The EU regulation on the use of biometrics in law enforcement

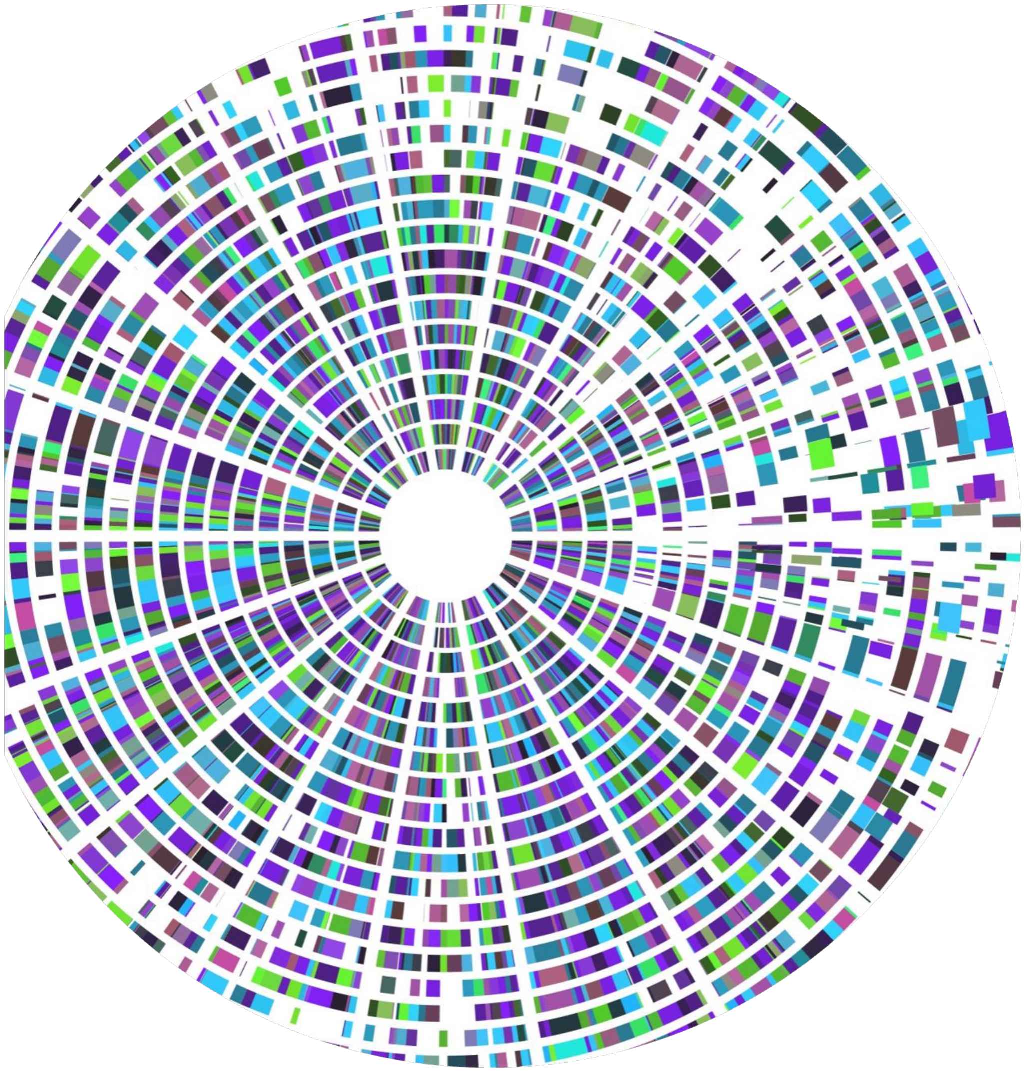
Catherine Jasserand, PhD

International Summer School on Cybercrime and Forensic Computing

4 June 2025

expertise

- Expert in fundamental rights (privacy/data protection) with an interest in biometrics
- Part of the 'Biometric Law Lab' led by Prof. Els Kindt (KU Leuven, CiTiP, Belgium)
- Marie Curie postdoctoral research on facial recognition in public spaces and the right to privacy (DATAFACE)
- Assistant Professor – Faculty of Law, STeP research group, University of Groningen, Netherlands



Overview

- Functioning of FRTs
- Law Enforcement Directive
- AI Act: Biometric Systems, Case studies
- Food for Thought

Context

FACIAL RECOGNITION TECHNOLOGIES

Functioning of FRTs

Technical steps (brief recap):

- **Images captured** through CCTV cameras, drones, other video devices (**image acquisition**)
- **Human faces detected** in the framed images **(face detection)**
- Quality of the images enhanced to **extract the facial features** to perform facial recognition (**feature extraction**)
- Extracted features **transformed into a template**, i.e. mathematical representation of the salient features (**template generation**)
- To perform facial recognition, stored biometric data are **compared** with the biometric data of an individual passing in front of a FRT system (**biometric comparison**)

Functioning of FRTs

- Comparison can be **live** (‘real-time) or **retrospective** (‘post’)

⚠ The concept of real-time/live is not defined from a technical perspective

- At each technical stage, personal data/biometric personal data might be generated

    ▶ data protection rules (LED)

- Rules on the development, putting into the EU market and use of FRTs

    ▶ AI Act

⚠ **Facial recognition**: only identification (1-to-many comparison, e.g. criminal investigation context) and verification (1-to-1 comparison, e.g. identity check) functionalities.

Using **‘facial recognition technologies**’ for **categorisation purposes** (age, sex, etc.) or **emotion recognition** based on facial expressions **≠ performance of facial recognition**

Context

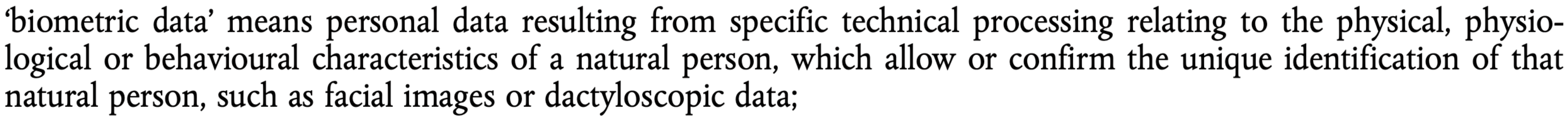
LAW ENFORCEMENT DIRECTIVE

Law Enforcement Directive (LED)

- **Directive 2016/680** – sibling instrument to the GDPR

- **Scope:** personal data processed for law enforcement purposes (*prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties* Art.1(1) LED) by competent authorities (e.g. *police, criminal justice authorities*, Art. 2(1) LED/Art. 3(7) LED)

- **Concept of biometric data :** Art. 3(13) LED



'biometric data' means personal data resulting from specific technical processing relating to the physical, physiological or behavioural characteristics of a natural person, which allow or confirm the unique identification of that natural person, such as facial images or dactyloscopic data;

Law Enforcement Directive (LED)

- **Concept of biometric data (from data protection perspective)**

  Article 3 (13) LED: **4 constitutive elements**

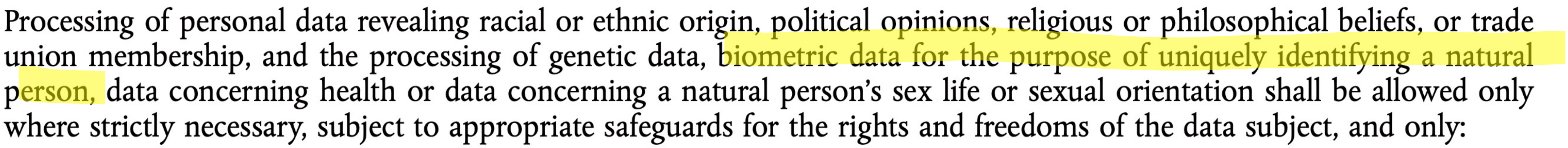
  1. Personal data as a pre-requisite (i.e. data relating to identified/identifiable individual)
  2. Resulting from specific technical means
  3. Relating to biometric characteristics (physical, physiological, and behavioural)
  4. Allowing or confirming the unique identification: uncertainty about exact meaning and scope

Law Enforcement Directive (LED)

- **Photographs, facial images, and biometric templates:** different status / biometric data
  - ✓**Photographs** not processed for facial recognition purposes, i.e. 'mere' photographs, i.e. images extracted from social media for retrospective use of facial recognition or images captured from CCTV before their 'pre-processing' **≠ biometric data**
  - ✓**Facial images** transformed for facial recognition purposes **= biometric data**
  - ✓**Biometric templates = biometric data**

Law Enforcement Directive (LED)

- **Criterion of ‘uniquely identifying’** is used to classify biometric data into the category of sensitive data (known as *special categories of personal data*)
- **Article 10 LED**



Processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person’s sex life or sexual orientation shall be allowed only where strictly necessary, subject to appropriate safeguards for the rights and freedoms of the data subject, and only:

- **Conditions to process sensitive data**:
  - ✓ Strict necessity of the processing, appropriate safeguards
  - ✓ Three legal grounds:
    - + Authorised by Union or national law (e.g. clear, precise, and foreseeable in its application)
    - + Protection of the vital interests of individuals, or
    - + Data manifestly made public by the data subject

Law Enforcement Directive (LED)

- **Various obligations linked to the processing of biometric data**

  ✓ **Data Protection Impact Assessment (Art. 27 LED):** obligation triggered when data processing **likely to result in a high risk** to the rights and freedoms to individuals assessed through the combination of, at least, two criteria (Art.29 WP's Guidelines on DPIA, WP248 rev.01)

  e.g. deploying FRTs in public spaces

  ✓ **Data Protection by Design and by Default (Art. 20 LED):** obligation for data controllers (e.g. law enforcement authorities to adopt technical and organisational measures to implement data protection principles

  e.g. use of relevant security standards and biometric template protection

  ✓ **Other obligations**: e.g. rules concerning automated decision-making (Art. 11 LED)

Context

AI ACT

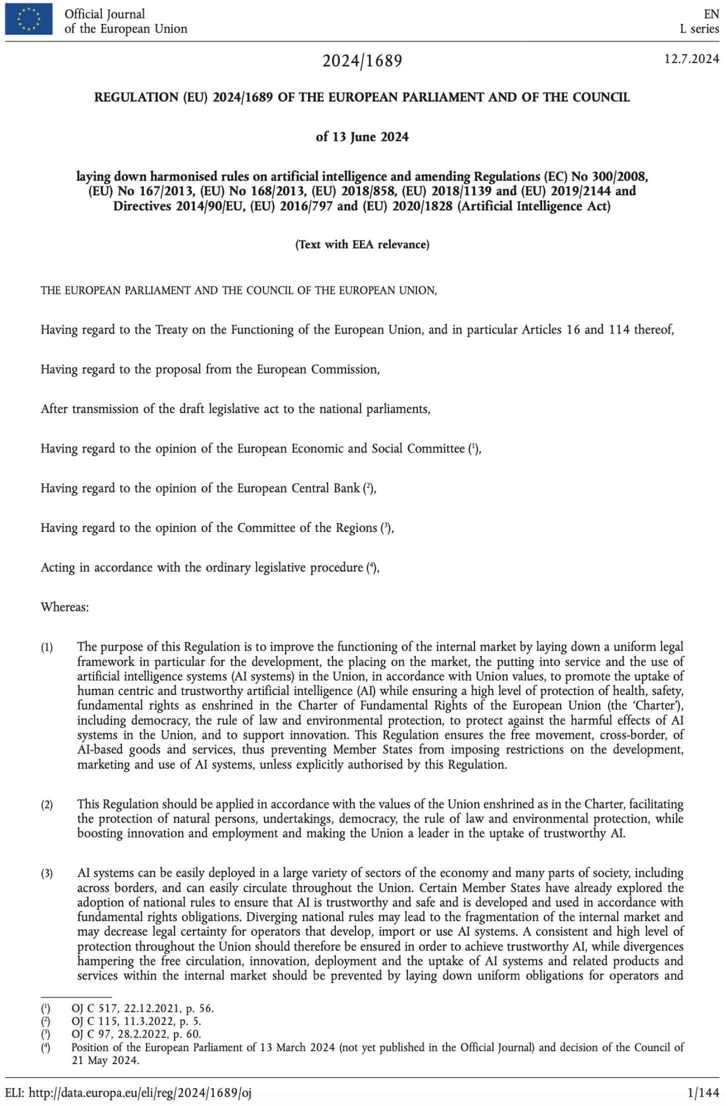
AI Act (Regulation 2024/1689)

Regulating the development, placing on the EU market, putting into service and use of certain AI systems

AI systems regulated according to the **risks** they pose to health, safety, and fundamental rights

Horizontal act, not replacing EU frameworks (e.g. data protection rules) still applying

+ European Commission's Guidelines and Future Standards



Official Journal
of the European Union

EN
L series

2024/1689

12.7.2024

REGULATION (EU) 2024/1689 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL

of 13 June 2024

laying down harmonised rules on artificial intelligence and amending Regulations (EC) No 300/2008, (EU) No 167/2013, (EU) No 168/2013, (EU) 2018/858, (EU) 2018/1139 and (EU) 2019/2144 and Directives 2014/90/EU, (EU) 2016/797 and (EU) 2020/1828 (Artificial Intelligence Act)

(Text with EEA relevance)

THE EUROPEAN PARLIAMENT AND THE COUNCIL OF THE EUROPEAN UNION,

Having regard to the Treaty on the Functioning of the European Union, and in particular Articles 16 and 114 thereof,

Having regard to the proposal from the European Commission,

After transmission of the draft legislative act to the national parliaments,

Having regard to the opinion of the European Economic and Social Committee ([1]),

Having regard to the opinion of the European Central Bank ([2]),

Having regard to the opinion of the Committee of the Regions ([3]),

Acting in accordance with the ordinary legislative procedure ([4]),

Whereas:

(1) The purpose of this Regulation is to improve the functioning of the internal market by laying down a uniform legal framework in particular for the development, the placing on the market, the putting into service and the use of artificial intelligence systems (AI systems) in the Union, in accordance with Union values, to promote the uptake of human centric and trustworthy artificial intelligence (AI) while ensuring a high level of protection of health, safety, fundamental rights as enshrined in the Charter of Fundamental Rights of the European Union (the 'Charter'), including democracy, the rule of law and environmental protection, to protect against the harmful effects of AI systems in the Union, and to support innovation. This Regulation ensures the free movement, cross-border, of AI-based goods and services, thus preventing Member States from imposing restrictions on the development, marketing and use of AI systems, unless explicitly authorised by this Regulation.

(2) This Regulation should be applied in accordance with the values of the Union enshrined as in the Charter, facilitating the protection of natural persons, undertakings, democracy, the rule of law and environmental protection, while boosting innovation and employment and making the Union a leader in the uptake of trustworthy AI.

(3) AI systems can be easily deployed in a large variety of sectors of the economy and many parts of society, including across borders, and can easily circulate throughout the Union. Certain Member States have already explored the adoption of national rules to ensure that AI is trustworthy and safe and is developed and used in accordance with fundamental rights obligations. Diverging national rules may lead to the fragmentation of the internal market and may decrease legal certainty for operators that develop, import or use AI systems. A consistent and high level of protection throughout the Union should therefore be ensured in order to achieve trustworthy AI, while divergences hampering the free circulation, innovation, deployment and the uptake of AI systems and related products and services within the internal market should be prevented by laying down uniform obligations for operators and

[1] OJ C 517, 22.12.2021, p. 56.
[2] OJ C 115, 11.3.2022, p. 5.
[3] OJ C 97, 28.2.2022, p. 60.
[4] Position of the European Parliament of 13 March 2024 (not yet published in the Official Journal) and decision of the Council of 21 May 2024.

AI systems

Art. 3(1) AI Act:

AI system means a machine-based system that is designed to operate with varying levels of autonomy and that may exhibit adaptiveness after deployment, and that, for explicit or implicit objectives, infers, from the input it receives , how to generate outputs such as predictions, content, recommendations, or decisions that can influence physical or virtual environments

CONSTITUTIVE ELEMENTS

1) Machine-based system
2) Level of autonomy
3) Adaptiveness
4) Explicit/implicit objective
5) Capacity to infer
6) Predictions, content, recommendations of decisions
7) Influences environments

No definition of AI but AI systems

No specific technology/ technical approach/system architecture mentioned

Exclusions

Scope of application

What: AI systems and General-Purpose AI models

Activities: placing on the market, putting into service or using AI systems regulated according to the risks they pose (fundamental rights, safety, and health)

Exclusions: AI systems exclusively developed or used for:

- military/defence/national security purposes
- scientific research and development purposes

Where: in the EU / extraterritorial application (e.g. beyond the EU if an AI system generates an output used in the EU)

Who: a range of actors concerned, but rules mainly apply to providers and deployers

Actors/ stakeholders

Provider: entity developing AI systems or general-purpose AI models

e.g. public authority developing a system in-house

Deployer: entity using AI systems

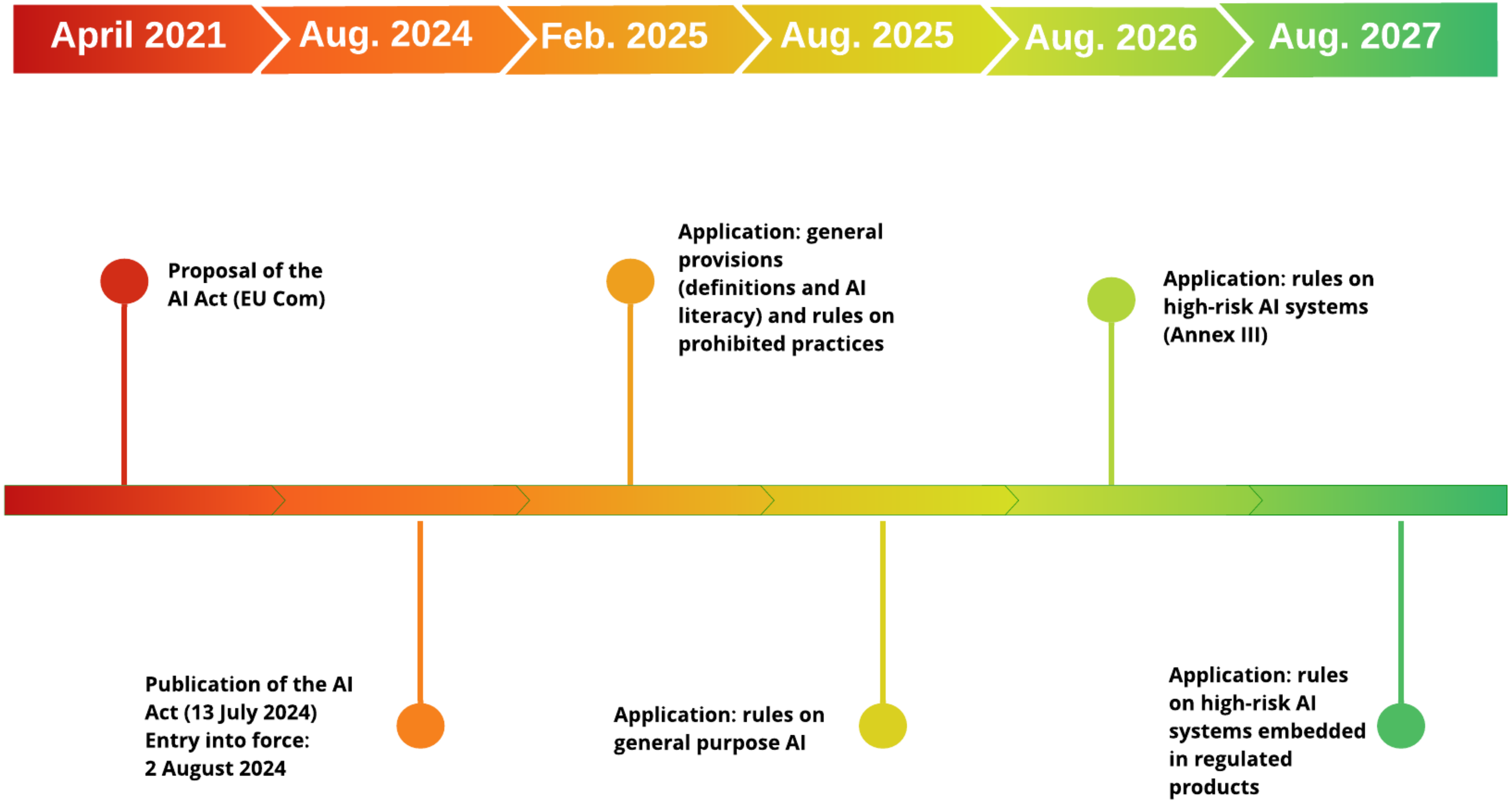
e.g. law enforcement authorities

Product Manufacturer: entity that manufactures products that integrate AI systems

Distributor: entity that makes an AI system available in the EU market

Importer: entity established/located in the EU that places an AI system bearing name/trademark of another entity established outside the EU market

Calendar AI Act (in brief)



April 2021

Aug. 2024

Feb. 2025

Aug. 2025

Aug. 2026

Aug. 2027

Proposal of the AI Act (EU Com)

Publication of the AI Act (13 July 2024)
Entry into force:
2 August 2024

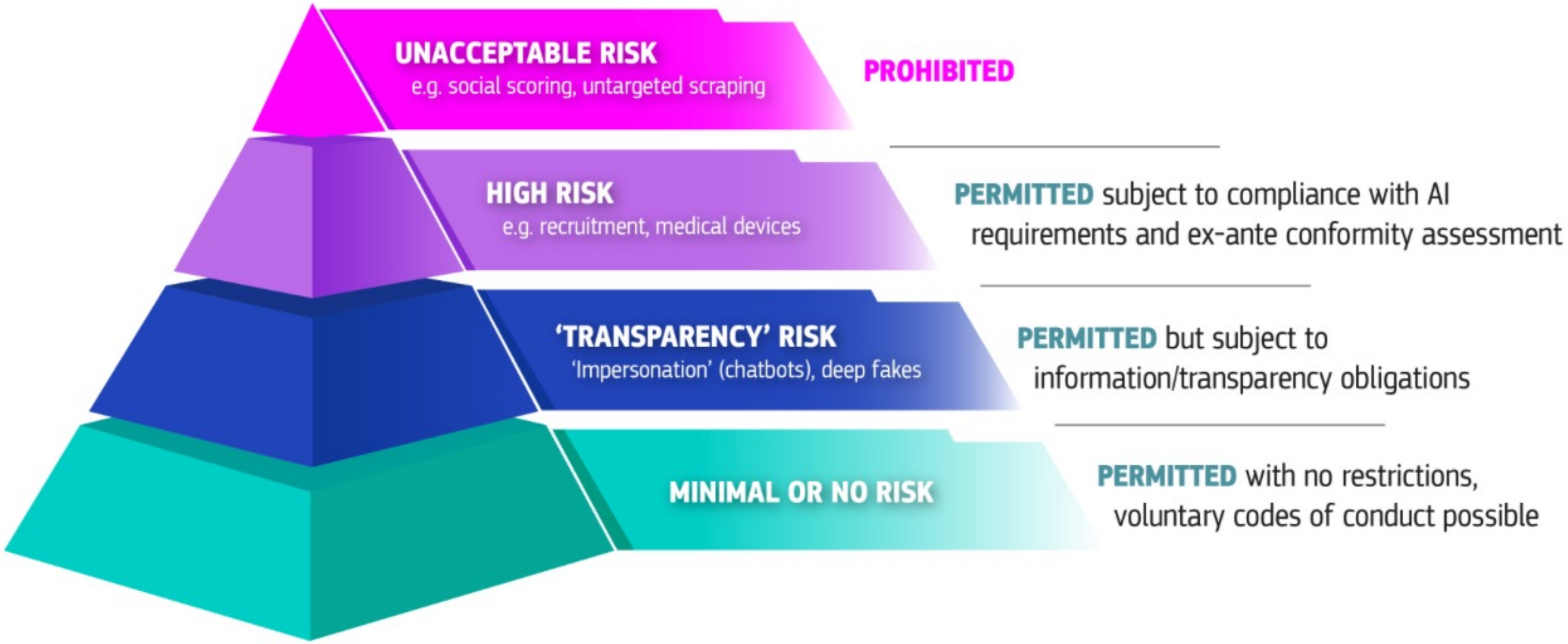
Application: general provisions (definitions and AI literacy) and rules on prohibited practices

Application: rules on general purpose AI

Application: rules on high-risk AI systems (Annex III)

Application: rules on high-risk AI systems embedded in regulated products

Risk-based approach


UNACCEPTABLE RISK
e.g. social scoring, untargeted scraping
HIGH RISK
e.g. recruitment, medical devices
'TRANSPARENCY' RISK
'Impersonation' (chatbots), deep fakes
MINIMAL OR NO RISK
PROHIBITED
PERMITTED subject to compliance with AI requirements and ex-ante conformity assessment
PERMITTED but subject to information/transparency obligations
PERMITTED with no restrictions, voluntary codes of conduct possible

Source: https://digital-strategy.ec.europa.eu/en/factpages/ai-act

Biometric Systems

Emotion recognition system: AI system for the purpose of **identifying** or **inferring emotions** or **intentions** of natural persons on the basis of their **biometric data**. (Art. 3(39) AI Act)

Biometric categorisation system : AI system for the purpose of assigning natural persons to **specific categories** on the basis of **their biometric data,** unless it is ancillary to another commercial service and strictly necessary for objective technical reasons. (Art. 3(40) AI Act)

Remote Biometric Identification system: AI system for the purpose of **identifying natural persons**, without their active involvement, typically at a distance through the comparison of a person's biometric data with the biometric data contained in a reference database (Art. 3(41) AI Act)

Untargeted Scraping of facial images : no definition in the AI Act

Definitions of biometric data

From data protection perspective

1. ‘biometric data’ means personal data resulting from specific technical processing relating to the physical, physiological or behavioural characteristics of a natural person, **which allow or confirm the unique identification of that natural person**, such as facial images or dactyloscopic data **(Art. 3(13) LED)**

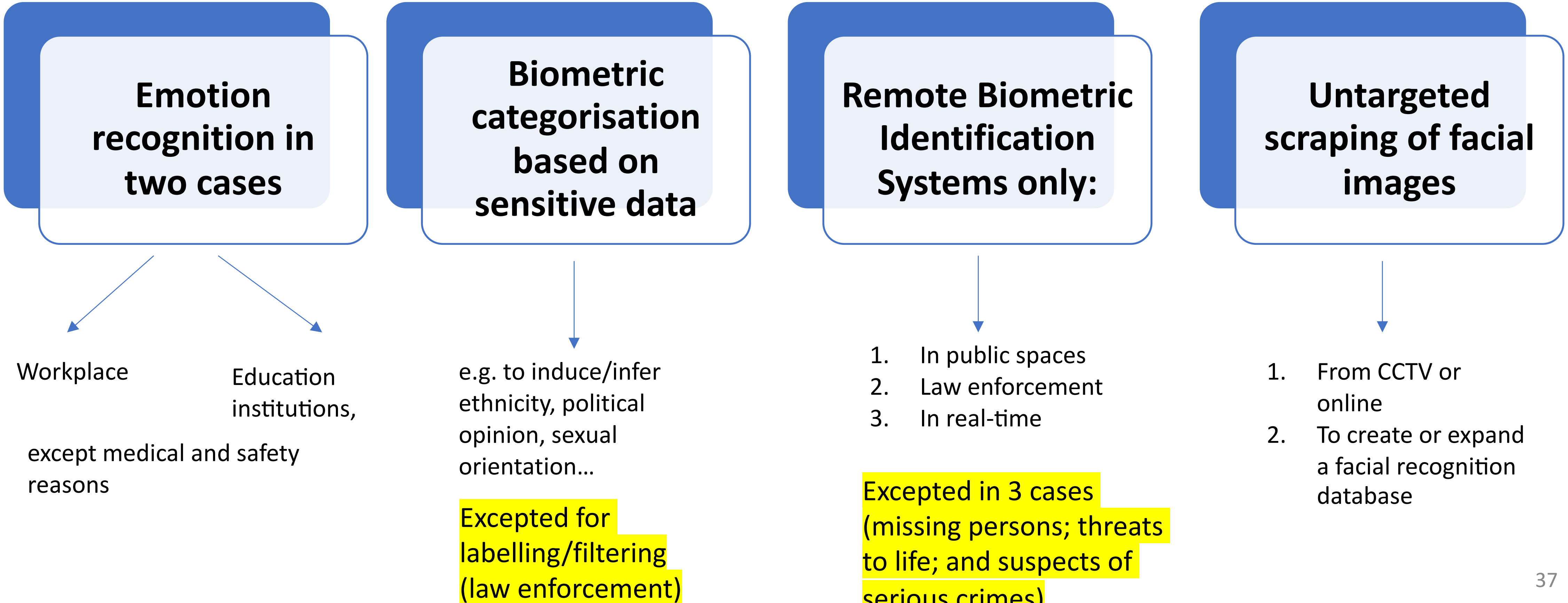
2. **Functionality purpose** of the processing of biometric data = to ‘uniquely identify’ an individual

From an AI Act perspective

‘biometric data’ means personal data resulting from specific technical processing relating to the physical, physiological or behavioural characteristics of a natural person, such as facial images or dactyloscopic data (**Art. 3(34) AI Act**)

Broader understanding to allow identification/authentication, categorisation of natural persons and emotion recognition of with biometric data **(Rec. 14 AI Act)**

Prohibited Biometric Systems (Art. 5(1) AI Act)



Emotion recognition in two cases

Workplace

Education institutions,

except medical and safety reasons

Biometric categorisation based on sensitive data

e.g. to induce/infer ethnicity, political opinion, sexual orientation…

Excepted for labelling/filtering (law enforcement)

Remote Biometric Identification Systems only:

1. In public spaces
2. Law enforcement
3. In real-time

Excepted in 3 cases (missing persons; threats to life; and suspects of serious crimes)

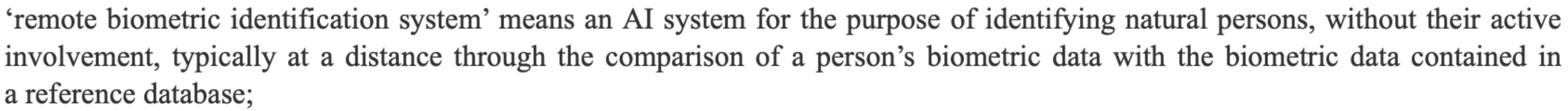
Untargeted scraping of facial images

1. From CCTV or online
2. To create or expand a facial recognition database

Remote Biometric Identification Systems

- No regulation of FRTs but regulation of the generic category of **Remote Biometric Identification** systems

- Art. 3(41) AI Act – definition

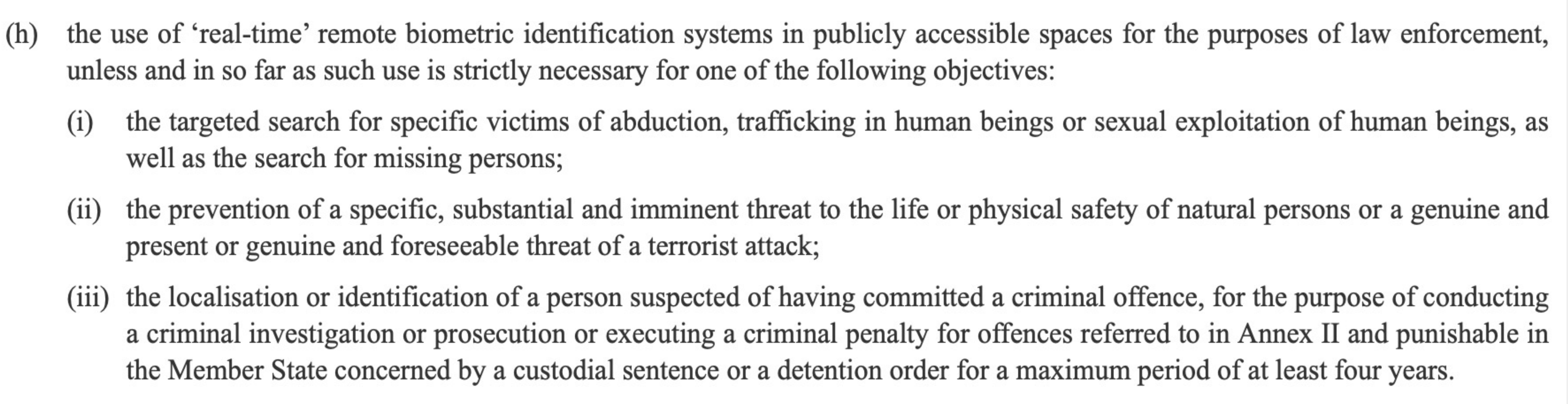


‘remote biometric identification system’ means an AI system for the purpose of identifying natural persons, without their active involvement, typically at a distance through the comparison of a person’s biometric data with the biometric data contained in a reference database;

- FRTs as the typical example of RBI and definition modelled after functioning of FRT: operate at a distance, w/o active involvement (and awareness)

Remote Biometric Identification Systems

REAL-TIME RBIs IN PUBLICLY ACCESSIBLE AREAS FOR LAW ENFORCEMENT (Art. 5(1)(h) AI Act)



(h) the use of 'real-time' remote biometric identification systems in publicly accessible spaces for the purposes of law enforcement, unless and in so far as such use is strictly necessary for one of the following objectives:

(i) the targeted search for specific victims of abduction, trafficking in human beings or sexual exploitation of human beings, as well as the search for missing persons;

(ii) the prevention of a specific, substantial and imminent threat to the life or physical safety of natural persons or a genuine and present or genuine and foreseeable threat of a terrorist attack;

(iii) the localisation or identification of a person suspected of having committed a criminal offence, for the purpose of conducting a criminal investigation or prosecution or executing a criminal penalty for offences referred to in Annex II and punishable in the Member State concerned by a custodial sentence or a detention order for a maximum period of at least four years.

Remote Biometric Identification Systems

- **REAL-TIME RBIs IN PUBLICLY ACCESSIBLE AREAS FOR LAW ENFORCEMENT (Art. 5(1)(h) AI Act)**
  - ✓ **Ban as the rule**

    e.g. police deploying live FRTs in public spaces to identify and locate protestors

  - ✓ But three exceptions, which must be authorised by national laws:
  - ✓ **1st exception**: Targeted search for actual (and not potential) victims of three crimes (abduction, trafficking in human beings or sexual exploitation) as well as missing persons

    e.g. real-time RBI cannot be used to search for a child who is at risk of being abducted by a relative

  - ✓ **2nd exception:** Prevention of specific, substantial and imminent threat to the life or physical safety or genuine and present or genuine and foreseeable threat of a terrorist attack

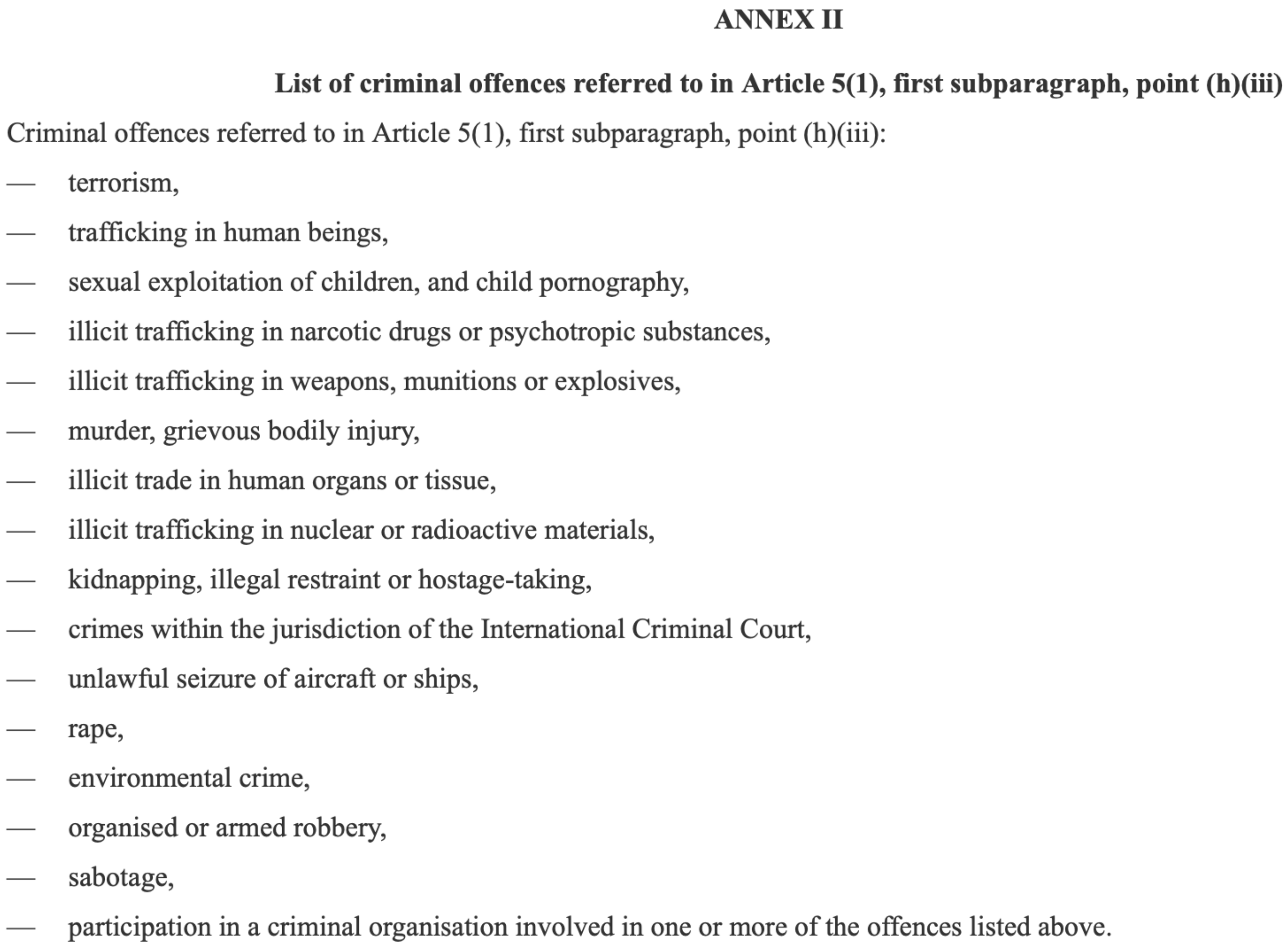
    e.g. hostage situations, threats to the security of critical infrastructures

    e.g. a threat of a terrorist attack that reaches a certain threshold

  - ✓ **3rd exception**: localisation and identification of suspects and perpetrators of listed serious crimes (Annex II) punishable by a custodial sentence/detention order for a maximum period of at least 4 years

    e.g. use of real-time RBI to identify a terrorist suspect after a serious terror attack and locate him close to the train station

Remote Biometric Identification Systems



ANNEX II

List of criminal offences referred to in Article 5(1), first subparagraph, point (h)(iii)

Criminal offences referred to in Article 5(1), first subparagraph, point (h)(iii):

- terrorism,
- trafficking in human beings,
- sexual exploitation of children, and child pornography,
- illicit trafficking in narcotic drugs or psychotropic substances,
- illicit trafficking in weapons, munitions or explosives,
- murder, grievous bodily injury,
- illicit trade in human organs or tissue,
- illicit trafficking in nuclear or radioactive materials,
- kidnapping, illegal restraint or hostage-taking,
- crimes within the jurisdiction of the International Criminal Court,
- unlawful seizure of aircraft or ships,
- rape,
- environmental crime,
- organised or armed robbery,
- sabotage,
- participation in a criminal organisation involved in one or more of the offences listed above.

Remote Biometric Identification Systems

- **CONDITIONS AND SAFEGUARDS FOR THE EXCEPTIONS TO THE BAN (Art. 5(2)-(7) AI Act)**
  - ✓ **National law authorising the use**
  - ✓ To **confirm the identity of a targeted individual**
  - ✓ **Assessment** of the seriousness, scale, and probability of the harm for individuals and nature of the situation
  - ✓ Geographic, personal, and time **limitations**
  - ✓ Performance of a **FRIA** and registration of the system in the EU database
  - ✓ System **authorised a priori** by a judge/independent authority (except in case of emergency)
  - ✓ No decision having an adverse effect on individuals with legal consequences can be taken solely on the basis of the output of the system
  - ✓ Use of real-time RBI documented and communicated to market surveillance authorities and DPAs
  - ✓ Annual reports to the EU Commission and by the EU Commission

Remote Biometric Identification Systems

- **RETROSPECTIVE USE of RBIs in publicly accessible spaces for law enforcement purposes**
  - ✓ e.g. FRT used for criminal investigations on video feeds
  - ✓ **High-risk systems (Art. 6(2) + Annex III (1)(a))**
  - ✓ **Rules for high-risk systems:** pre/post-market conformity assessments, FRIAs for deployers that are public entities governed by public law (e.g. police), data governance, record-keeping, risk management system, technical documentation, transparency obligations, human oversight, accuracy, robustness and cybersecurity
  - ✓ **Additional rules: Art. 26(10):** prior authorisation to use RBI, systems used in a targeted manner, i.e. 'in link with a criminal procedure, criminal proceeding, or a genuine and present or genuine and foreseeable threat of a criminal offence, or the search for a specific missing person', and no decision that would adversely affect an individual can be taken solely on the system's output, i.e. without human review or intervention

Remote Biometric Identification Systems

- **RETROSPECTIVE USE of FRTs and the French TAJ (criminal records) used for that purpose**

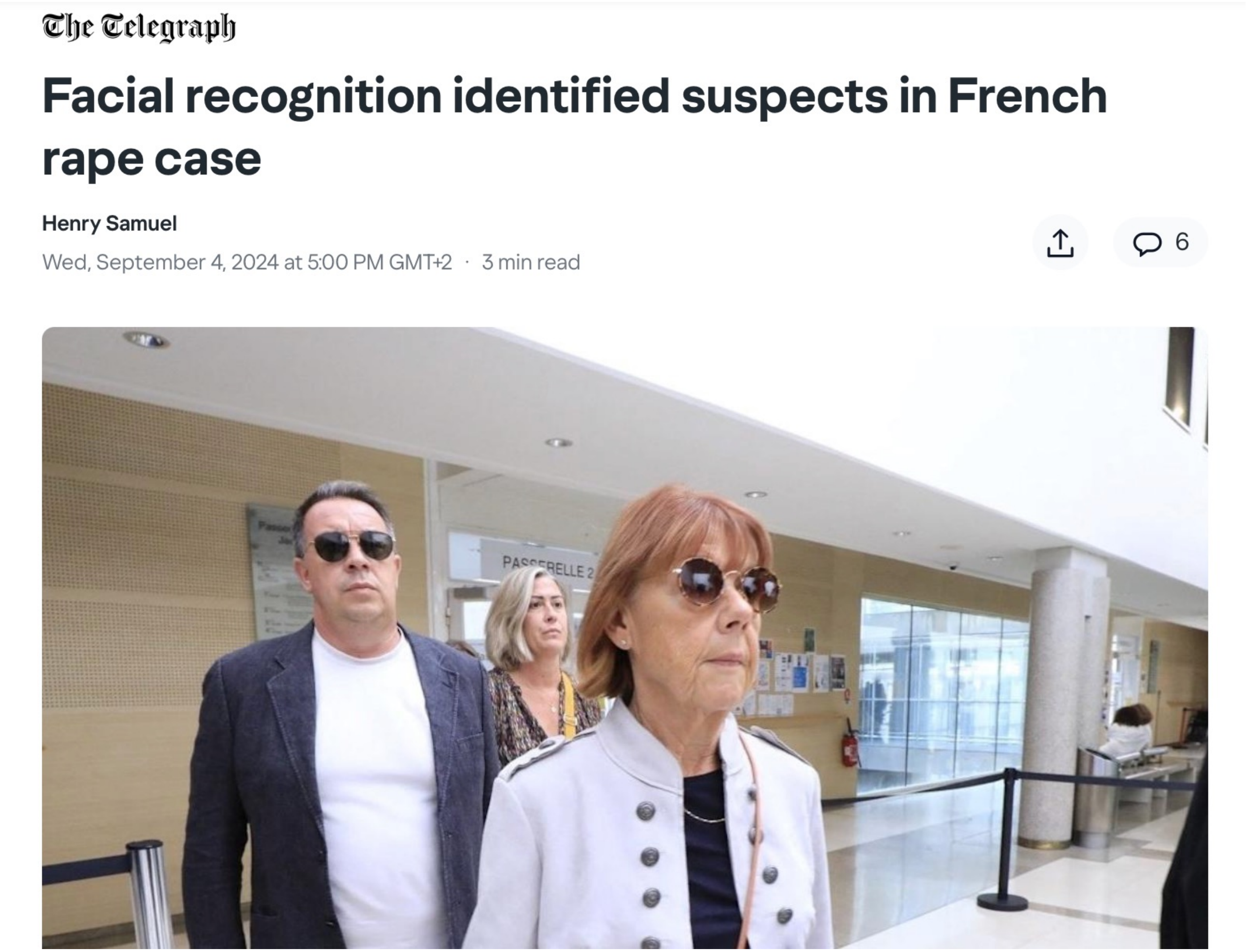
➢ Since 2018, French police authorities can perform retrospective FRT (decree of 2012)

➢ **Art. R.40-26 of French code of criminal procedure** lists the information recorded in the TAJ, including photographs having technical characteristics to perform FRT.

➢ Database containing images of offenders (of crime, offences, including minor offences), victims, and missing persons.

➢ 6 Million of images of suspects and victims in 2019 (TELEFI Report).

Remote Biometric Identification Systems



The Telegraph

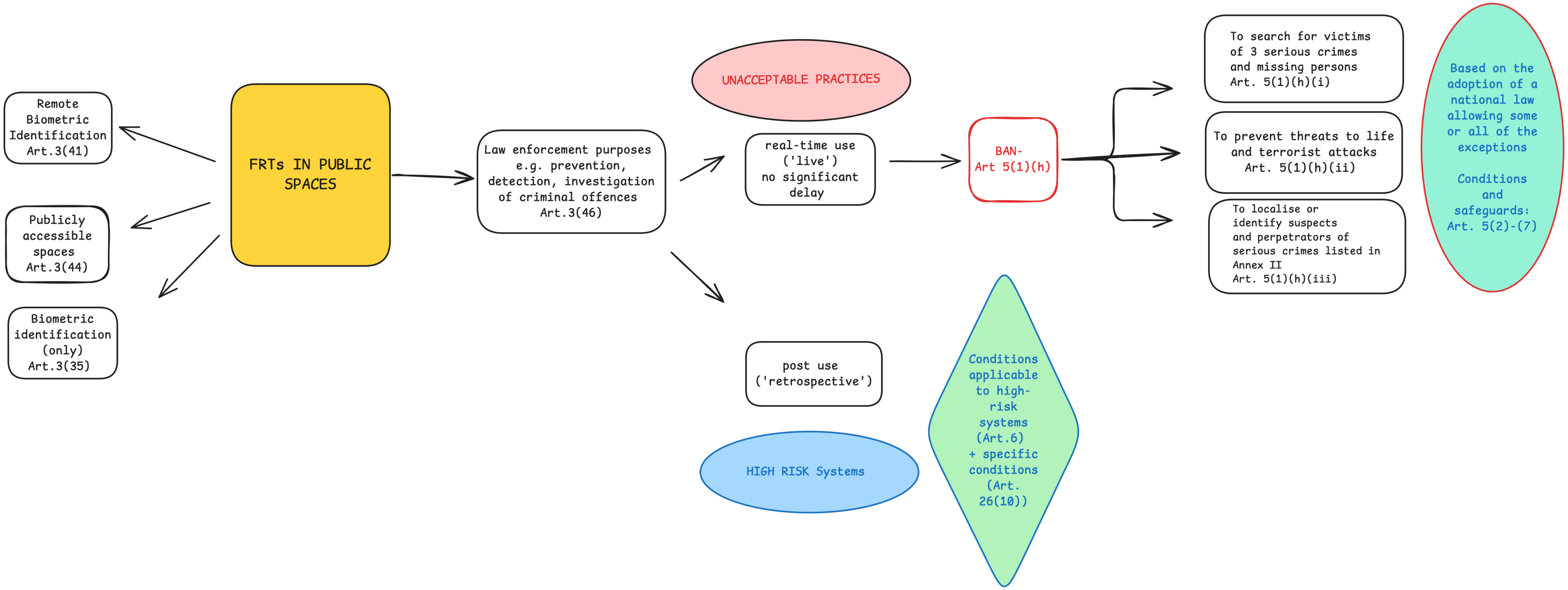
Facial recognition identified suspects in French rape case

Henry Samuel

Wed, September 4, 2024 at 5:00 PM GMT+2 · 3 min read

- ✓ Police used facial recognition software to identify suspects in videos
- ✓ ?: Which software was it?
- ✓ ?: Which legal basis for the retrospective use of FRT?
- ✓ ?: Did they perform the comparison against the TAJ criminal record?
- ✓ No legal basis for extracting images from social media

Remote Biometric Identification Systems



FRTs IN PUBLIC SPACES

Remote Biometric Identification Art.3(41)

Publicly accessible spaces Art.3(44)

Biometric identification (only) Art.3(35)

Law enforcement purposes e.g. prevention, detection, investigation of criminal offences Art.3(46)

UNACCEPTABLE PRACTICES

real-time use ('live') no significant delay

BAN- Art 5(1)(h)

To search for victims of 3 serious crimes and missing persons Art. 5(1)(h)(i)

To prevent threats to life and terrorist attacks Art. 5(1)(h)(ii)

To localise or identify suspects and perpetrators of serious crimes listed in Annex II Art. 5(1)(h)(iii)

Based on the adoption of a national law allowing some or all of the exceptions

Conditions and safeguards: Art. 5(2)-(7)

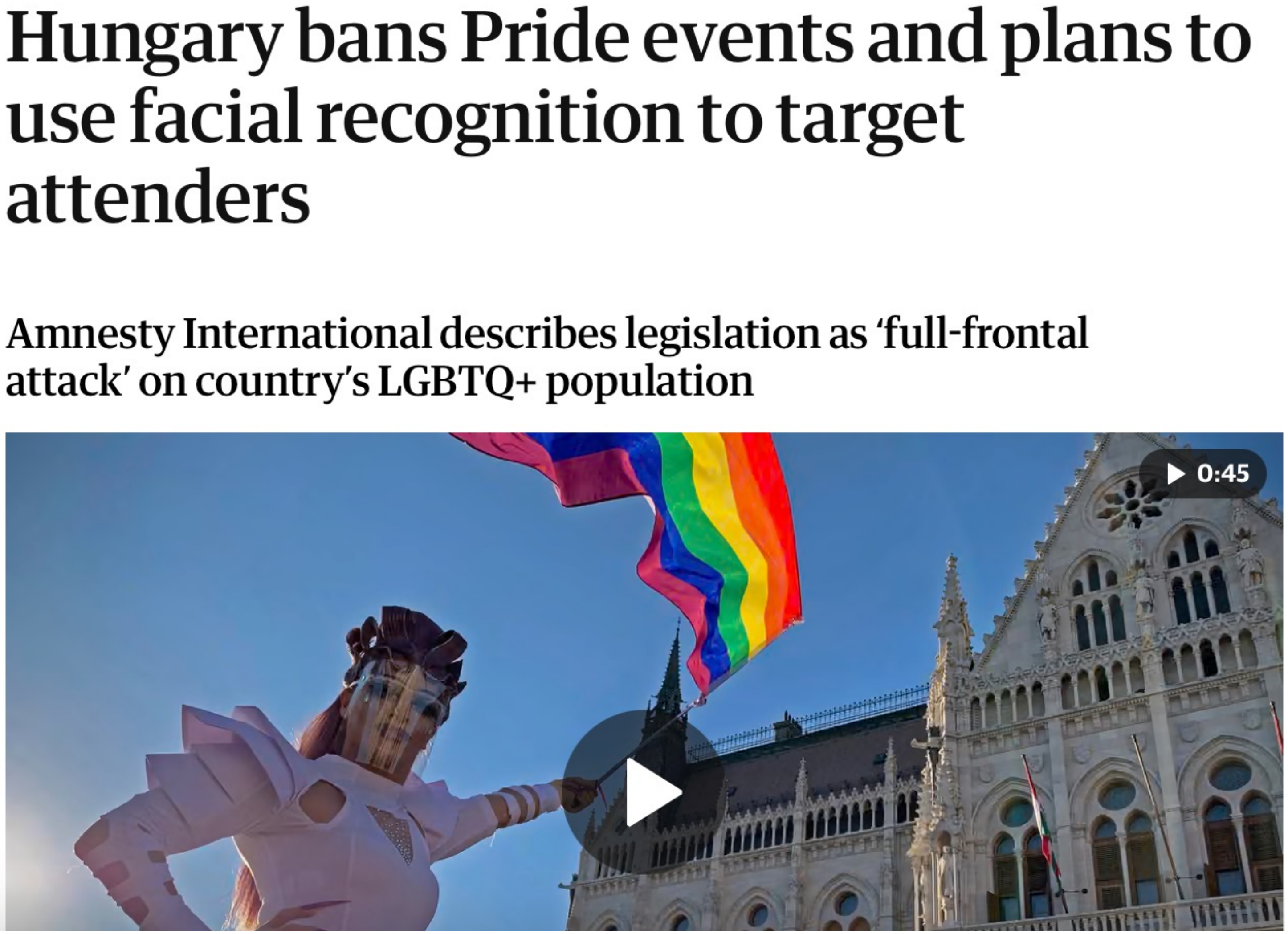
post use ('retrospective')

HIGH RISK Systems

Conditions applicable to high-risk systems (Art.6) + specific conditions (Art. 26(10))

Made with Excalidraw

Focus: Hungarian law to identify protesters



Hungary bans Pride events and plans to use facial recognition to target attenders

Amnesty International describes legislation as 'full-frontal attack' on country's LGBTQ+ population

Source: The Guardian

Focus: Hungarian law to identify protesters

LAW

1. Prohibited to hold an assembly that violates the ban set out in the Child Protection Act (amendment/ March 2025)
2. Anyone participating in an event, such as Pride events, could be fined; people would be identified (live?/retrospectively?) thanks to the vast network of CCTV cameras

Legal under EU Regulations?

1. Does it fall into the prohibition of Art. 5 of the AI Act?
2. What about data protection rules?
3. And most important, compliance with fundamental rights?

Emotion Recognition

Prohibition: Art. 5(1)(f)

> No placing on the market, putting into service or use of AI systems to **infer emotions** of a natural person in the areas of workplace and education institutions, except for medical or safety reasons.

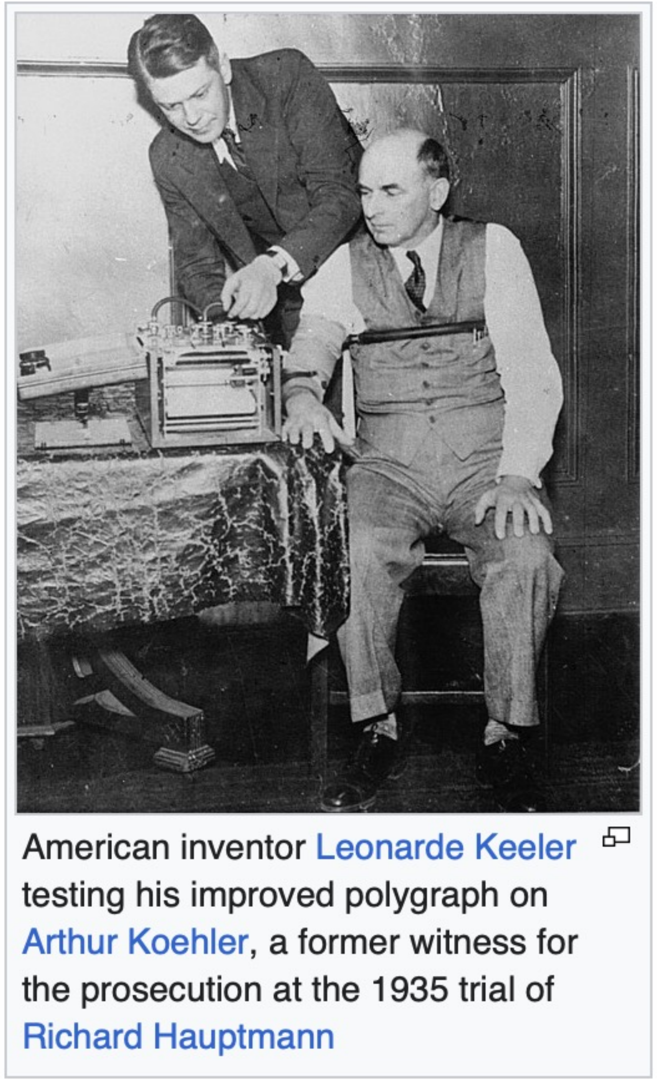
✓**Rationale**: concerns about the non-scientific basis and imbalance of powers (Rec. 44 AI Act)

✓Emotions or intentions such as happiness, sadness, anger, surprise, disgust, embarrassment, excitement, shame, contempt, satisfaction and amusement.

✓**Exclusions:** physical state (fatigue or pain) and mere detection of gestures, apparent expressions…(rec. 18/ Art. 3(39))

Case of polygraph

- Presumption that lies can be detected
- At the **intersection** between **predictive policing** and **emotion recognition systems**
- But not classified under ‘biometrics systems’ in the AI Act
- Their use raises **legal and ethical questions** (challenge for the fundamental right to privacy, presumption of innocence, right to not self-incriminate)
- Thus, their use even if authorised by national law (in application of the AI Act) must **comply with fundamental rights** to be legitimate



American inventor Leonarde Keeler testing his improved polygraph on Arthur Koehler, a former witness for the prosecution at the 1935 trial of Richard Hauptmann

Source image: Wikipedia

Case of polygraph

What the AI Act provides for:

Use of polygraphs by **law enforcement and migration authorities classified as high-risk (Annex III of AI Act)**

6(b):

*AI systems intended to be used by or on behalf of **law enforcement authorities** or by Union institutions, bodies, offices or agencies in support of law enforcement authorities as polygraphs or similar tools*

And

7(b)

*AI systems intended to be used by or on behalf of **competent public authorities** [migration, asylum and border control management] or by Union institutions, bodies, offices or agencies in support of law enforcement authorities as polygraphs or similar tools*

What the AI Act CANNOT provide for:

1. **The scientific validity** of polygraphs
2. And thus, which scientific studies **could back up** the development of polygraphs and reliability of their results
3. **The legal basis to use polygraphs**; it recognises that law enforcement and migration authorities may use it, provided their use is permitted under EU/national law

⚠ *The use of polygraph is already prohibited in some Member States*

Biometric categorisation

Prohibition: Art. 5(1)(g)

No placing on the market, putting into service or use of biometric categorisation systems that categorise individually natural persons to **deduce or infer sensitive data** (e.g. race, political opinions, trade union membership, religious or philosophical beliefs, sex life or sexual orientation)

Examples of prohibited practices

1) Inferring political opinions from a facial image
2) Deducing sexual orientation based on voice

Biometric categorisation

- **Exceptions** (Recs 16 and 30, Art. 3(40) AI Act)
  - ➢Ancillary services linked to another commercial service, which include filters proposed by social media
  - ➢Labelling biometric datasets in compliance with other legislation (e.g. data protection rules)
  - ➢Classifying images based on hair/eye colour for law enforcement purposes

Untargeted Scraping

- **Prohibition: Article 5(1)(e)**

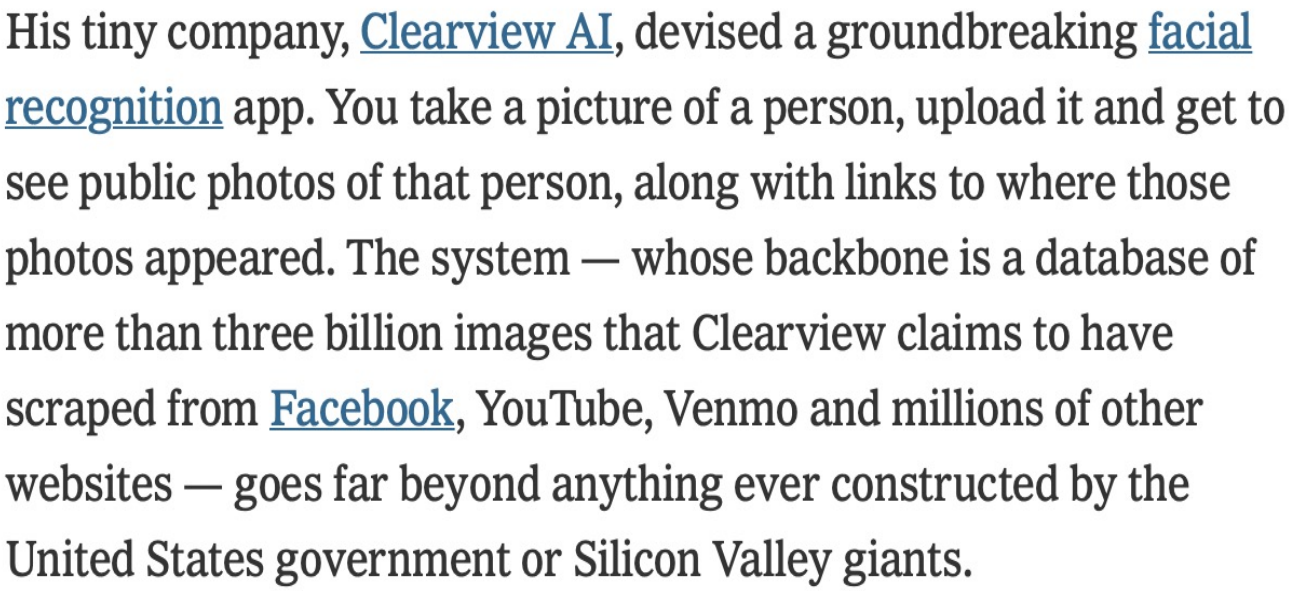
No placing on the market, putting into service, or use of **AI systems** to **create/expand facial recognition databases** through **untargeted scraping** of facial images from **the Internet or CCTV**

Rationale/background: practices of **Clearview AI** and **PimEyes**

Only covers facial images and creation /expansion of existing facial databases (but not use of existing databases)

Scope limited

Use case: Clearview AI



His tiny company, Clearview AI, devised a groundbreaking facial recognition app. You take a picture of a person, upload it and get to see public photos of that person, along with links to where those photos appeared. The system — whose backbone is a database of more than three billion images that Clearview claims to have scraped from Facebook, YouTube, Venmo and millions of other websites — goes far beyond anything ever constructed by the United States government or Silicon Valley giants.

New York Times – The Secretive Company That Might End Privacy as We Know It- 18 January 2020

Technical description of the tool

(based on NOYB's complaint)

1. Clearview AI uses an '**automated image scraper**' to search the Internet and collect images where it detects human faces + 'metadata' (information associated with the images) – all stored on Clearview AI's servers

2. **Facial features** are then **extracted** through image processing

'for each image collected, every face contained in the image is scanned and processed in order to extract its uniquely identifying facial features. Faces are translated into numerical representations which [NOYB] refer(s) to as "vectors". These vectors consists of 512 data points that represent the various unique lines that make up a face.'

Technical description of the tool
(based on NOYB's complaint)

3. Clearview AI **stores vectors** in a database (associated with images and other info) – The vectors are then **hashed** for indexation and future identification purposes.

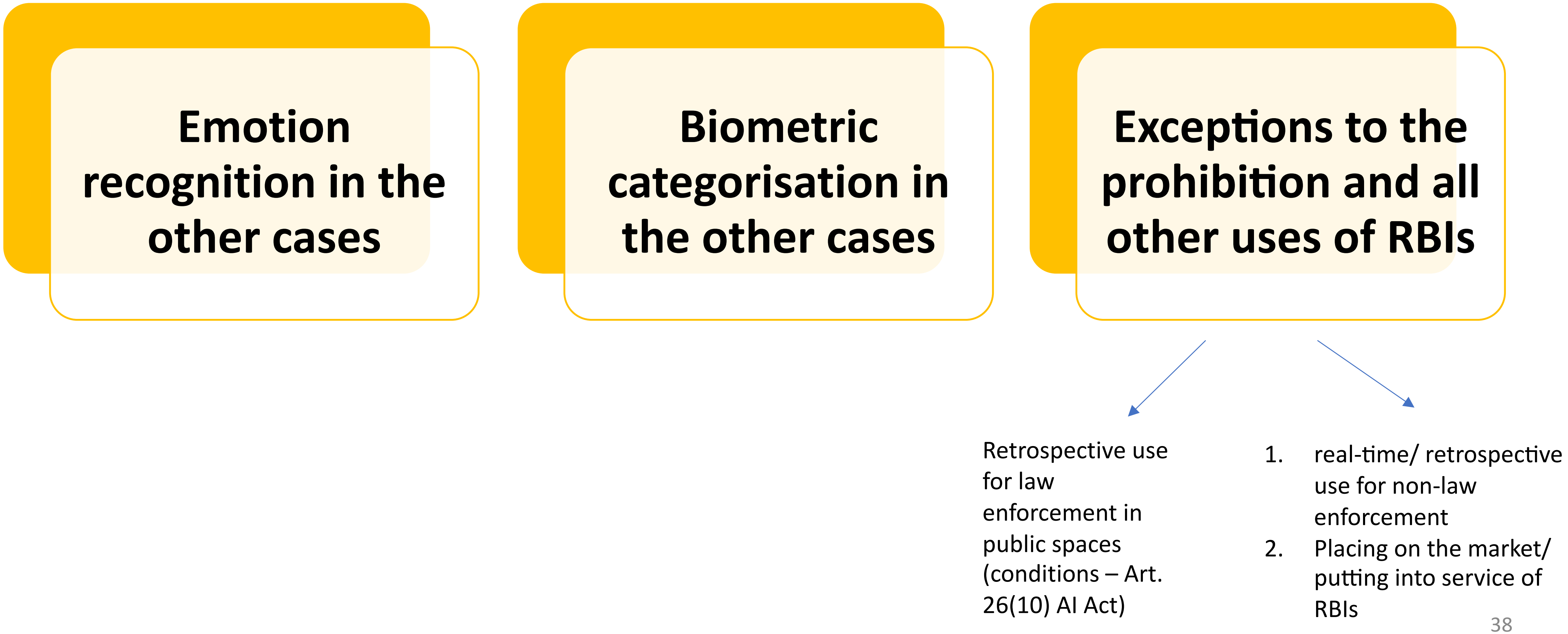
4. When a user uploads a picture, the platform analyses the image, extracts the features and hashed them to **compare** them against existing hashed vectors. Matching images will be shown to the user.

* For more details, see complaint by NOYB to the Austrian Data Protection Authority and by Privacy International to the UK Data Protection Authority (ICO)

Legal issues raised by Clearview AI Practices

1. From a data protection perspective?
2. What about the use of the platform/database by police authorities in the EU?
3. Does the AI Act prohibition cover the practices of Clearview AI?

High-risk systems (Art. 6(2) + Annex III AI Act)



Emotion recognition in the other cases

Biometric categorisation in the other cases

Exceptions to the prohibition and all other uses of RBIs

Retrospective use for law enforcement in public spaces (conditions – Art. 26(10) AI Act)

1. real-time/ retrospective use for non-law enforcement
2. Placing on the market/ putting into service of RBIs

High-risk obligations for actors

Providers

1. Pre/post market **conformity assessment**
2. **Risk management**
3. **Registration** in EU database
4. Specific requirements, further described in ***CEN-CENELEC standards*** currently under development (e.g. human oversight, data governance, cybersecurity risks, accuracy, technical documentation, etc.)

⚠️ *standards not focusing on risks to organisations (traditional role of standards) but on possible risks to individuals*

Deployers

1. **Fundamental Rights Impact Assessment** (for certain deployers, e.g. public sector)
2. **Information** to delivered to impacted persons (e.g. right to explanation of decision-making)
3. **Registration** of AI systems deployed for public sector
4. **Requirements specific to the AI systems**: input data quality and governance, human oversight, record-keeping of logs, etc.

Food for Thought

- AI Act does not supersede the LED rules and other EU legislation
- Rules still need to comply with necessity and proportionality tests and the Charter of Fundamental Rights
- Two coexisting definition of biometric data
- Challenges for the implementation of the exceptions in national law/ criminal procedure
- While Art. 5 applies since 2 Feb. 2025, the provisions relating to non-compliance only apply as from 2 August 2025. But Art. 5 can be enforced by national courts (EC Guidelines)

Many thanks for your attention

Catherine Jasserand, PhD

Assistant Professor, Faculty of Law, STeP, University of Groningen

Affiliated Research Fellow, Faculty of Law, CiTiP, KU Leuven

c.a.jasserand@rug.nl
catherine.jasserand@kuleuven.be