University of Basel
Faculty of Law

AI, Data Quality & the Implications for Evidence from a Comparative Perspective

Prof. Dr. Sabine Gless
Faculty of Law, University of Basel/Switzerland

April 2024

Outline

1	Data Quality Affecting the Poor & Vulnerable - European examples
2	General Data Protection Regulation's (GDPR) Potential – and where it falls short as a safeguard for data quality
3	AI Act's Potential for Data Quality in European Courts – and where it may fall short
4	Will EU Regulation Deliver High Data Quality in European Courts?
5	A Comparative Outlook

1 Data Quality Affecting Vulnerable Parties–not only an AI issue:

British Post Office Scandal

From 1999 to 2015 more than 900 subpostmasters were wrongly prosecuted for “stealing” money because of incorrect information provided by the Horizon computer system. The system falsely reported shortfalls because it had not been tracking money from lottery terminals, Vehicle Excise Duty payments or cash machine transactions. According to their contracts subpostmasters had to cover the (non-existent) shortfalls as they were responsible for any unexplained loss.

The **British answer**:

- redress and compensation schemes (apparently not sufficient to cover what has been lost);
- criminal investigation;
- regulatory action;
- TV drama: “Mr Bates vs the Post Office” (broadcast in January 2024);
- *and call for reform on “digital evidence”; British Computer Society called for reconsideration of “courts' default presumption that computer data is correct”.*

1 Data Quality Affecting the Poor – not only in the U.S.:
Dutch Data Scandal (Fraude Signalering Voorziening FSV)

In 2019 it was revealed that the Dutch tax authorities had used FSV to create risk profiles in an effort to spot childcare benefits fraud. Authorities penalized families based on the system's risk indicators, until it turned out that

- the authorities had no statutory basis for processing personal data in the FSV;
- the purpose of the FSV was not specifically described in advance (and its “self-learning algorithm” was “biased”); and
- it contained partly incorrect information.

The **European answer: comply with the General Data Protection Regulation (GDPR)**, i.e.
- data has to be of good quality [accurate & up-to-date, [Art. 5 (1) lit. d GDPR];
- define the purpose of data processing (according to the legal basis, Art. 5 (1) lit. b GDPR]);
- and adhere to «fairness principles», [Art. 5 (1) lit. d GDPR]

or pay (€3.7 million fine for Tax Authority that used FSV for blacklisting).

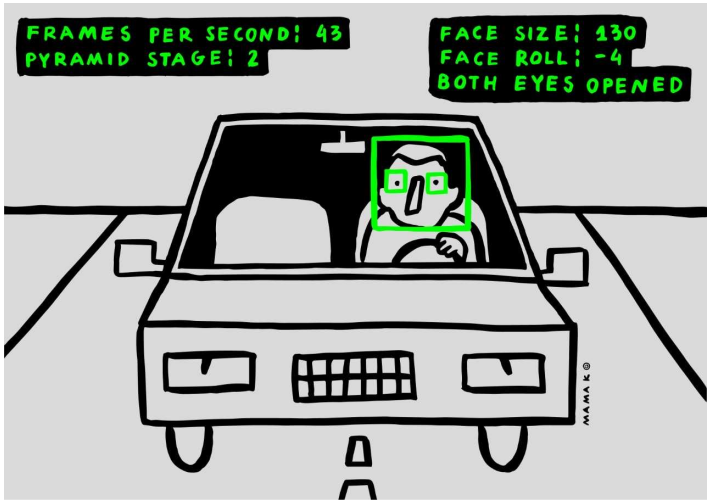
2 General Data Protection Regulation's (GDPR) Potential – and where it falls short as a safeguard for data quality

Art. 5 GDPR requires:
- **lawfulness;**
- **fairness (accuracy, timeliness);**
- **transparency** (in relation to the data subject)

based on various principles, e.g. the principle of accuracy laid down in 5(1)(d)GDPR stipulates that personal data must be 'accurate and, where necessary, kept up to date'.
*Furthermore: Art. 22 GDPR grants a «**right to contestation**» etc.*

Two paradigmatic **shortfalls of GDPR**
1.
lacks specification of metrics to measure accuracy (i.e. margin of error or frequency of updates), only requires that controllers must take 'every reasonable step.
2.
only applies where **«personal data»** is processed, i.e. "any information relating to an identified or identifiable natural person".

2 General Data Protection Regulation's (GDPR) Potential – and where it falls short as a safeguard for data quality

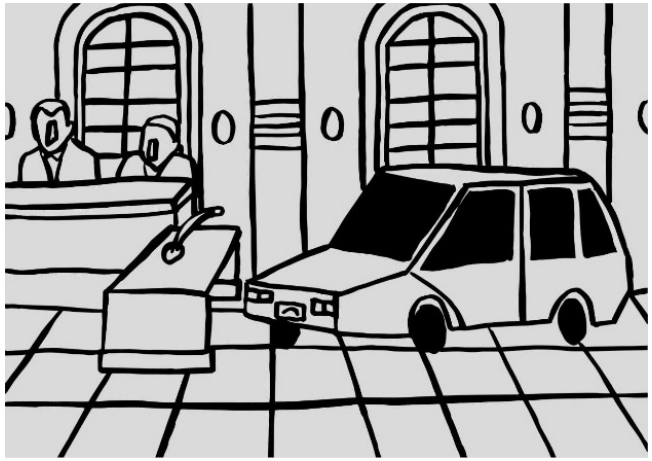


Does the GDPR apply to AI generated evidence,
like an alert issued by a driver drowsiness detection system that is based on a "smart mix" of

- steering pattern monitoring & vehicle position in lane monitoring; and
- driver eye/face monitoring as well as other physiological measurements like muscle activity, sitting positions, etc. ?

3 AI Act's Potential for Data Quality in European Courts – and where it may fall short

Cars that monitor their drivers,
or "forensic dogs"



or other *AI systems generating evidence do not necessarily process personal data and thus may not fall into the scope of GDPR*,

and cannot be called upon to give testimony and be confronted about their "observations", and expert testimony also falls short for various reasons.

In this light the *AI Act rightly takes a … «risk-based» approach, with AI systems producing evidence for legal proceedings considered «high risk»*.

3 AI Act's Potential for Data Quality in European Courts – and where it may fall short

Art. 10 AI Act requires for "high risk" AI system's data
- **relevance** (timeliness);
- **freedom of errors** (accuracy & bias detection) [Art. 15(1) and (2) & 13(3) AI Act];
- **completeness** (& factor diversity) [Art. 10(3) & 13(2) AI Act];
- **balancing**, "appropriate statistical properties" [Art. 10(3) AI Act];
- **representativeness** [Art. 10(3) and (4) AI Act].

The required measures are
- continuous monitoring, testing documentation [Art. 10-12 AI Act] ;
- transparency, human oversight, iterative updates [Art. 13 &14 AI Act] ;
- publication of the provenance of training data
  [Art. 13(3) & Art. 15(2) AI Act]

3 AI Act's Potential for Data Quality in European Courts – and where it may fall short

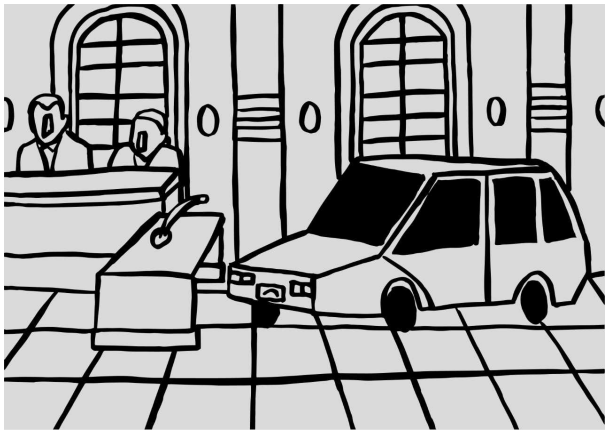
Does Art. 10 AI Act square the circle? As it

- **lacks adequate links to other EU instruments**, e.g. Art. 10(2) AI Act stipulates bias screening of training data, but leaves open what follows from a detection of bias - *exclusion of AI generated evidence?*;
- **seems too vague** ('freedom from errors'; 'completeness'; 'appropriate statistical properties' without offering further guidance) **for the looming sanctions**, Article 71(3) AI Act reserves the maximum fine of up to 6% of global annual turnover for the violation of the training data regime;

- *zooming in:* Art. 10 (5) AI Act exception to the prohibition to process sensitive data enshrined in Article 9 (1) GDPR for the purpose of rebalancing data sets.
  But the tension between data protection and non-discrimination law should be resolved for all cases where it is necessary for the purposes of ensuring bias monitoring, detection and correction, or not?

4 Will the EU Regulation Deliver High Data Quality in European Courts?

When AI- generated information becomes evidence, the court must assess data quality in areas where it lacks conventional standards, e.g. ‘correctness’ or “representativeness”.



In a European courtroom, the **bench acts as gatekeeper**, based on a rather vague “reliability test” for evidence, that today lacks generally recognized criteria for “data quality” (beyond GDPR).

As a rule: All relevant evidence is admissible. Reliability is based on the weight of the evidence, not the admissibility. Whether evidence is persuasive or not is a question for the trier of facts (being the jury in the U.S. or bench judges in Europe).
As an exception: untrustworthy evidence is excluded, like, for instance, observations that cannot be discredited through “confrontation”.

4 Will the EU Regulation Deliver High Data Quality in European Courts?

A Functional Legal Approach

(1) **legal systems face similar problems**: *AI systems become sort of witness without a meaningful reliability test*;

(2) **for the same problem, different legal systems take different legal measures**, e.g.
- *regulate technology?*
EU approach aims for regulation furnishing "trustworthy AI"
- GDPR
- AI Act
- *modify re-interpret procedural rules if necessary?*
U.S. approach aims for
(a) re-inventing tried principles, like the confrontation clause, for AI-evidence;
(b) introduce new rules specifically tailored for scrutinizing AI evidence.

(3) **despite differing measures, legal systems reach similar results, *but of different form***.

5 A Comparative Outlook

Despite its regulation aiming for trustworthy AI,
Europe has to overcome more hurdles for ensuring evidence based on quality data,
because it lacks the “evidentiary toolkit”, e.g.

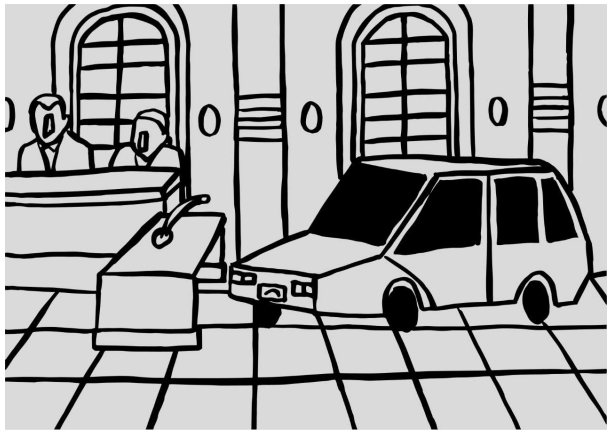
U.S. Federal Rules of Evidence, Rule 403

The court may exclude relevant evidence if its probative value is substantially outweighed by a danger of one or more of the following: unfair prejudice, confusing the issues, misleading the jury, undue delay, wasting time, or needlessly presenting cumulative evidence.

No such rule in German or Swiss Criminal Procedure (or NL)

as the bench is the trier of facts and judges are expected to be “professionals”.

5 A Comparative Outlook



In Europe,
the bench as the ‘trier of fact’
decides whether evidence is to be
excluded from its own knowledge.

Thus, “admissibility of evidence” is more a slogan than a substance, or phrased differently,

In Europe, trustworthy evidence may depend on the judges’ morning commute to court.”

Thank you.

Sabine.Gless@unibas.ch

Trustworthy Evidence - A dog?

e.g., Germany:

Results produced by tracker dogs
("scent trace matching dogs") may be used,
as evidence for the presence of a suspect
at the scene of a crime, but only if the following conditions are met:

1. Dogs must be trained for «scent trace matching» in a standardized program.
2. The “scent trace” used must be clearly traceable to a specific person. The process must be documented in a protocol.
3. Two tracker dogs must independently come up with identical results, without involvement of the same dog handler.
4. Each operation must be recorded in order to enable the court, parties and/or expert witness to vet the plausibility of the results.
   Landgericht Nürnberg-Fürth, Urteil vom 13.12.2012 - 13 KLs 372 Js 9454/12