Facial recognition technology and protection of fundamental rights

Raphaël Déchaux

Co-funded by the
Erasmus+ Programme
of the European Union

FACIAL RECOGNITION TECHNOLOGY AND PROTECTION OF FUNDAMENTAL RIGHTS

Raphaël Déchaux

Lecturer in Public law

Facial recognition technology (FRT)

Increased *computing power* (Deep-Learning)
Increased *data access* (pictures)

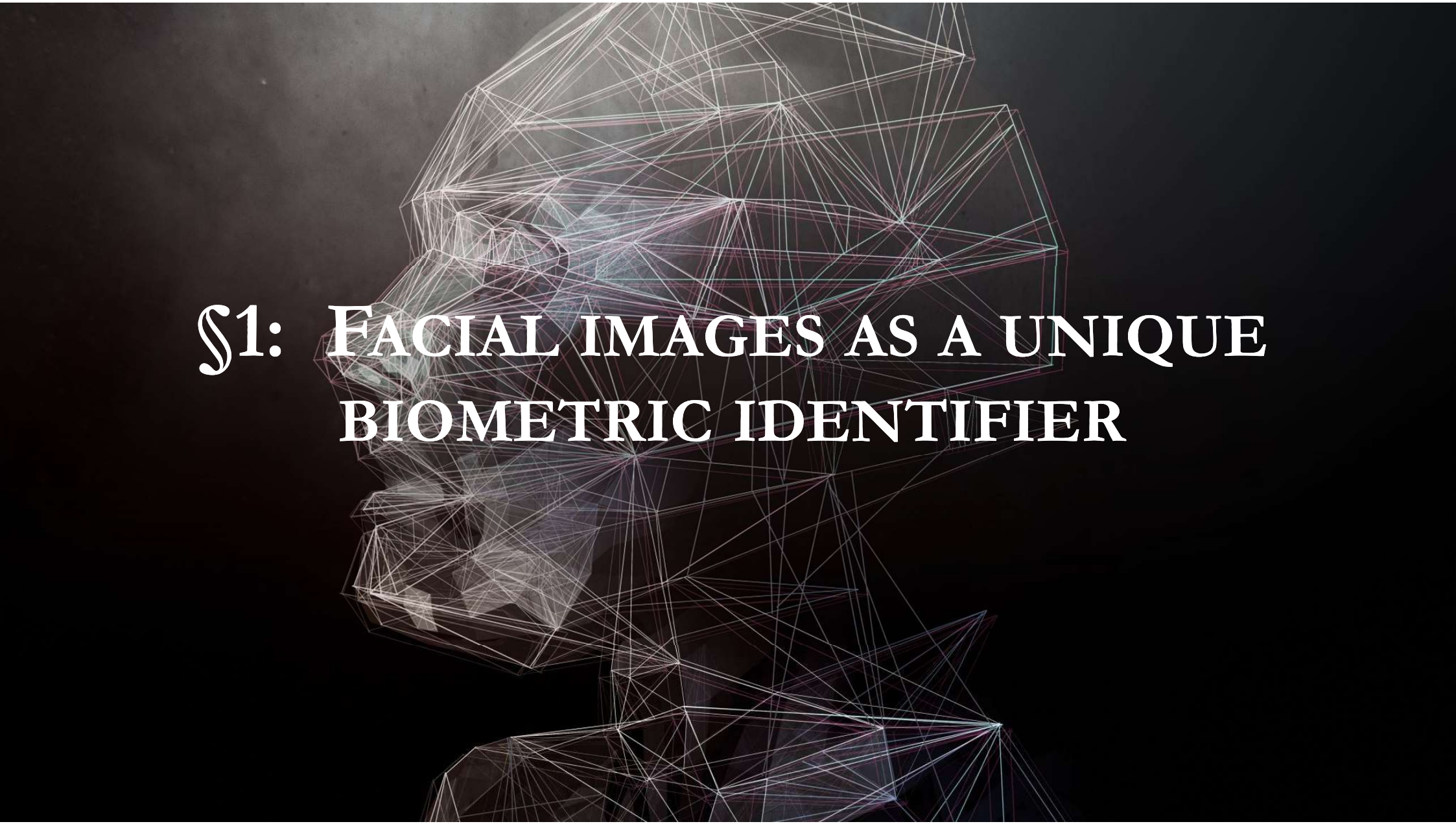
3 QUESTIONS

Part 1: What is facial recognition?

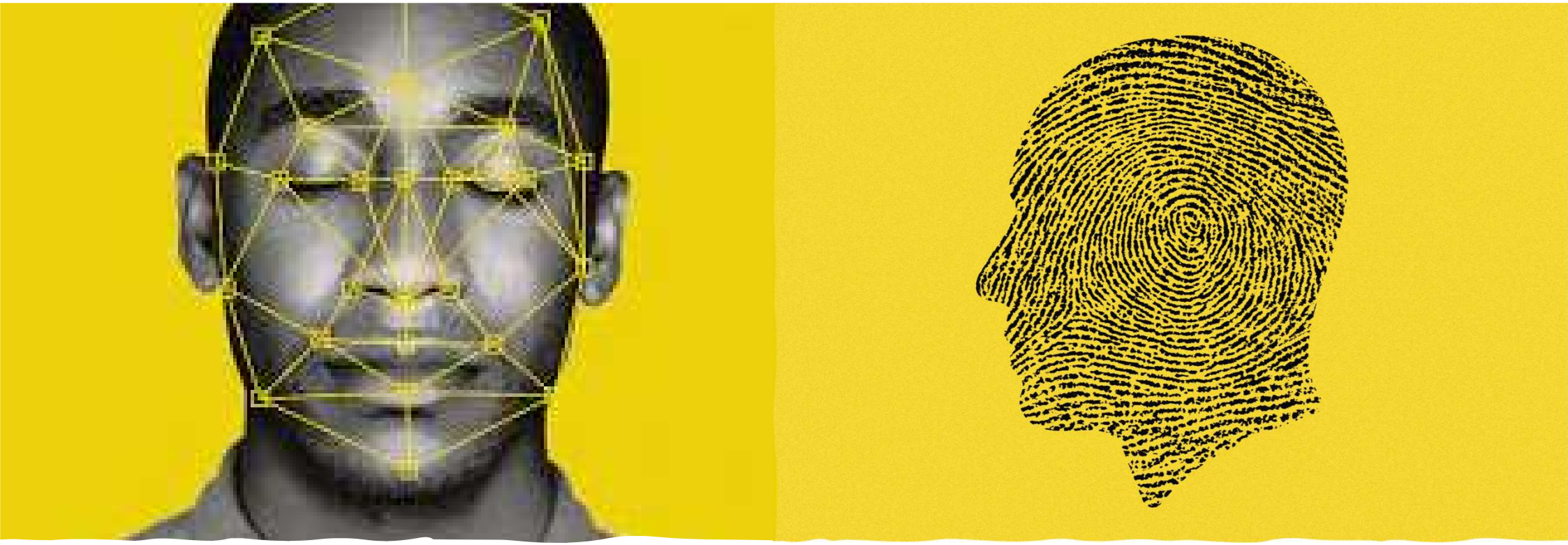
Part 2: What are the potential harms for human rights?

Part 3: What is the position of the European regulation?

Part 1:
What is facial recognition?



§1: Facial images as a unique biometric identifier



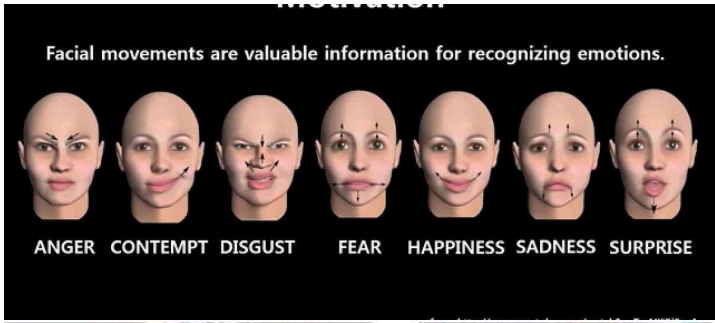
FRT = identification system

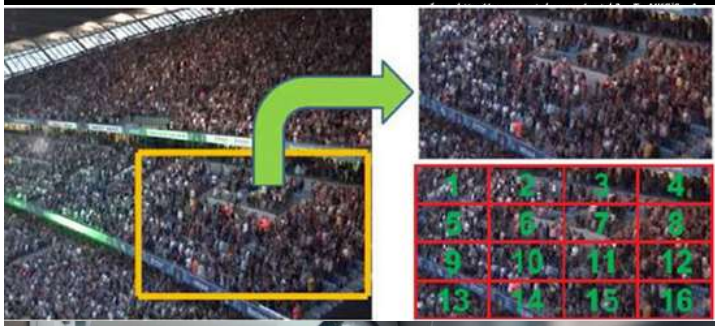
The three kinds of recognition

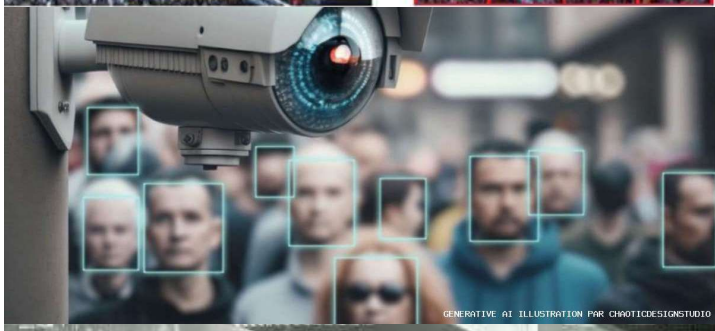
- ***Verification*** or authentication : one-to-one matching (Automated Border Control)
- ***Identification*** : the FRT returns a *score* for each comparison indicating the likelihood that two images refer to the same person.
  - Automated Facial Recognition (AFR)
  - Live Facial Recognition Technology (LFRT)
- ***Categorisation*** the technology is not used to identify or match individuals, but only characteristics of individuals, for example, sex, age, or race.

The three uses of FRT

- **Personal** : identification or verification (most common)
- **Emotional** : could read human émotions (quackery)
- **Behavioral**: "physiognomonic" FRT (behavioral categorization) : crowd control.







§2: The applications of FRT

In the public sector

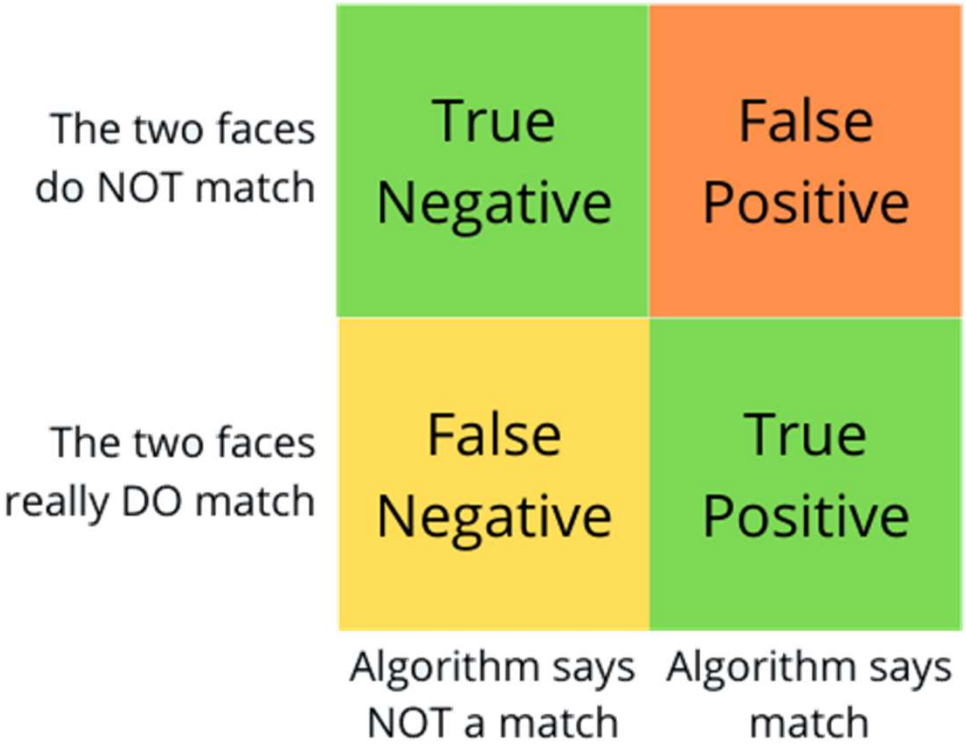
In the private sector

Part 2:
What are the potential harms for human rights ?

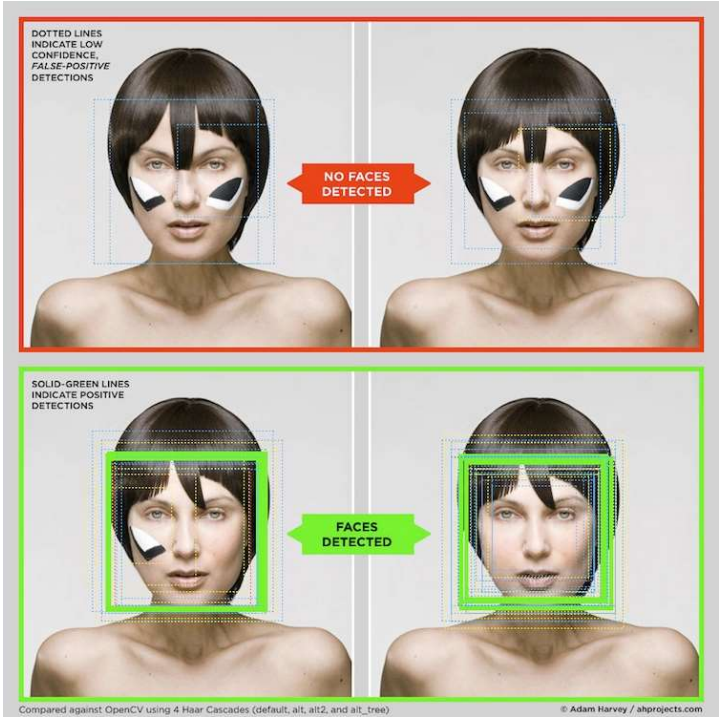
§1: The risks of FRT malfunctioning

False facial recognition

- **False positive**: situation where an image is falsely matched to another image on the watchlist
- **False negatives**: situation where the images deemed not to be matches, but in fact are matches

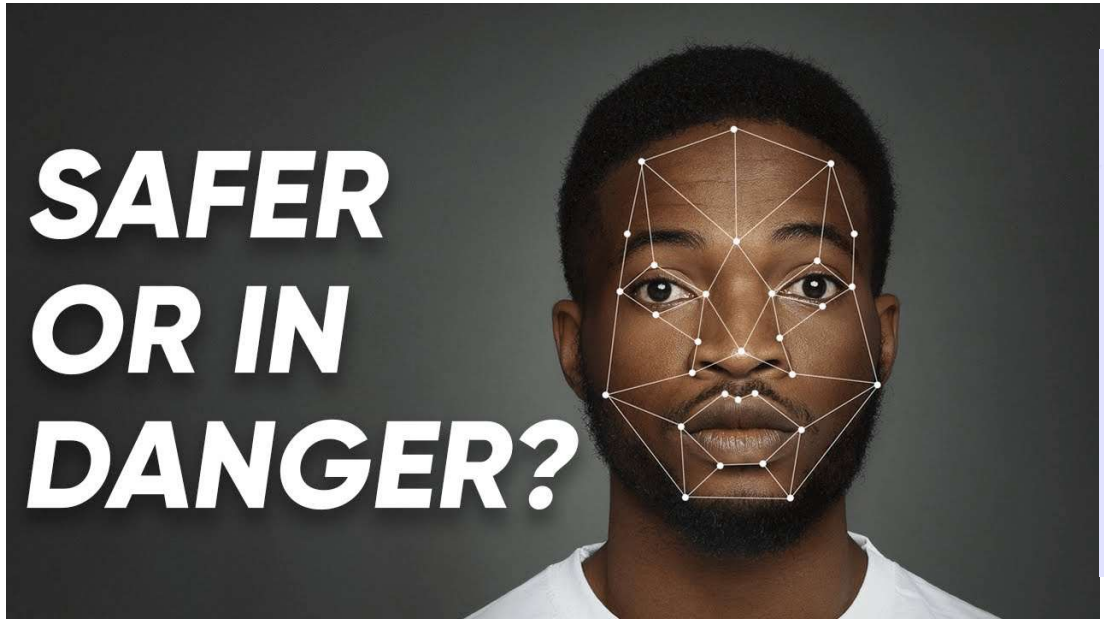


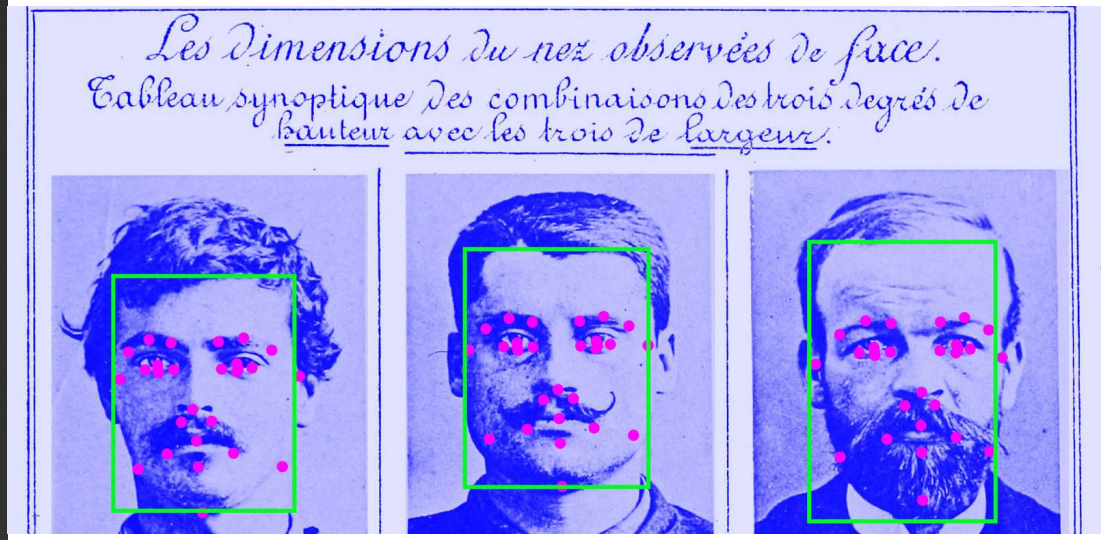
A question of quality of facial images ?



§2: From digital government to generalized surveillance

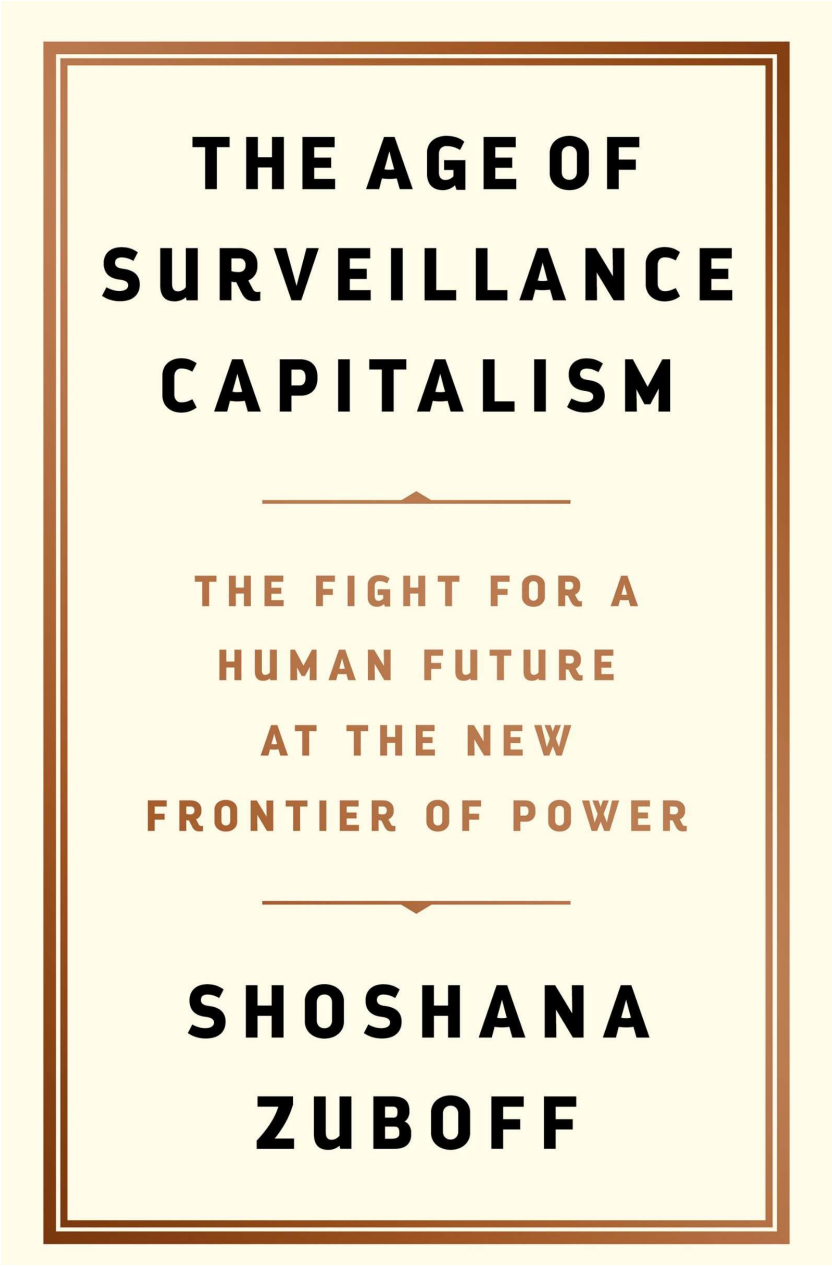
FRT is the new Bertillonage

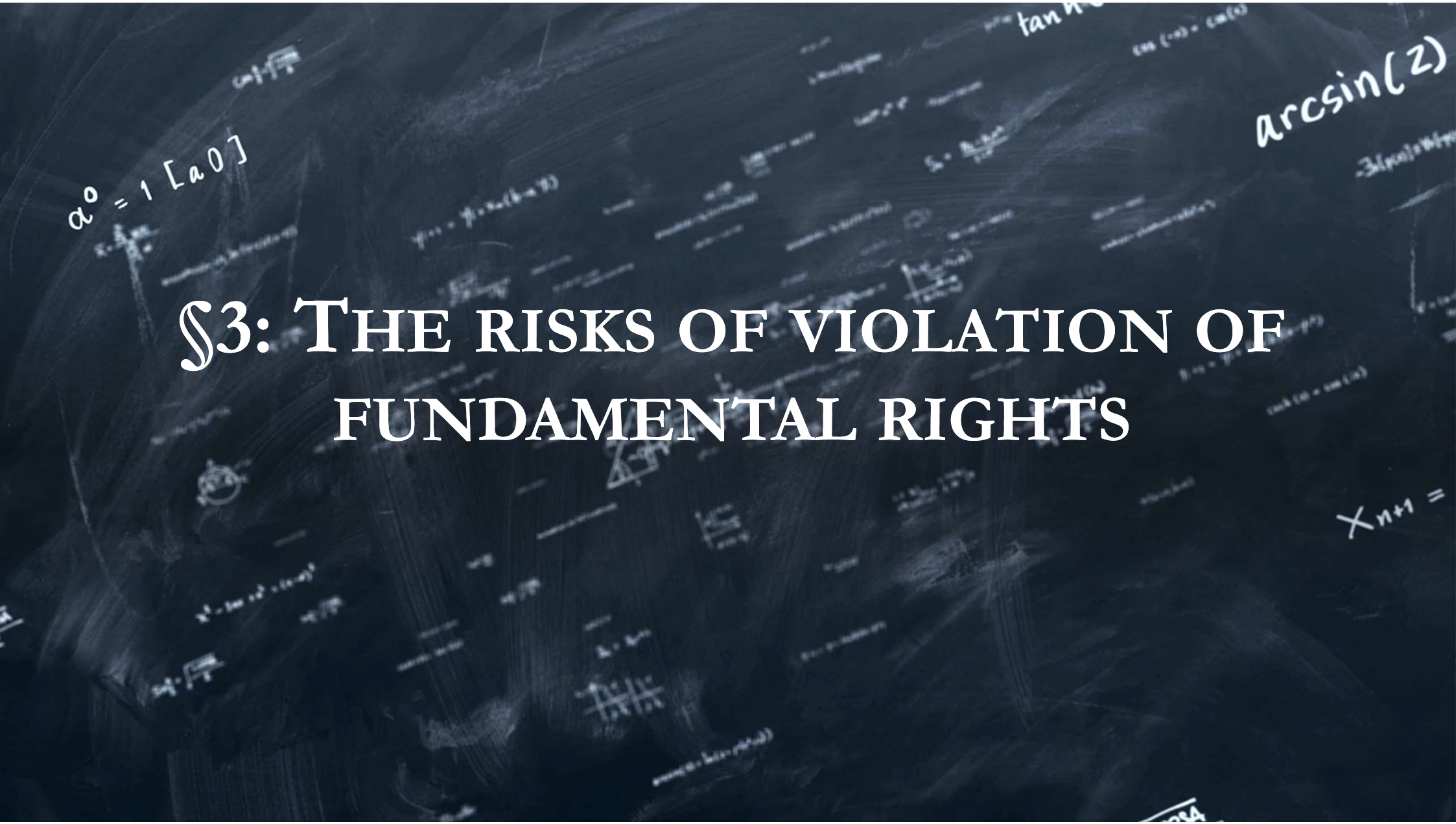




Toward a general surveillance society

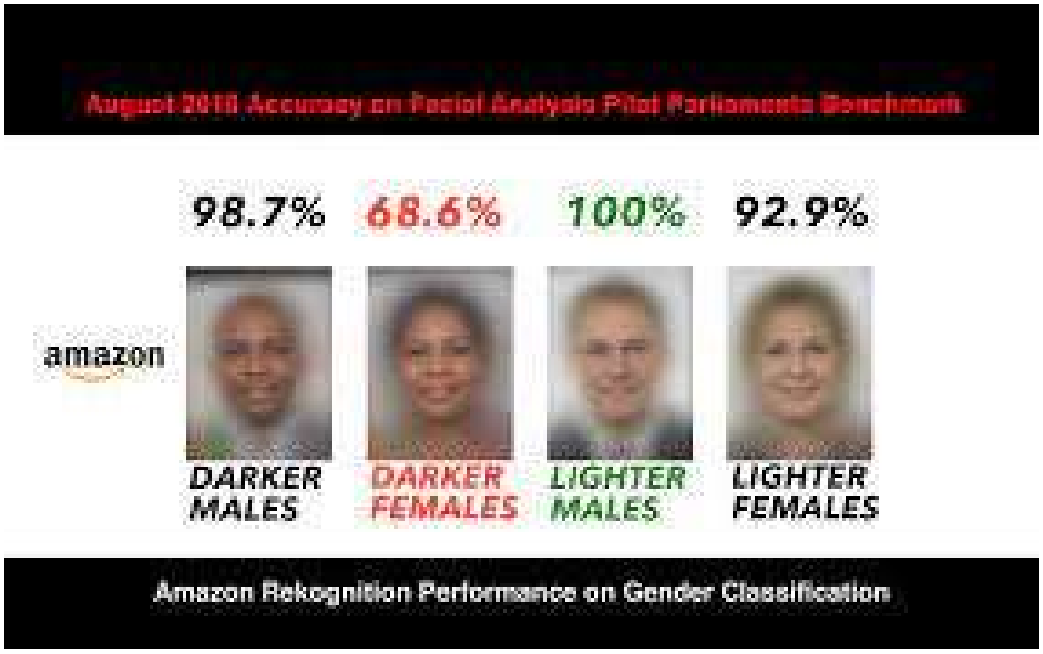
- CJEU, GC, *Tele2*, 21 December 2016, C-203/15, C-698/15
- ECrHR, *Glukhin v. Russia*, 4 July 2023, n° 11519/20
- CC, *Olympic Games Act*, 17 May 2023, 2023-850 DC

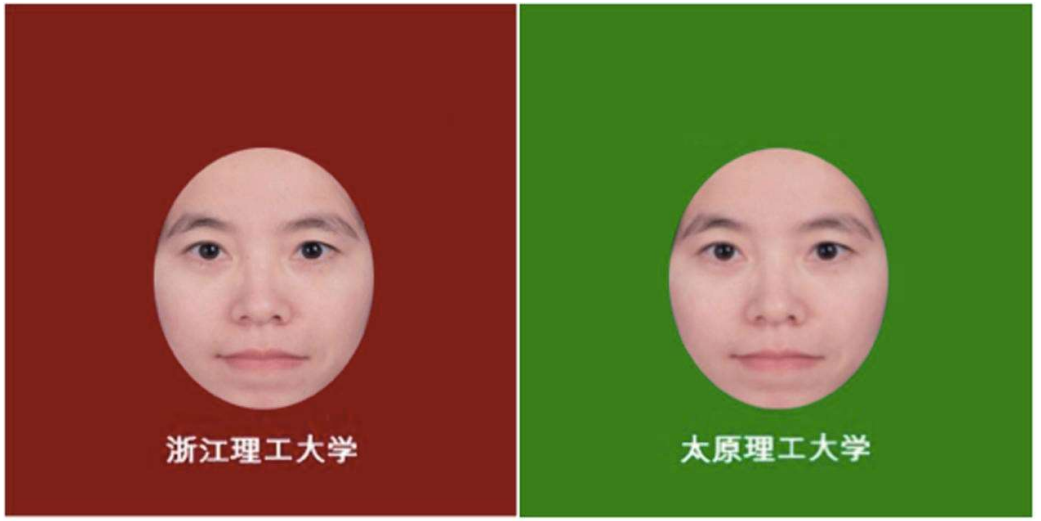




§3: The risks of violation of fundamental rights

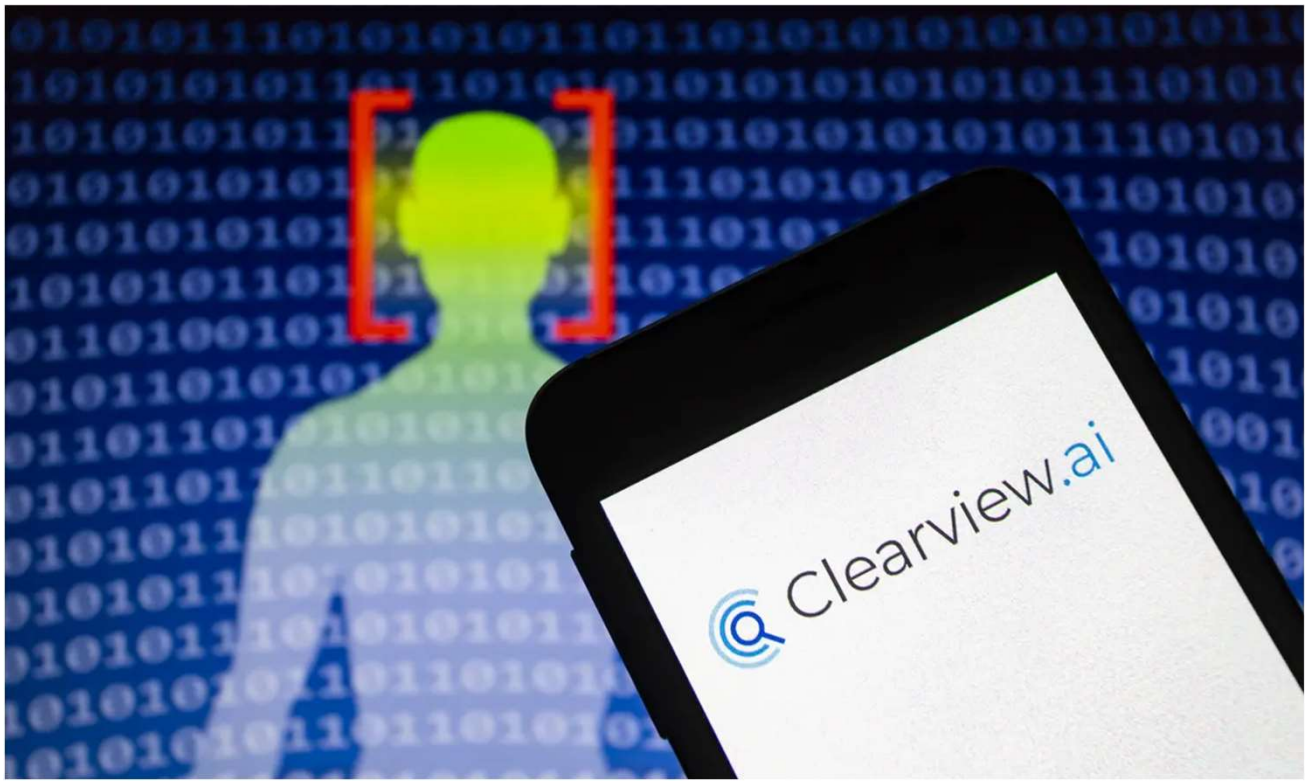
Discrimination issue





Privacy issues

- ECrHR, *Glukhin v. Russia* : increased risks when combined with political data => "heightened level of protection" (*Olsson v. Sweden* – 1988)
- GDPR: facial images fall into the 'special categories of personal data'
- Where the dataset comes from ?



Clearview.ai

€20 Million GDPR Fine

Clearview AI scandal

JNLF 2022 STRASBOURG 12 au 15 avril

Other fundamental principles

- ***Proportionality***
  - restricted to prevention or resolution of the most serious crimes.
- ***Transparent and clear provision of information***
- ***Freedom of expression and freedom of assembly and of association***
  - Prohibition to use facial recognition for political reasons

Part 3:
What is the position of the European regulation on facial recognition?

The need for european legal regulation

No domestic regulation : Italian memorandum (31 December 2021).

Why should international regulation be "better" or "more effective" than national regulation?

- globalization of the digital economy
- context of international competition

§1: The Council of Europe's approach

The Council of Europe's approach

- Right to transparency (art. 8)
- Right not to be subject to a unilateral decision (art. 9,1a).
- Right to obtain knowledge of the reasoning (art. 9,1c).

Guidelines on facial recognition

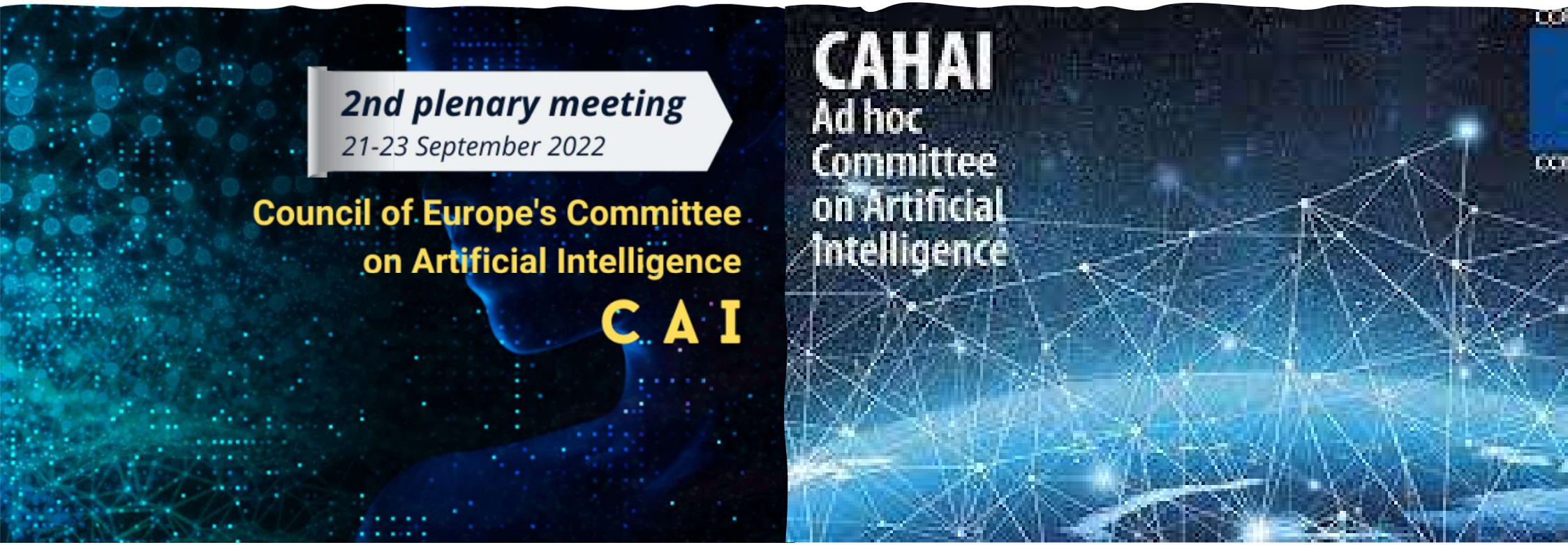
Consultative Committee of the Convention for the protection of individuals with regard to automatic processing of personal data

Convention 108

COUNCIL OF EUROPE

CONSEIL DE L'EUROPE

Convention on Artificial Intelligence



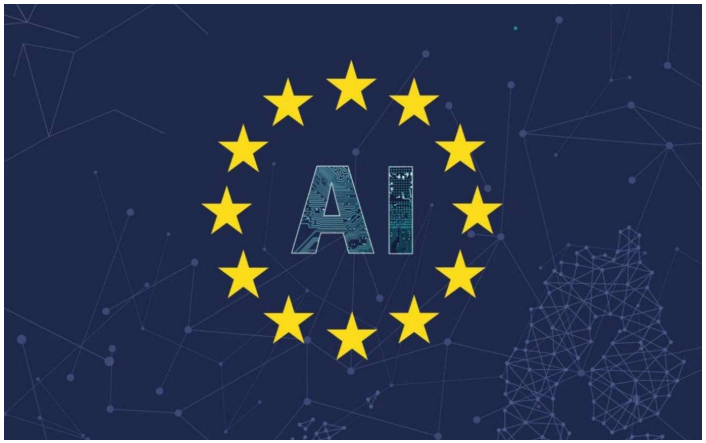
§2 The EU's approach

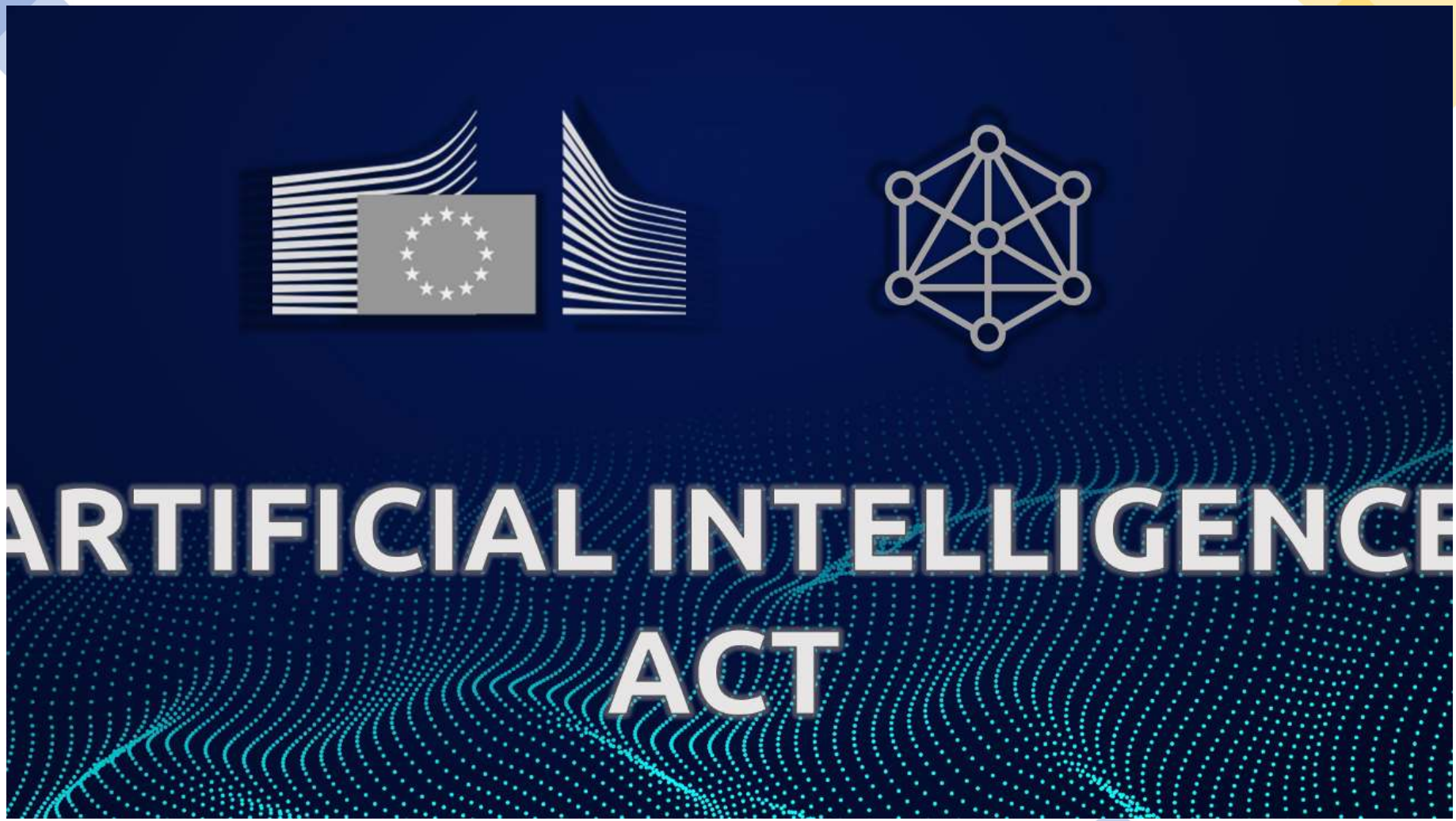
EU soft law

European Parliament's resolution on *artificial intelligence in criminal law* (October 2021)

European Data Protection Board, *opinion* (June 2021)

European Union Agency for Fundamental Rights



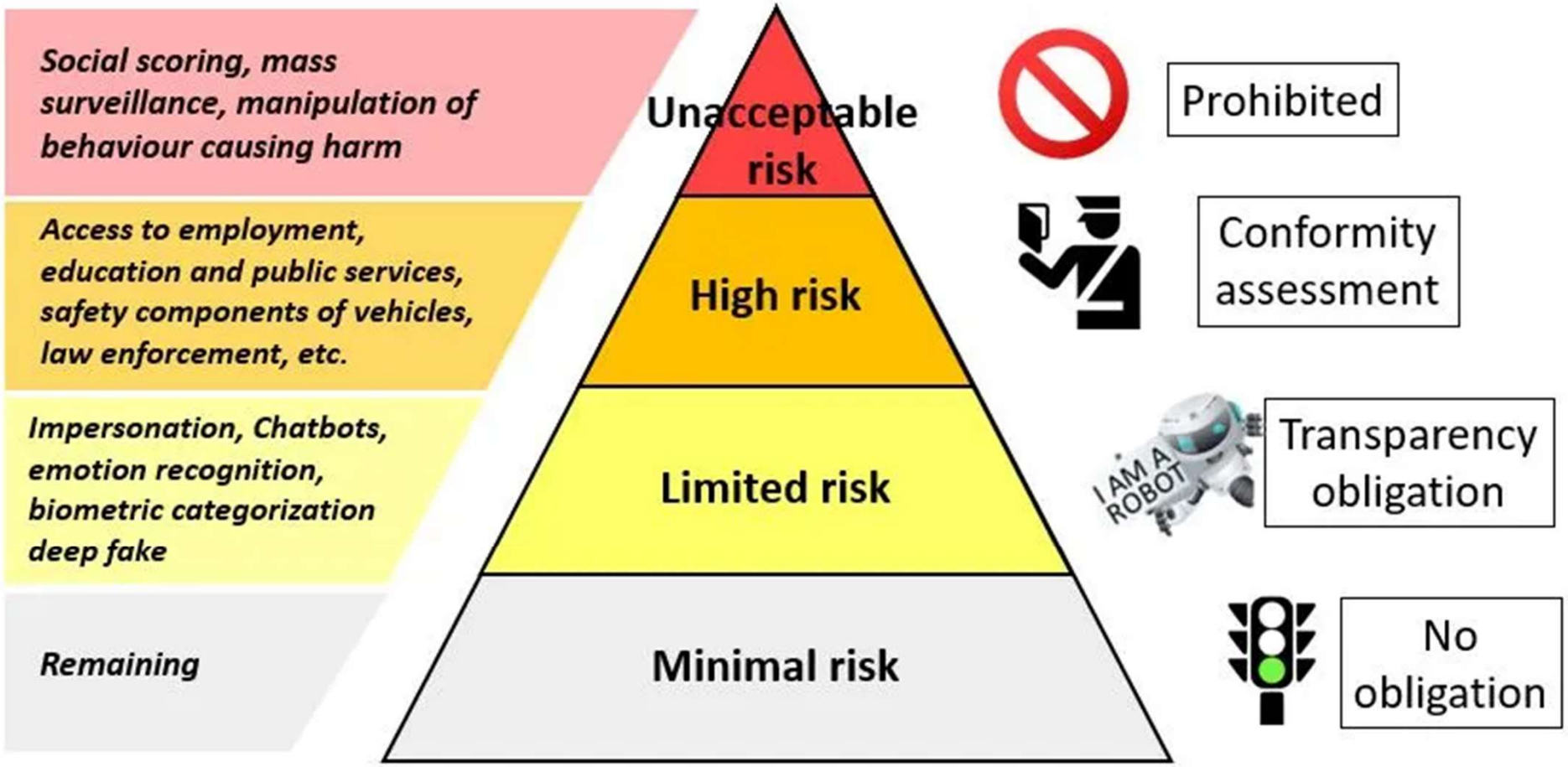

ARTIFICIAL INTELLIGENCE
ACT

2) The AI Act

Key dates

- 14 June 2018 : Independent High-Level Expert Group on Artificial Intelligence
- 19 February 2020 : White paper
- 2 October 2020 : Decision of the European Council
- 21 April 2021 : AI Act draft, start of the discussion in the EU Council
- 25 January 2022 : start of discussions in the EP.
- 14 June 2023 : Adoption of the draft by the EP
- Décember 2023 : political agreement
- 2 February 2024: adoption by the EU Council
- 13 Mach 2024: final adoption by the EP

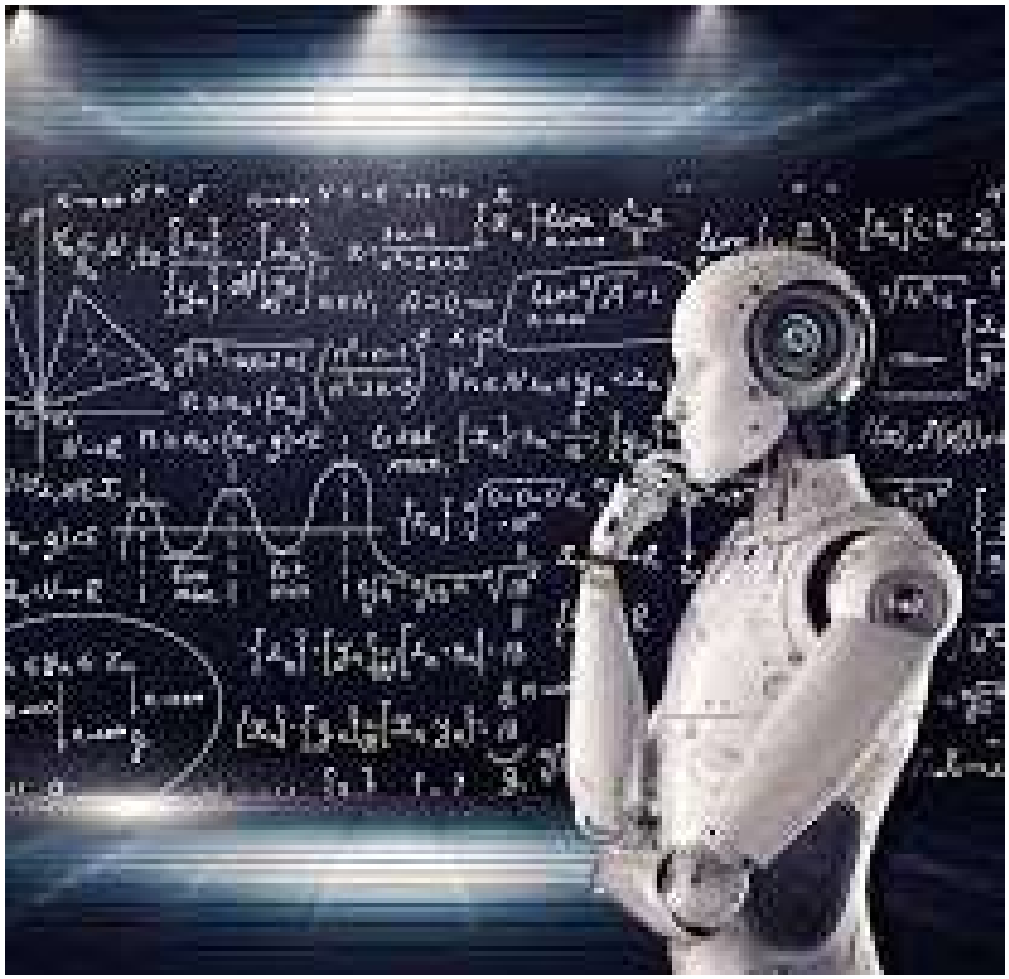
EU Artificial Intelligence Act: Risk levels



Needs for a CE label

1) The facial recognition systems included in the high risk group

- Remote biometric identification systems, excluding biometric verification that confirm a person is who they claim to be.
- Biometric categorisation systems inferring sensitive or protected attributes or characteristics.
- Emotion recognition systems.
- For migrations, asylum and border control management, AI that are detecting, recognising or identifying individuals, except verifying travel documents.



2) The facial recognition systems included in the ban group

- If FRT is compiling facial recognition databases by untargeted scraping of facial images from the internet or CCTV footage.
- If FRT is inferring emotions in workplaces or educational institutions, except for medical or safety reasons.
- If FRT is in 'real-time' remote biometric identification (RBI) in publicly accessible spaces for law enforcement.

Thank you for your attention…