



HAL
open science

Facial recognition technology and protection of fundamental rights

Raphaël Déchaux

► **To cite this version:**

Raphaël Déchaux. Facial recognition technology and protection of fundamental rights. Doctoral. Rights and Democracy: The Multilevel Protection of Fundamental Rights and the Role of Constitutional and European Courts, Onlince Conference, France. 2024. hal-04566971

HAL Id: hal-04566971

<https://amu.hal.science/hal-04566971v1>

Submitted on 2 May 2024

HAL is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L'archive ouverte pluridisciplinaire **HAL**, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d'enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.



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?

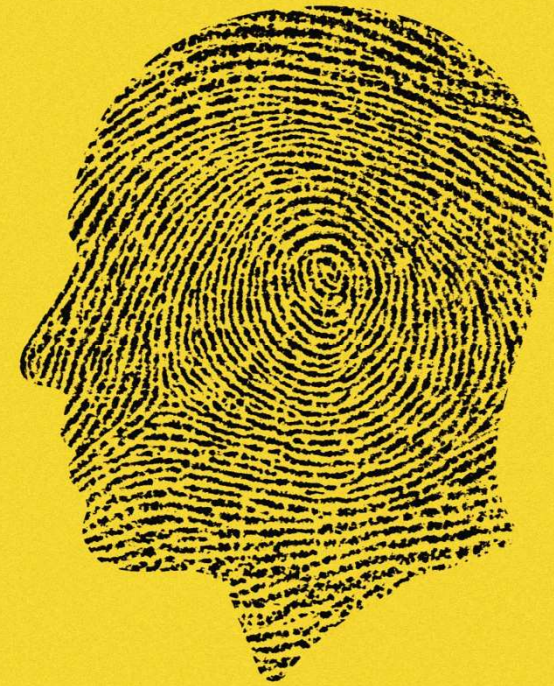
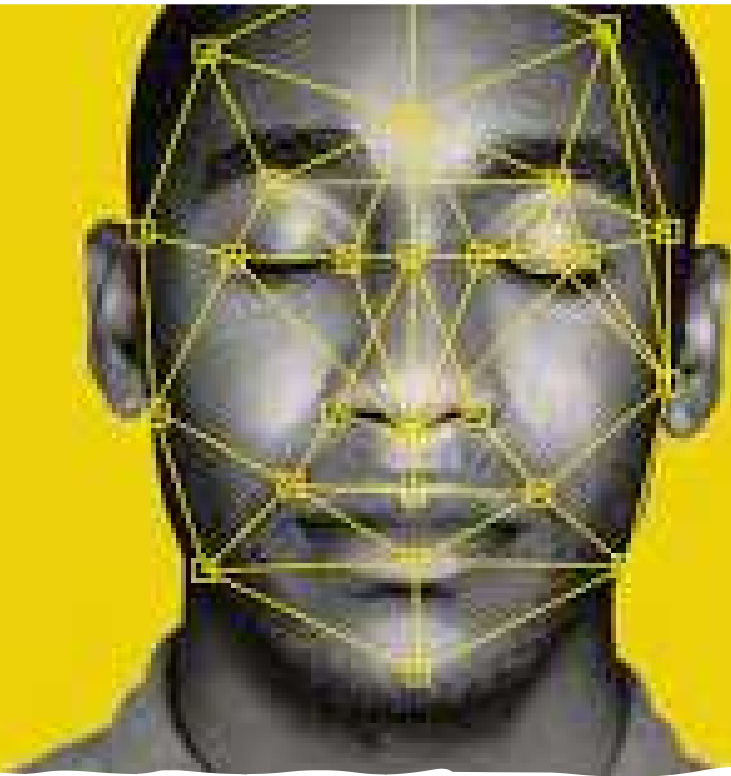
Part 3: What is the position of the European regulation?



PART 1:
WHAT IS FACIAL RECOGNITION?



**§1: FACIAL IMAGES AS A UNIQUE
BIOMETRIC IDENTIFIER**



FRT = identification system

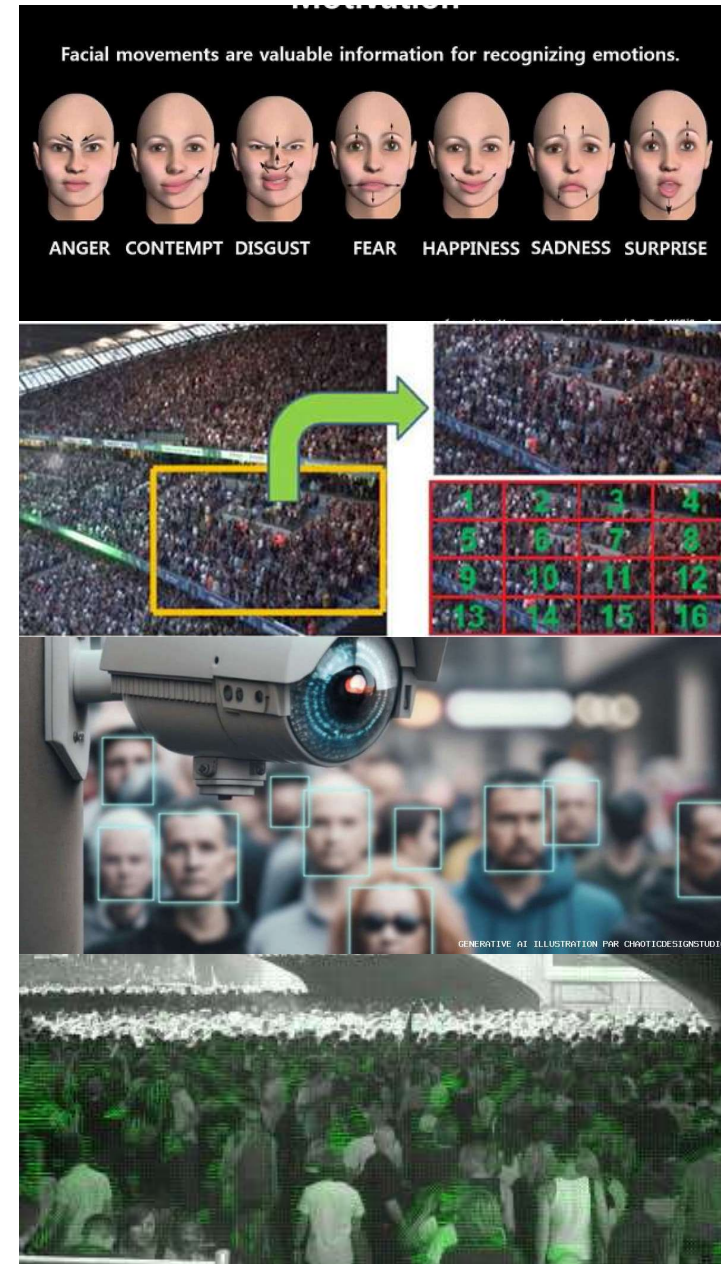
The three kinds of recognition

- **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 emotions (quackery)
- **Behavioral**: “physiognomonic” FRT (behavioral categorization) : crowd control.



An abstract, complex geometric structure composed of numerous interconnected white and light-colored lines, forming a dense, multi-faceted mesh. The structure is set against a dark, almost black background, which makes the lines stand out prominently. The overall appearance is that of a digital or mathematical construct, possibly representing a network or a complex data structure.

§2: THE APPLICATIONS OF FRT



In the public sector



In the private sector



Face recognition



To ensure the quality of the premise, according to customer feedback, the function of a comprehensive optimization, more humane upgrade



Multi-language



Verification



3 level user rights



Face recognition

PART 2:
**WHAT ARE THE POTENTIAL HARMS
FOR HUMAN RIGHTS ?**



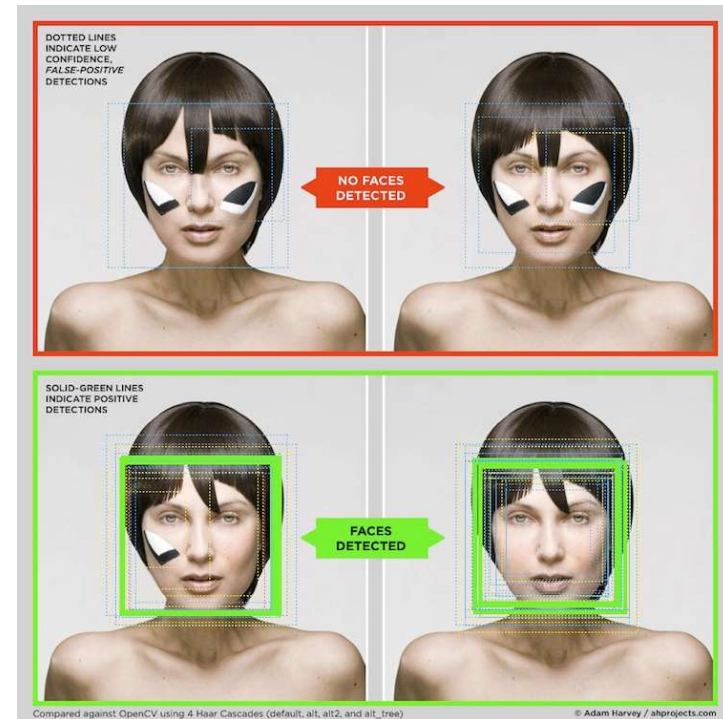
§1: THE RISKS OF FRT
MALFUNCTIONING

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

The two faces do NOT match	True Negative	False Positive
The two faces really DO match	False Negative	True Positive
	Algorithm says NOT a match	Algorithm says match

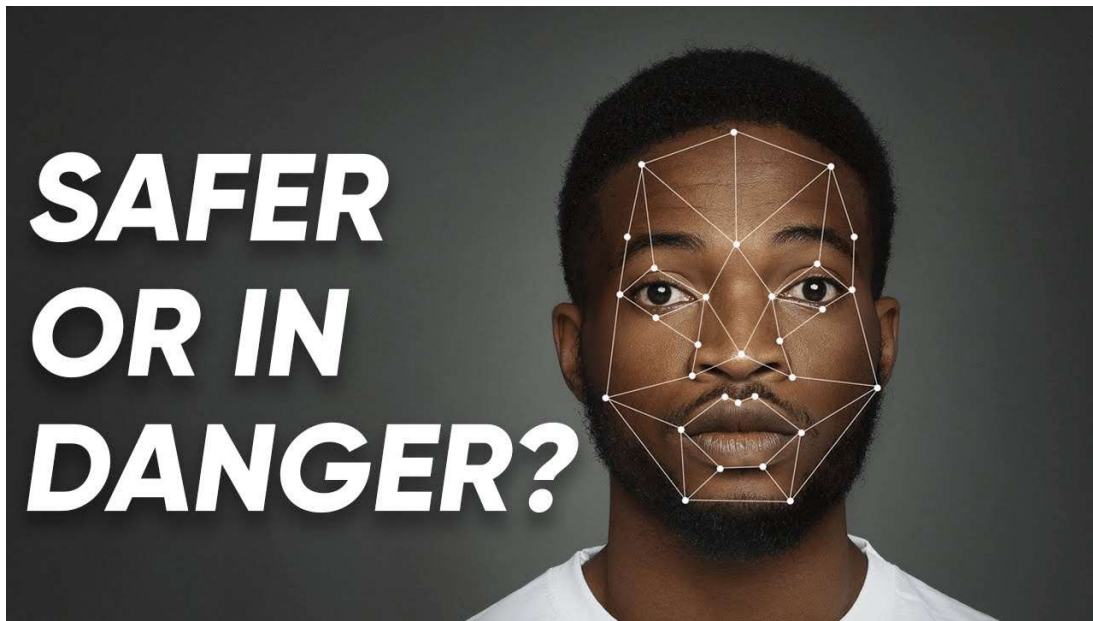
A question of quality of facial images ?





§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

THE AGE OF SURVEILLANCE CAPITALISM

THE FIGHT FOR A
HUMAN FUTURE
AT THE NEW
FRONTIER OF POWER

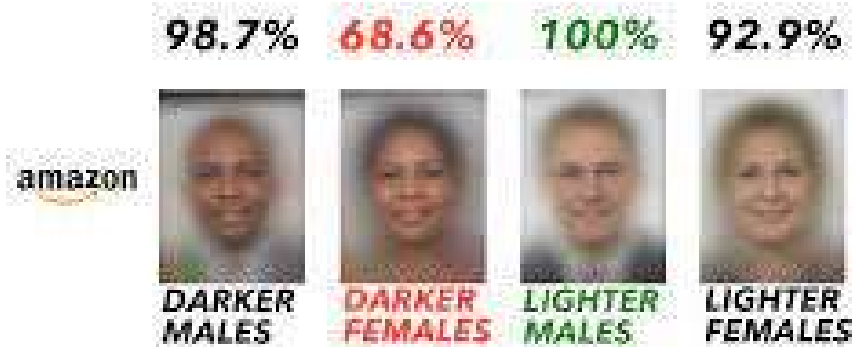
SHOSHANA
ZUBOFF



§3: THE RISKS OF VIOLATION OF
FUNDAMENTAL RIGHTS

Discrimination issue

August 2018 Accuracy on Facial Analysis Pilot Parliaments Benchmark



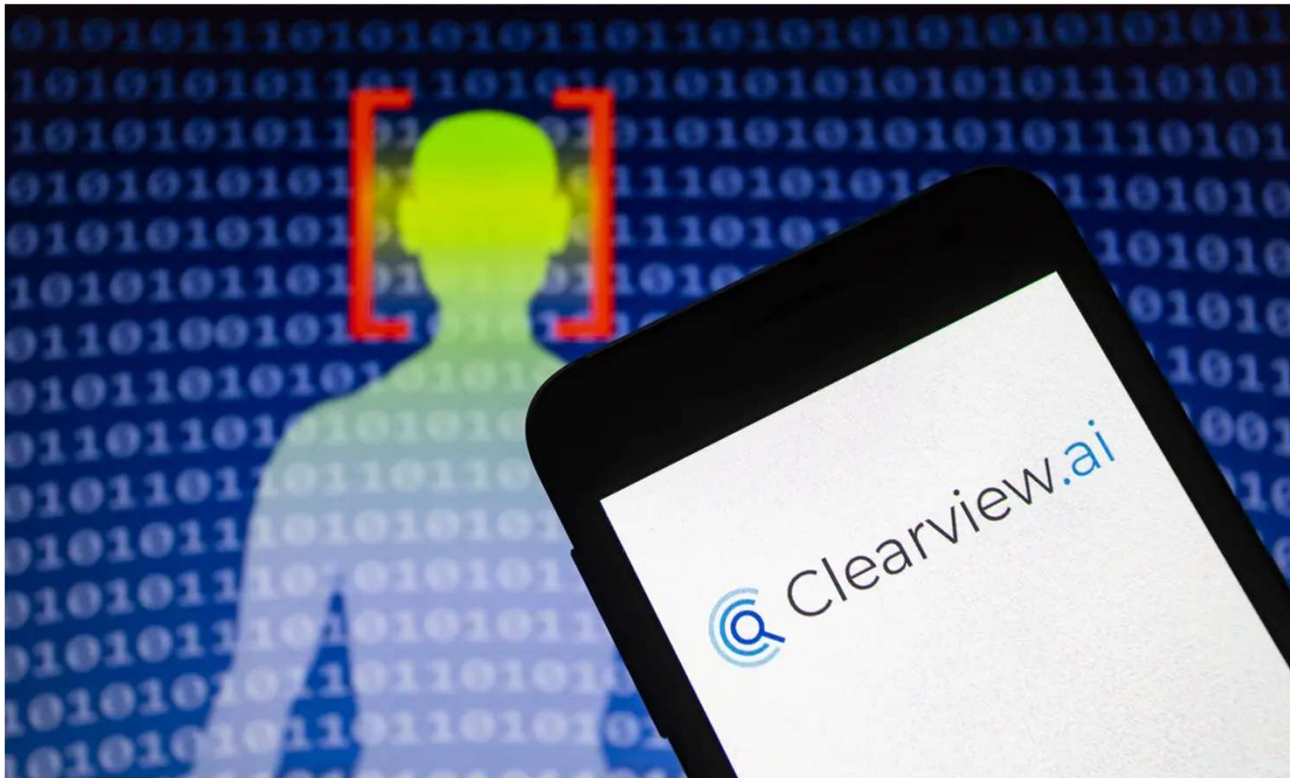
Amazon Rekognition Performance on Gender Classification



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**



**ClearviewAI has 10
BILLION images of
our faces**



Here's what they are doing and
how we are fighting it



Clearview AI scandal



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

Council of Europe Conseil de l'Europe



Convention 108 on data protection

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



Convention on Artificial Intelligence

2nd plenary meeting
21-23 September 2022

**Council of Europe's Committee
on Artificial Intelligence**

CAI

CAHAI
Ad hoc
Committee
on Artificial
Intelligence



§2 The EU's approach

EU soft law

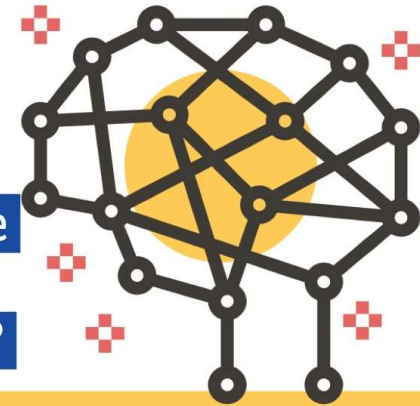
European Parliament's
resolution on *artificial
intelligence in criminal law*
(October 2021)

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

European Union Agency
for Fundamental Rights



How do
we ensure
Artificial
Intelligence
respects
your rights?



JOIN THE DEBATE 14.12.2020





ARTIFICIAL INTELLIGENCE ACT

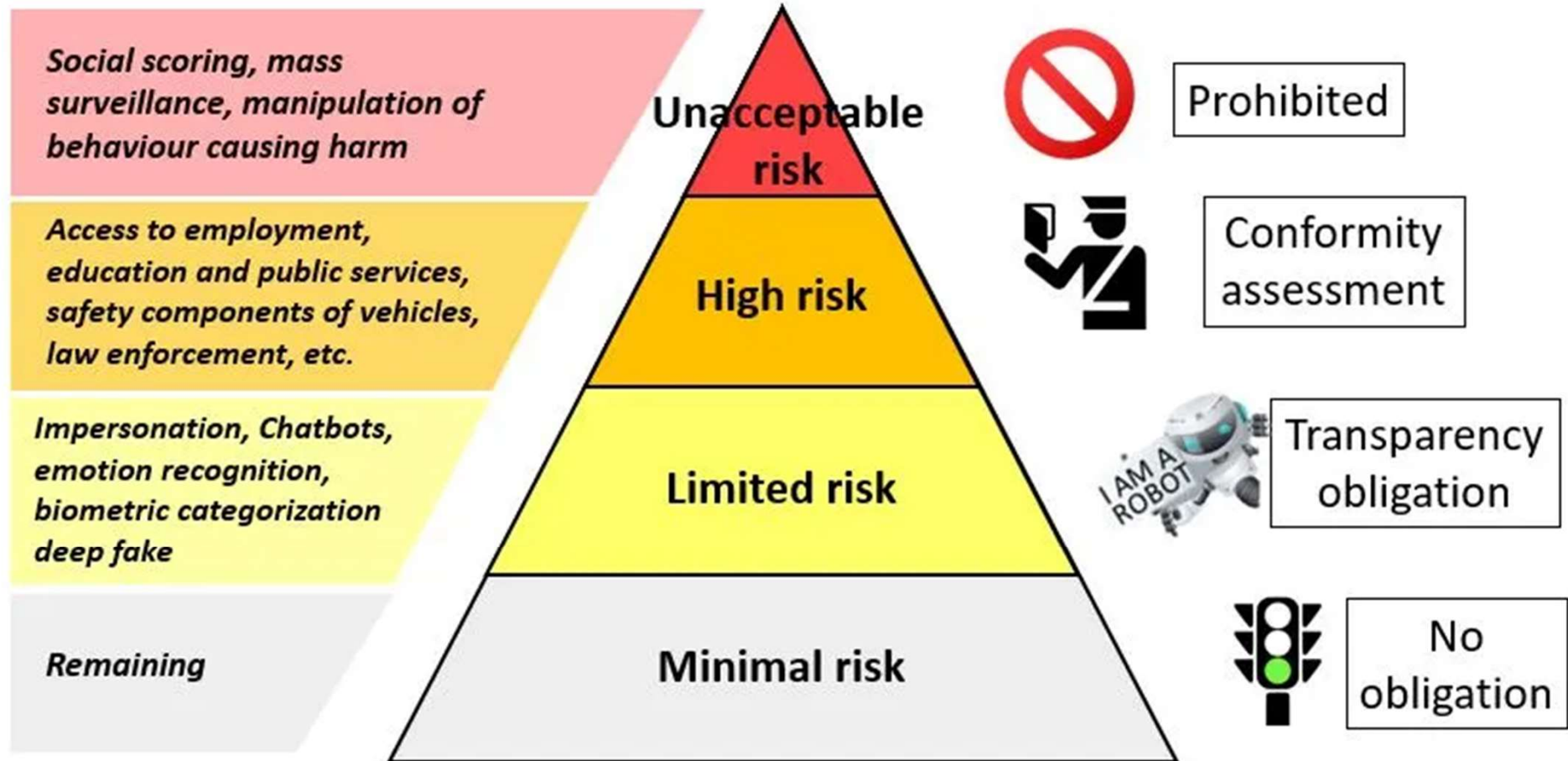
2) The AI Act



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
- Décembre 2023 : political agreement
- 2 February 2024: adoption by the EU Council
- 13 March 2024: final adoption by the EP

EU Artificial Intelligence Act: Risk levels



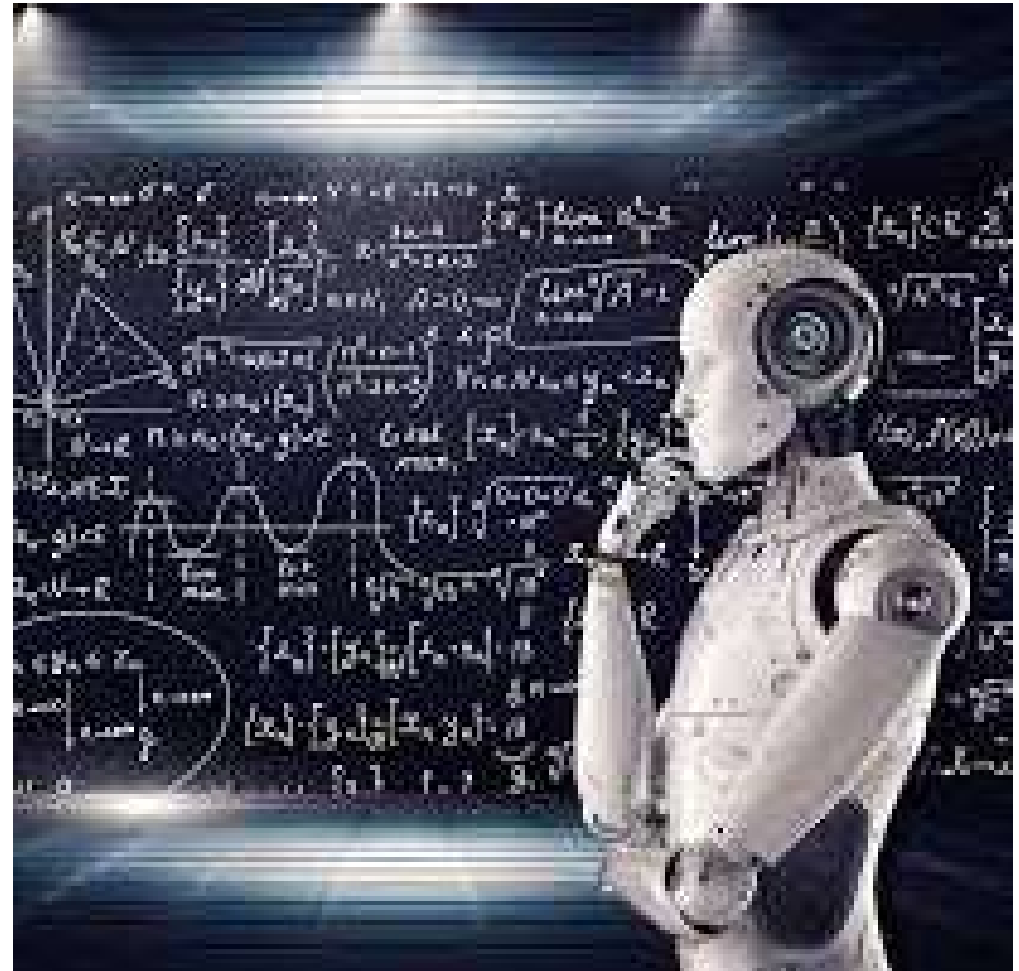


Needs for a CE label



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...
