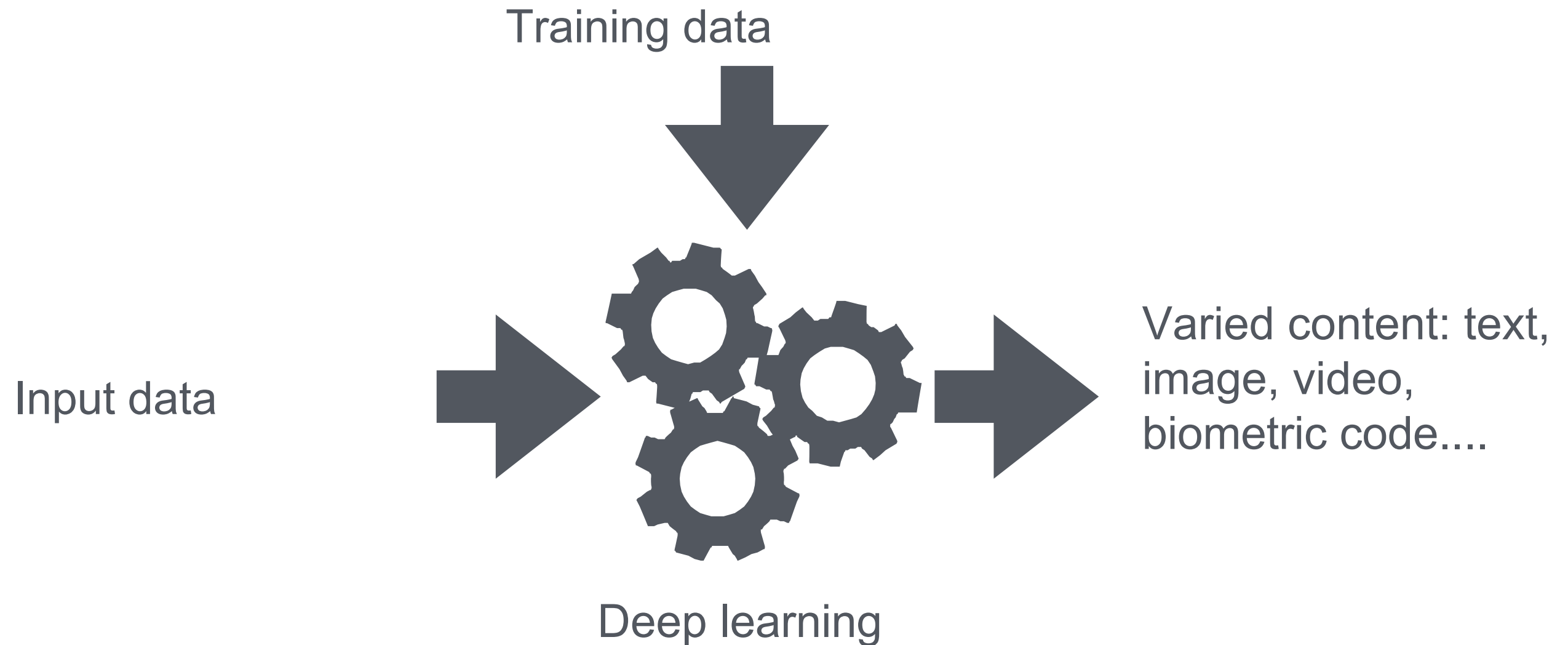


The presumption of innocence put to the test by AI

The presumption of innocence challenged by AI evidence

Generative AI



- Autonomous operation: black box
- Choice and quality of training data
- Results: probabilities, margin of error

Proof through AI

- The truth or a truth?
- Aimed at convincing the judge
- Respect for the presumption of innocence?
- Exercising the rights of the defence?

Presumption of innocence

A principle with constitutional value

- Article 9 of the 1789 Declaration of the Rights of Man and of the Citizen
- Universal Declaration of Human Rights 1948
- Art 14§2 International Covenant on Civil and Political Rights
- Art. 48§1 EU Charter of Fundamental Rights
- Art. 6§2 European Convention on Human Rights
- Linked to the exercise of the rights of defence (ECHR 25 March 1983 Minelli v Switzerland req. no 8660/79)
- Linked to the right to remain silent and not to incriminate oneself (Directive (EU) 2016/343 of the European Parliament and of the Council of 9 March 2016 strengthening certain aspects of the presumption of innocence and the right to be heard in criminal proceedings).

Plan

(Analysis limited to facial recognition)

I. AI makes it easier to prove guilt

A/ The lawfulness of AI evidence

B/ The probative value of AI evidence

II. Towards a requirement for proof of innocence?

A/ The presumption of truth induced by AI evidence

B/ The difficulty of proof to the contrary

I. AI makes it easier to prove guilt

New form of imbalance without a priori questioning of the burden of proof

Chasing party:

- AI = richer, faster, more powerful, more accurate evidence



Party sued

- Presumption of innocence
:
 - Exercise of rights of defence
-
- Legality of AI evidence?
 - Probative value of AI evidence?

A/ The lawfulness of AI evidence

Data Protection Act

- Law no. 78-17 of 6 January 1978 on data processing, data files and individual liberties + RGPD + "Police-Justice" Directive
- Principle prohibiting automated processing of biometric data to uniquely identify a person
- Exception "for the prevention, detection, investigation and prosecution of criminal offences" (art. 87)
- Conditions: competent authority designated, legislative or regulatory framework, authorisation by decree of the Council of State after published opinion of the CNIL.
- "only in cases of absolute necessity, subject to appropriate safeguards for the rights and freedoms of the data subject" (art. 88)

A/ The lawfulness of AI evidence

Code of Criminal Procedure

- Articles 230-6 to 230-11, R. 40-23 to R. 40-34 CPP
- Facial recognition based solely on data from the criminal records file (TAJ)
- Article R. 40-26 CPP: allows for the recording of "photographs with technical characteristics enabling the use of a facial recognition device (facial photograph)" of suspects or deceased or missing persons under investigation.

A/ The lawfulness of AI evidence

Validation by the Conseil d'Etat

- Conseil d'État, 26 Apr. 2022, no. 442364
- Conditions: "the facial recognition system may be used by the competent services **only in cases of absolute necessity**, assessed solely in the light of the purposes of the processing, **where there is doubt as to the identity of a person** whose identification is required".
- First manual identification by a human? Control of subsidiarity of use? Check that the probabilistic result has been confirmed by a human (Lyon Correctional Court 31/10/2019 which emphasises confirmation by an investigator).
- Possibility of main use according to the Conseil d'Etat: "In view of the number of suspects recorded in this processing, which amounts to several million, **it is materially impossible for the competent officers to carry out such a comparison manually, (...)**".

A/ The lawfulness of AI evidence

Legality of input data

- Rouen, Aliens Chamber, 18 October 2022 - no. 22/03388: the person concerned claimed to be a minor and refused to be identified. A photograph taken of her without her knowledge was subjected to the TAJ facial recognition algorithm, which provided a 68% probability of a match with a person of full age.
- The problem of 'passive' technology in the face of freely available images on networks
- However, Article 88 of the Data Protection Act authorises the use of data "manifestly made public by the data subject": problem of the extent of consent when published on the Internet?
- Clearview case: company sanctioned in October 2022

B/ The probative value of AI evidence

Intelligible proof

- The black box of self-learning algorithms
- Results with error rates, probabilities
- To what extent does poor intelligibility reduce probative value?

B/ The probative value of AI evidence

Reliable proof - reliability of AI tools

- Presumption of reliability of facial recognition: "In view of the number of suspects recorded in this processing, which amounts to several million, it is materially impossible for the competent officers to carry out such a comparison manually, moreover with the **same degree of reliability as that offered by a properly parameterised facial recognition algorithm**". Conseil d'État, 26 Apr. 2022, no. 442364, point 5.
- The issue of parameter control and independent certification of the tool: very opaque

B/ The probative value of AI evidence

Reliable evidence - reliability of input data and results

- Impact of the quality of the input data on the results provided
- TAJ parameterised to provide a maximum of 200 matches with a rate of 40 to 100% (Senate report no. 627 of 10 May 2022)
- What is the threshold for considering that the result provides a plausible identification that does not allow doubt in a system of free evidence?
- Rouen, Aliens Division, 18 October 2022: "The appellant's counsel explained that the appellant was a minor. The police carried out a facial recognition, using the TAJ file, and the judge noted (in a 'shameful' way) that there was a 68% chance that it was her, but there was therefore a two out of three chance of being wrong." = false positive?

B/ The probative value of AI evidence

Consequences of relying on AI evidence

- Two examples: whatever the probability, identification has influenced the rest of the procedure.
 - Rouen, Aliens Chamber, 18 October 2022: procedure applicable to adults with a 68% similarity between the person concerned and an adult.
 - Rennes, Foreigners' Chamber, 27 January 2023 - no. 23/00055: on the basis of a photograph of a person "identified by facial recognition as being Mr [G], that this identification made it possible to recognise him in the street, to obtain authorisation from the Public Prosecutor to arrest him on the public highway, to apply the provisions of article 78 of the Code of Criminal Procedure, to place him in police custody and then to renew the custody".

Plan

(Analysis limited to facial recognition)

I. AI makes it easier to prove guilt

A/ The lawfulness of AI evidence

B/ The probative value of AI evidence

II. Towards a requirement for proof of innocence?

A/ The presumption of truth induced by AI evidence

B/ The difficulty of proof to the contrary

Presumption of innocence

The point of view of the suspected or accused party



A/ The presumption of truth in AI evidence

Reversal of the burden of proof

- Rouen, Aliens Division, 18 October 2022: The Prefect invoked the fact that, while in police custody, "Mrs [O] refused to have her photograph and fingerprints taken, **which may suggest that she is known as an adult**" and stated that "it is **up to the appellant declaring herself to be a minor to prove her minority by any means**". The court considered that although the facial recognition showed a 68% similarity with a person of full age, the appellant "did not provide any evidence in favour of her minority, nor any evidence likely to counter the evidence of her majority established during the proceedings".
- Respect for the right not to incriminate oneself to be reconciled with this requirement
- Reasonable doubt?

B/ The difficulty of proof to the contrary

- The right not to incriminate oneself
- Proof of negative fact
- No access to the AI's technical operating data: insufficient evidence to challenge its operation
- Need for an expert appraisal, but for what result?
- No requirement for transparency of algorithms used in criminal proceedings in the Data Protection Act (Title III), only a guarantee to report operating errors and data integrity (art. 99).

B/ The difficulty of proof to the contrary

Consequences for decisions in criminal proceedings

- Article 47 of the French Data Protection Act: "No decision having legal effects on a person or significantly affecting him or her may be taken solely on the basis of automated processing of personal data" but covered by Title II (RGPD) **not applicable** to the processing of personal data for the purposes of the prevention, investigation, detection and prosecution of criminal offences (art. 42).
- Art. 95: prohibition of individual decisions based on automated processing of personal data only if the processing is intended to anticipate or evaluate certain personal aspects relating to the data subject: does not concern facial recognition, which identifies the data subject.

Conclusion

- Facial recognition calls into question a "classic" application of the presumption of innocence
- A useful tool
- To what extent and how can guarantees be strengthened?

Thank you for your
attention