation, and accountability.

**2nd layer:** Principles of legality, legitimacy, necessity, and proportionality shall infuse its application, particularly when AI is expected to restrict the right to privacy. Sometimes, less interfering measures, or no AI, could be required. For instance, demanding welfare beneficiaries to subject to biometric identification is disproportionate in the absence of alternatives.

**3rd layer:** AI applications should aim at ensuring availability, affordability, accessibility, and quality as central elements for the realization of economic, social, and cultural rights.

**4th layer** The High Commissioner underlines the importance of human rights due diligence,

➔a cyclic process through which human rights risks are identified, assessed, and prevented when AI systems are *acquired*, *developed*, *deployed*, *and operated*, as well as before individuals’ data are shared or used. If due diligence establishes that AI is incompatible with human rights law and no meaningful means exist to mitigate harm, it should be banned.

➔Due diligence also requires states to engage in a meaningful consultation with AI-affected stakeholders, primarily vulnerable groups.

# Outcome of this toolbox-exercise should be laws with safeguards and oversight

Safeguards need to be implemented as AI continues expanding its reach.

- Data privacy laws remain the front-line framework to prevent harmful AI, but these need to be constantly adjusted, and tightened if necessary.
- Other laws and sector-specific legislation, particularly in areas where AI crucially impacts upon people's life, shall be enhanced, tailored, or adopted *in a rights-respecting way*: 'the higher the risk for human rights, the stricter the legal requirements for the use of AI technology should be' (para. 45). Specific AI tools that cannot comply with human rights may have to be prohibited under a legislative risk-based approach.
- Moreover, moratoriums should be placed on potentially high-risk technologies before they can be assessed and have safeguards implemented. Also, export control regimes should be strengthened to prevent cross-border trade of technologies that could violate human rights.
- States should make human supervision and decision-making mandatory when AI is likely to have an adverse effect on human rights
- Independent data privacy oversight bodies, aided by a cross-sectoral combination of administrative, judicial, quasi-judicial and/or parliamentary oversight bodies, and civil society engagement are paramount to challenge the complexities, opacity, and power asymmetries of the global data environment.

## 2. Data protection principles

At the level of the Council of Europe

-Data protection as such first regulated in 1981 Council of Europe treaty 108

- All EU Member States have ratified Convention 108.
- Open for accession by non-Contracting Parties of the CoE: countries from Africa and South-America also acceded.
- Recent mondernization led to the adoption of a protocol amending Convention 108 (Protocol CETS No. 223, Strasbourg, 10.X.2018).
- Provides new rights, e.g. the right to object to a data processing, or the right not to be subject to decisions solely based on automated processing.

-Council of Europe's Framework Convention on Artificial Intelligence and Human Rights, Democracy and the Rule of Law (published on 5.9.2024)
-Council of Europe Cybercrime Convention (see later)

At the level of ther EU

-the General Data Protection Regulation (EU) 2016/679 (GDPR).
-the Law Enforcement Directive (EU) 2016/680 (LED) was published together with GDPR and defines (the same) basic principles, such as purpose limitation and data minimisation, much along the lines of the GDPR

# GDPR/LED Principles/rights/good ideas

1. Lawfulness, fairness and transparency
2. Purpose limitation
3. Data minimization
4. Accuracy
5. Storage limitations
6. Integrity and confidentiality
7. Accountability

➔on these principles next slide

- Right to information;
- Right to access
- Right to rectification
- Right to object to a data processing,
- Right not to be subject to decisions solely based on automated processing.

***Good ideas***: privacy by design/mandatory data protection officers/data protection impact assessments

1. **lawfulness, fairness and transparency**

   =processed lawfully, fairly and in a transparent manner in relation to the data subject

2. **purpose limitation**

   = collected for specified, explicit and legitimate purposes + not further processed in a manner that is incompatible with those purposes (except for archiving)

3. **data minimization**

   =adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed

4. **accuracy**

   = accurate and kept up to date + inaccurate data shall be erased or rectified without delay

5. **storage limitation**

   = kept in a form which permits identification of data subjects for no longer than is necessary **except** for archiving in public interest /statistical scientific purposes

6. **integrity and confidentiality**

   =appropriate technical or organisational measures that ensures appropriate security of the personal data and protection against unauthorised or unlawful processing/accidental loss, destruction or damage

7. **accountability**

   = The controller shall be responsible for, and be able to demonstrate compliance with lawfulness, fairness and transparency ➔ demands HUMAN OVERSIGHT OR HUMAN IN THE LOOP OR HUMANS CONTROLLING THE LOOP

# MAIN ELEMENTS IN THE LED

- LED *(lex specialis* to GDPR*)* objective: protection of individual rights by ensuring transparency in data processing for criminal investigation and prosecution
- Data protection principles:
  - purpose limitation (Art. 4 LED),
  - data minimisation (Art. 4 (1) (c) LED)
  - data quality (Art. 7 LED)
- Human Oversight in automated decision-making (Article 11 LED)
- Transparency and the Right to Information (Article 13 LED):
  - Art. 13 (1): content of information (including rights of the data subject)
- Ex Post Notification – Article 13 (2) (d):
  - Obligation to provide *further information*, where personal data is collected *without the knowledge* of the data subject

# PURPOSE LIMITATION PRINCIPLE

- purpose limitation principle and its two components (‘purpose specification’ and ‘compatible use’) is embedded in Article 4(1)(b) LED

- Article 4(2) then introduces specific conditions for the change of purpose: *subsequent* processing by the *same or another* controller is permitted if *authorised by law* and if *necessary and proportionate* to the new purpose as long as the n*ew purpose remains within the scope of the Directive*

- every subsequent change of purpose by the police or other controllers within the scope of the LED, such as prosecutors or criminal courts, is regulated by this Article 4(2).

- Necessity and proportionality of each re-use has to be reassessed

➔Law enforcement authorities that are considered as data controllers in the light of the LED when using advanced data-driven analytics have to verify these standards

# CJEU JUDGMENT IN *INSPEKTOR V INSPEKTORATA KAM VISSHIA SADEBEN SAVET* CASE C-180/2 [2022

data necessary for investigation of a criminal offence might not be necessary for the prosecution of a criminal offence as well as that different phases of criminal proceedings might result in a different intensity of interference with the right of personal data protection

When the purpose of processing personal data under those listed in Article 1(1) changes from “detection and investigation” to “prosecution”, and the data were collected and originally processed for “detection and investigation” purposes only, the further processing for “prosecution” must be “*necessary and proportionate to that other purpose in accordance with Union or Member State law*”

About the the purposes of processing determined by Article 1(1) LED, : the Court has clarified that “prevention”, “detection”, “investigation”, “prosecution” and “execution of criminal penalties” must be considered as separate and distinct processing activities

“Competent authorities will have to consider “the consequences of the processing of personal data for the data subjects”, “in particular, the degree of interference with the right to the protection of those data”[55] which may be “substantially different” in the case of processing for the purposes of detection and investigation, as opposed to the purposes of prosecution, and therefore differently affect the legality of further processing”. Bonetto, G. (2024). The judgment of the CJEU in Inspektor (Purposes of the processing of personal data – criminal investigations) of 8 December 2022 and the concept of further processing under the Law Enforcement Directive. New Journal of European Criminal Law, 15(1), 58-71.

# DATA MINIMISATION PRINCIPLE

Article 4(1)(c) LED requires data controllers to limit themselves, from the original data collection and throughout the processing, to only the data required for accomplishing the purposes of processing

However: Unlike under the GDPR, there is no need to reduce the processing to the necessary minimum. Controllers under the LED can operate with less precision. They can grab and hold on to data in a rougher manner. However, they must make sure not to process *excessive* datasets,

CJEU (recently) held that a court is bound to observe the principle of data minimisation stemming from the GDPR when deciding on whether to make an order for disclosure in civil proceedings.(Case C-268/21 Norra Stockholm ECLI:EU:C:2023:145, para 55.)

However: Courts, however, are not subject to the supervision of "ordinary" national data protection supervisory authorities.

# ACCURACY PRINCIPLE

Article 4(1)(d) LED contain a data quality requirement relating to the reliability of evidence. Those provisions state that the processing of personal data shall take place in an accurate manner, ensuring also that the personal data being processed are up to dat

➔Law enforcement authorities that are considered as data controllers in the light of the LED when using advanced data-driven analytics have to verify and maintain the quality of the personal data they process in the fulfilment of their duties.

Source: Quezada-Tavárez, Katherine & Vogiatzoglou, Plixavra & Royer, Sofie. (2021). Legal challenges in bringing AI evidence to the criminal courtroom. New Journal of European Criminal Law. 2021, 12, n° 4, 538

# ACCURACY PRINCIPLE

Moreover

1) Member States must make a distinction between personal data based on facts and personal data based on personal assessments (art. 7(1) LED)

2) Adding a layer of data quality, the Directive proposes the requirement of verification in its Article 7(2).

= In order to make sure that personal data which is inaccurate, incomplete, or no longer up to date is not transmitted or made otherwise available, competent authorities must, as far as practicable, verify the quality of this data before its transmission

# TRANSPARENCY

=Article 13 LED (the right to information) is a central provision within the LED, as it encompasses the minimum content of the information sought to be made available to data subjects

- individuals should be informed about the intended purposes of the processing and the existence of their right to request from the controller access to and rectification or erasure of their personal data and restriction of processing of personal data. Article 13(1)(c) and (e) LED, respectively.
- the competent authorities must give further information to the data subject in specific cases (Article 13(2) ➔see next slide
- A gem somewhat hidden in Article 13(2)(d) LED is ex post notifications of data-processing activities within criminal proceedings which took place without the knowledge of data subject.

➔They are a crucial safeguard in criminal proceedings (for example when the purposes of a covert surveillance measures have been achieved

# WHAT IS FURTHER INFORMATION?

The ‘further information’ to be given to particular data subjects is important in cases of automated decision-making, as the opacity of the law enforcement practices requires an advanced level of protection for the data subject

➔This obligation imposed on LEAs expands to AI applications, which should be accompanied by substantial information about the logic and the algorithm used for processing, its significance, its error rate, and the implications it may have for the data subject.

(European Union Agency for Fundamental Rights, *Handbook on European data protection law* (2018), p. 211)

# RESTRICTIONS?

The right of information can be restricted, delayed, or even omitted if so provided by Member State law and for purposes explicitly mentioned in Article 13 (3) (a-e) LED.

Respective legislative measures may be adopted with a view to determining the categories of processing, or parts thereof, which fall under the derogations to the obligation for giving further information.

➔In the context of criminal investigations and evidence gathering, this means that data subjects will not get information about things like automated decision-making or the use of AI until the purposes have been achieved by the investigative authorities.

➔However, it also means that data subjects should receive all necessary information ex post and be able to challenge the respective investigative techniques before both the trial court and the supervisory authority.

# EXPANDING THE LED TO THE USE OF HIGH-RISK AI SYSTEMS IN LAW ENFORCEMENT

- LEAs as Controllers of personal data and Developers of high-risk AI systems
  - Article 10 AIA: development of training, validation and testing datasets to meet **quality** criteria
  - Article 13 AIA: design and development of high-risk AI systems in a way that ensures their **transparency** to deployers
- LEAs as Controllers of personal data and Deployers of high-risk AI systems
  - Article 26(1) AIA: obligation to take measures to ensure compliance with instructions of use
  - Article 26 (2) AIA: obligation of to assign **human oversight**
  - Article 26 (11) AIA: obligation to **inform** natural persons that they are subject to the use of high-risk AI systems
  - Article 86 AIA: obligation to provide clear and meaningful **explanations** to the data subject for a decision taken on the basis of the output of a hirgh-risk AI system
  - Article 27 AIA: obligation to perform a fundamental rights impact assessment *prior to the system's deployment* – link to Art. 27 LED
  - Article 26 (10) AIA: obligation for documentation of each use of high-risk AI systems in the case file

# ASSESSING THE ADDED VALUE OF LED

Prepared together with the GDPR , LED shows clear signs of willingness to push data protection level higher as compared to earlier EU regulations

Being granular and specific, the level of detail matters and careful balancing has been done to apply data protection principles without closing the door for intelligence led policing, police innovation and use of big data analytics and AI

-P. De Hert & Juraj Sajfert, ‘Regulating Big Data in and out of the data protection policy field: Two scenarios of post-GDPR law-making and the actor perspective’, *EDPL*, 2019, vol. 5/3, 338 – 351

-P. De Hert & Juraj Sajfert, 'The fundamental right to personal data protection in criminal investigations and proceedings: framing big data policing through the purpose limitation and data minimisation principles of the Directive (EU) 2016/680, *Brussels Privacy Hub Working Paper*, 2021, vol. 7 (31), December 2021, 17p. Direct link to page https://brusselsprivacyhub.eu/publications/wp731

# IMPACT IS SUBTLE: EXAMPLE

“In the context of the re-assessment of the proportionality requirement, however, the fundamental right to data protection will require specific consideration. Competent authorities will have to consider “the consequences of the processing of personal data for the data subjects”, “in particular, the degree of interference with the right to the protection of those data” which may be “substantially different” in the case of processing for the purposes of detection and investigation, as opposed to the purposes of prosecution, and therefore differently affect the legality of further processing. This may greatly affect the discretion of those competent authorities vested with prosecutorial functions. It may also affect their independence, as the findings on proportionality with respect to the data protection rights may be open to challenge before the data protection supervisory authorities established under Article 41 LED. However, Article 4(2)(b) LED requires the re-assessment of proportionality to be “*in accordance with national law and EU law*”, which may include, for example, safeguards to the discretion and independence of the prosecutorial function”.

-Bonetto, G. (2024). The judgment of the CJEU in Inspektor (Purposes of the processing of personal data – criminal investigations) of 8 December 2022 and the concept of further processing under the Law Enforcement Directive. New Journal of European Criminal Law, 15(1), 58-71.

# ASSESSING THE ADDED VALUE OF LED

-LED recalibrates the general data protection principles and has an impact on evidence law but

1. Implications of the LED for court’s activities rand office of prosecutors (independent or not?) remain unclear
2. hesitates to enter into the details about the processing work done by contemporary police. Big data relevant processing practices (web crawling, data mining, data matching, etc.) are not mentioned in the LED.
3. hestitates to incorporate the case law of Europan Courts on mass surveillance
4. ideas such as predictive policing are launched in the recitals and provisions of the Directive without any elaboration apart from the requirement that such processing operations need to be envisaged by law.

➔see https://brusselsprivacyhub.eu/publications/BPH-Working-Paper-VOL7-N31.pdf

# ASSESSING THE ADDED VALUE OF EU AI ACT

1. AI Act does not integrate well, preamble pays hommage to LED that is all

2. It’s focus is respectfull of ideas of privacy by design and default by adressing developpers

3. Human oversight as warranted by the GDPR is enhanced by documentation duties

**(**Guillermo Lazcoz, Paul de Hert, 'Humans in the GDPR and AIA governance of automated and algorithmic systems. Essential pre-requisites against abdicating responsibilities', *Computer, Security and Law Review*, 2023, vol. 50, 20p **)**

<u>But pay attention to its function as a legal ground for processing rather than its function as a framework for processing</u>

1. Art. 59 AI Act and scraping

2. Ai Act and low risk tools (see yesterday)

# 3. Data protection and interaction with evidence Law /defense rights

# EVIDENCE LAW AND DATA PROTECTION: CONSISTENT RATIONALE WITH A CAVEAT

- Dual Compliance for LEAs when collecting evidence
  - Adherence to criminal procedural rules ensures proper gathering, preservation and presentation of evidence in court
  - Adherence to data protection laws ensures lawful, transparent and fundamental rights compliant processing of data
- Why it matters?
  - Evidence Law and Data Protection as pillars of legality in criminal proceedings
- The Belgian Example
  - Article 32 PT CCP allows evidence to be excluded under three conditions:
    1. i. Nullity as sanction in statutory law
    2. ii. Irregularity in evidence collection affects evidence's reliability
    3. iii. Use of evidende would violate the right to a fair trial
  - Impact of the *Antigone judgment* in 2003

# WHAT IS FAIR TRIAL/ WHAT DEFENSE RIGHTS ARE WE TALKING ABOUT

Gless, Sabine. "AI in the Courtroom: a comparative analysis of machine evidence in criminal trials." *Geo. J. Int'l L.* 51 (2019): 195.

Gless, Sabine, Fredric Lederer, and Thomas Weigend. "AI-Based Evidence in Criminal Trials?." *Tulsa L. Rev.* 59 (2024): 1.

Quezada-Tavárez, Katherine & Vogiatzoglou, Plixavra & Royer, Sofie. (2021). Legal challenges in bringing AI evidence to the criminal courtroom. *New Journal of European Criminal Law*. 2021, 12, n° 4, 531-552.

Quezada-Tava´rez et al. approach this question in four steps that tackle the main categories of criminal procedure rules in the European criminal law landscape: admissibility, reliability, challenging by the defendant and evaluation by the judge.

# APPLYING THE EXCLUSIONARY PRINCIPLE IN THE ALGORITHMIC CONTEXT: MAY PROVE CHALLENGING!

Identifying unlawfully obtained evidence and applying the exclusionary principle in the algorithmic context may prove challenging (p538)

➔requires an unambiguous application of relevant legal frameworks, and a clear definition of what it means to obtain evidence when AI functionalities are employed (p538)

➔is not the case

➔Problems may occur already when determining whether AI evidence complies with or violates applicable laws. (next slide)

➔given that unlawfully obtained evidence is not necessarily inadmissible, assessing the weight such violations hold on the overall fairness of the trial may be particularly difficult for judges,.

# THESE PROBLEMS ARE EVIDENT WHEN ONE THINKS ABOUT ASSESSING VIOLATIONS TO NON-DISCRIMINATION OR DATA PROTECTION RULES BY AI TOOLS

-Lawfulness may be affected during the design phase; for instance, the use of discriminatory or biased datasets to train the algorithms could guide officers towards the biased collection of data or the biased profiling and identification of new suspects.

➔In that case, it is unclear how discrimination law applies in the first place, and whether such an outcome could be considered as unlawfully obtained evidence.

-Lawfulness may also be affected when privacy and personal data protection principles like transparency and purpose limitation are not respected.

The lawfulness of data collection may be dubious when, for instance, police hacking is involved or due to the opacity of the AI system generating evidence.

Similarly, discerning the exact purpose of each AI system and whether any reusing of datasets for different criminal cases complies with the purpose limitation principle and its permissible restrictions may necessitate a case-by-case analysis, creating a degree of uncertainty

# STEP 2 RELIANCE OF OF EVIDENCE: AUTHENTICITY AND INTEGRITY
(QUEZADA-TAVAREZ ET AL., P539)

= Reliability strongly correlates with the weight of evidence in a criminal trial.

Whereas it is primarily a task for the national judge to assess the reliability of the evidence, the ECtHR has set out some requirements in terms of reliability and accuracy of evidence.

For evidence to be considered reliable, there must be no doubt over its authenticity and integrity.

-*Authenticit*y refers to the irrefutable provenance of the evidence. In other words, LEAs must be able to establish the source of the evidence.

-*Integrity* refers to the fact that evidence remains intact and that it is not tampered with during its collection or subsequent handling by LEAs.

The ECtHR also pays attention to whether the defendant had the opportunity to challenge both the authenticity and the use of the contested evidence

BUT ECtHR only concentrates on manifest flaws; gives national courts a considerable margin of appreciation when assessing the reliability of evidence. Result: all boils down to a case-by-case approach.

➔Qu -Tavarez et al. illustrate this with ECtHR, Khodorkovskiy and Lebedev v Russia,25 October 2013 App no11082/06 and 13772/05,paras72,674- 681, 700.

# ECTHR, KHODORKOVSKIY AND LEBEDEV V RUSSIA, 25 OCTOBER 2013

**FACTS:** K&L alleged that Russian police and prosecuting authorities

-had planted evidence on the crime scene (some of the seized materials were added to the criminal file after the closure of the investigation.)

-had copied information from a hard disk and presented it to the trial judge on paper.

-had presented more evidence to the court than had originally been seized, as the servers had not been properly locked up, and that the evidence was not reliable.

**ECtHR decided that the use of the evidence did not breach Article 6 ECHR**

-defendants had had the opportunity to interrogate witnesses present at the search

-no detection of manifest flaws in the process of seizing and examining the hard drives, which would make the information obtained unreliable.

➔This case shows that the ECtHR only considers obtained evidence as unreliable if there are manifest flaws to be detected in its processing. National courts thus have a considerable margin of appreciation when assessing the reliability of evidence, which boils down to a case-by-case approach (Quezada-Tavarez et al., p539)

# APPLYING RELIANCE PRINCIPLE (AUTHENTICITY AND INTEGRITY) TO THE ALGORITHMIC CONTEXT (QUEZADA-TAVAREZ ET AL., P540)

**Reliability of AI-generated evidence can be affected at three levels.**

authenticity and integrity of the ‘raw’ digital data can be at stake (think about data given by informants)

AI tools can contain miscodes that could remain hidden because of the opacity issue (also known as the ‘black box’ problem),

human experts who are operating AI tools can jeopardise the reliability of AI evidence: low reliability between digital forensics experts examining the same evidence file with the same contextual information, in their observations, interpretations and conclusions. There is a similar risk when it comes to human experts operating AI tools.

Source: Quezada-Tavarez et al. Refer to study by Nina Sunde and Itiel E. Dror, ‘A hierarchy of expert performance (HEP) applied to digital forensics: Reliability and biasability in digital forensics decision making’ (2021) 37 Forensic Science International: Digital Investigation.

## Solution

chronological documentation of evidence and respect the soft law guidance such as Council of Europe, ‘Electronic Evidence Guide. A Basic Guide for Police Officers, Prosecutors and Judges’ (Council of Europe 2013); and :European Union Agency for Cybersecurity (ENISA), ‘Electronic Evidence - a Basic Guide for First Responders’ (2015

**➔contain requirements for a solid chain of custody both at the collection of ‘raw’ digital data and the subsequent processing of this data by AI tools. See** Quezada-Tavarez et al., p541

# WHAT IS FAIR TRIAL/ WHAT DEFENSE RIGHTS ARE WE TALKING ABOUT

-I refer to their analysis for a good understanding of the impact of fair trial and defense principles on AI us

-Yesterday we got a usefull update of this analysis by K Ligetti when discussing the country reports and more recent case law

n**ew procedural guarantees needed in criminal guarantees**

1. -right to information on the AI tool (can be done with ai act )à
2. -a right touches to the full collection of data
3. -right to access to the AI tool
4. -right to seexplanaiton of the forensic methods and results
5. -rights to have digital forensic assistance

# FAIR PROCESS RIGHTS ENHANCED BY DATA PROTECTION LAW?

My guess is that the data protection standards inspire new developments with regard to defence rights

That does not surprise me: these standards where initially conceived as fair information principles and ‘fair’ is also the essence of what kind of trial we want

But there are limits of what we can do with data protection

Article 6 ECHR requirements in many ways equal data protection rights and in some cases might go further

Example: *Yüksel Yalçınkaya v Türkiye* App No 15669/20, para. 341 (ECtHR, 26 September 2023). Next slide

# *YÜKSEL YALÇINKAYA V TÜRKIYE (2023)*

in *Yüksel Yalçınkaya v Türkiye* the Court emphasised that such an opportunity might entail more than mere access to the data-processing reports included in the case file. In order to be able to contest (*in casu*, electronic) evidence and effectively conduct his defence, the <u>disclosure of raw </u>data is necessary, enabling integrity and reliability assessments of evidence deriving therefrom.

In the same spirit, S Gless et al. rightly argue that, with regard to device evidence, mere access to the prosecutor's dossier may fall short of fulfilling Article 6 ECHR requirements, as defendants may "have interest in learning how and on what basis the device came to its conclusions". Notably, they highlight a judgment of the German Federal Constitutional Court (BverG, 12.11.2020, 2 BvR 1616/18), which recognised a 'right to raw data' in cases involving device evidence, affirming that defendants are entitled to access all relevant raw and/or measurement data that have been stored for investigation purposes, even if they were not included in the case file, see S Gless et al. 'AI-Based Evidence in Criminal Trials?.' (2024) 59 Tulsa Law Review, pp. 28-29.

# FAIR PROCESS RIGHTS ENHANCED BY DATA PROTECTION CASE LAW?

- ECtHR (*Uzun v Germany*) and CJEU (Case C-205/21 *Bulgarian Court*) often reading criminal procedural codes through a data protection lens.
- However, they are both reluctant to ‘sanction’ evidence obtained through privacy violations
- ECtHR case law confirms that using evidence obtained via privacy violactions **does not automatically lead** to fair trial violations, provided that the defendant can challenge the evidence in court ( e.g. *Khan v the United Kingdom, Lee Davies v Belgium, Yüksel Yalçınkaya v Türkiye*)
- CJEU also places the emphasis on the ability to **comment effectively** on the way evidence was collected, as a reflection of the right to a fair trial (e.g. *La Quadrature du Net and Others, Prokuratuur, MN*)