



Tracing Biometrics Between the Lines:

First Guidelines on Prohibited AI Practices under the EU AI Act & More

Abdullah Elbi LL.M., PhD(c), CIPP/E, CIPM

KU Leuven Center for IT and IP Law | PopEye Project

EAB and CITeR Biometrics Workshop, Martigny | 20 May 2025

Biometric Law Lab



KU LEUVEN

CiTIP

CENTRE FOR IT & IP LAW

Centre for IT & IP law

- Research unit of the KU Leuven Faculty of Law and Criminology
- Over 30 years of experience in conducting research on the legal and ethical aspects of technologies
- More than 100 researchers involved in interdisciplinary projects funded by European and national research programmes

CiTIP



Biometric Law Lab

- Focus on **legal & ethical** aspects of various applications of biometric technologies, including, border control, blockchain, eID, the financial sector, law enforcement etc.
- Lead by Professor Els Kindt, and Dr. Catherine Jasserand
- Provides cutting-edge legal research and analysis that empower individuals, organizations, and governments to **responsibly use biometric data** while respecting fundamental rights and freedoms.

Plan

1. **Setting the Scene**
2. **Prohibited Biometric Practices**
3. **More is going on...**
4. **Key takeaways**



Setting the Scene: AI Act Guidelines



- **Consultations** on (1) AI system definition, and (2) Prohibited AI Systems | December 2024
- **Guidelines** published by the EU Commissions / Issued under Article 96 of the AI Act in February 2025
- Offers **practical examples** (**non-exhaustive**) and clarification about the AI Act provisions.
- The guidelines are **not set in stone** and are not binding.
- **More** to come...

For prohibited ones...

→ **Fines:** up to EUR 35 Million or 7% of worldwide annual turnover for the undertaking- whichever is higher. (lowered administrative fines on EU institutions) (**Art. 99 and 100**)

→ **Post-implementation monitoring:** assessing the potential need for possible revision (**Article 112**)

Setting the Scene: Prohibited AI Practices



→ **Unacceptable risk** to fundamental rights and EU values

→ **NO** *'the placing on the market, the putting into service or the use of an AI systems'*

- For biometric ones: 'specific purpose' or only 'the use' → RBIS

→ **Actor-agnostic** prohibitions (limitations through specific context or purpose e.g., RBIs)

→ **Prohibition** in other Union laws remains applicable. (Art. 5(8))

Prohibited AI practices	Provisions
Subliminal, Manipulative and Deceptive technics Exploitation of vulnerabilities	Article 5(1)a Article 5(1)b
Social scoring	Article 5(1)c
Criminal risk prediction and predictive policing	Article 5(1)d
Untargeted scraping of Facial images	Article 5(1)e
Emotion Recognition	Article 5(1)f
Biometric categorization	Article 5(1)g
Remote Biometric Identification Systems(RBIS)	Article 5(1)h, 5(2)-(8)

Untargeted scraping of Facial images



Prohibition: Article 5(1)e

- '...AI systems that **create or expand** facial recognition databases(1) through the **untargeted** scraping of facial images(2) **from the internet or CCTV** footage;'

→ Examples: Permitted or out of scope

- Facial image databases used for **AI model training or testing** purposes, where the persons are not identified.
- AIs which **generate synthetic** images, because no recognition but the transparency requirements of Article 50 AI Act applies.
- Targeted
- Only parts of the face, e.g., scraping the nose or the Iris at the source?
- Research exemption (Article 2(6) and (8))

Emotion Recognition



Prohibition: Article 5(1)f

- ‘...to infer emotions(1) of a natural person in the areas of workplace and education institutions(2), except where the use of the AI system is intended to be put in place or into the market for medical or safety reasons;’

→ Examples:

- Monitoring employee performance + recruitment.
- Tracking student attention or engagement levels | eye tracking software when examining students online to track the fixation point and movement of the eyes
- Using cameras by a supermarket or a bank to track its employees' emotions | to detect suspicious customers,
- Using voice recognition systems by a call centre to track their employee's emotions | to track their customers emotions



Biometric Categorisation

Prohibition: Article 5(1)g

- ‘...categorise individually(1) natural persons based on their biometric data(2) to deduce or infer their race, political opinions, trade union membership, religious or philosophical beliefs, sex life or sexual orientation(3); this prohibition does not cover any labelling or filtering of lawfully acquired biometric datasets(1), such as images, based on biometric data or categorising of biometric data in the area of law enforcement(2)’

→ Examples:

- **Inferring** political leanings from facial images
Cambridge Analytica-like practices (deducing political or religious orientation)
- Identifying **sexual orientation** through voice analysis.
- **Fairness in hiring algorithms**: Labelling (e.g. by ethnicity) can help prevent discriminatory outcomes
- **Medical Diagnosis Support**
- **Filters on social media**

→ **Exceptions** (1), (2) and **Ancillary services** linked to another commercial service (Recitals 16, 30)

Real-time Remote Biometric Systems(1/2)

Prohibition: Article 5(1)h

- 'The use of '*real-time*'(1) remote biometric identification systems(2) in *publicly accessible spaces* (3) for the *purposes of law enforcement* (4) [...]

Exceptions: Article 5(1)h(i), (ii), (iii)

- **Targeted** search of victims / missing persons
- Preventing **imminent threats** to life/physical safety or **terrorist attacks**
- Identification of localisation of suspects of identified **serious crime**

→ Procedure and safeguards (Art. 5(2)-Art. 5(8) AI Act) including recipe for national laws

Real-time Remote Biometric Systems (2/2)

→ Examples:

- **Requests/instructions by law enforcement** to banks, transport firms, or sports federations → might trigger obligations under AI Act. **Metro access systems (e.g. biometric metro tickets)** - **Not covered, as users voluntarily interact with the system.**
- **Chatrooms, social media, online platforms** - **Out**
- **Prisons and border control** - **Not publicly accessible** → **exempt from RBI ban.** **Airports** - **Dual functions** → **may require case-by-case assessment.**
- **Identifying shoplifters** via RBI and comparing to criminal databases → **Prohibited** (see Annex II)
- **Mobile CCTV cameras equipped with AI-FRT** on a police van around the stadium- **Prohibited** if *unspecific and is not linked to the event of the football match*

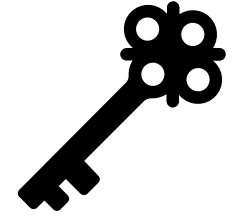
More is going on... [1/4]

Recital 54 of the AI Act:

prohibited under this Regulation, and emotion recognition systems that are not prohibited under this Regulation, should be classified as high-risk. Biometric systems which are intended to be used solely for the purpose of enabling cybersecurity and personal data protection measures should not be considered to be high-risk AI systems.

- **No reference** elsewhere. This might refer to Presentation Attack Detection, Morphing Attack Detection, Deepfake Attack Detection...
- See the result of the [EU Horizon iMARS Project](#)

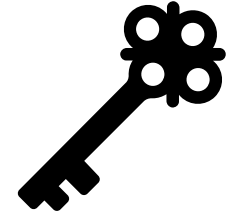
More is going on... [2/4]



Bavarian Data Protection Authorities' Worldcoin [Decision](#) | December 2024

- "Orb" device scans → biometric iris codes → identity verification
- Violations of **data security**(due to plaintext iris code storage), **unlawful** biometric data processing (lack of explicit consent), no option for **right to erasure**
- **Privacy-enhancing** technologies, such as Secure Multi-Party Computation (SMPC) are not sufficient to make data anonymous.
- Enforcement measures (including mandatory erasure of data) and penalties are introduced. More to come...

More is going on... [3/4]



Datatilsynet SALT AI Sandbox [Report](#) | January 2025

- Assess legal and technical challenges in Mobai's **SALT** solution: a privacy-preserving facial biometric system for eID verification using **homomorphic encryption**.
- *Biometric templates (even encrypted) are likely personal/biometric data under the GDPR.*
- Also analysed, primary and secondary **purposes** of the data processing, **central/cloud storage of biometrics** (the necessity and proportionality must be justified.)
- The NDPA **sees its potential in enhancing the security of encrypted data**, as well as its potential use in other areas that can benefit from **analysing and processing data while preserving confidentiality**.

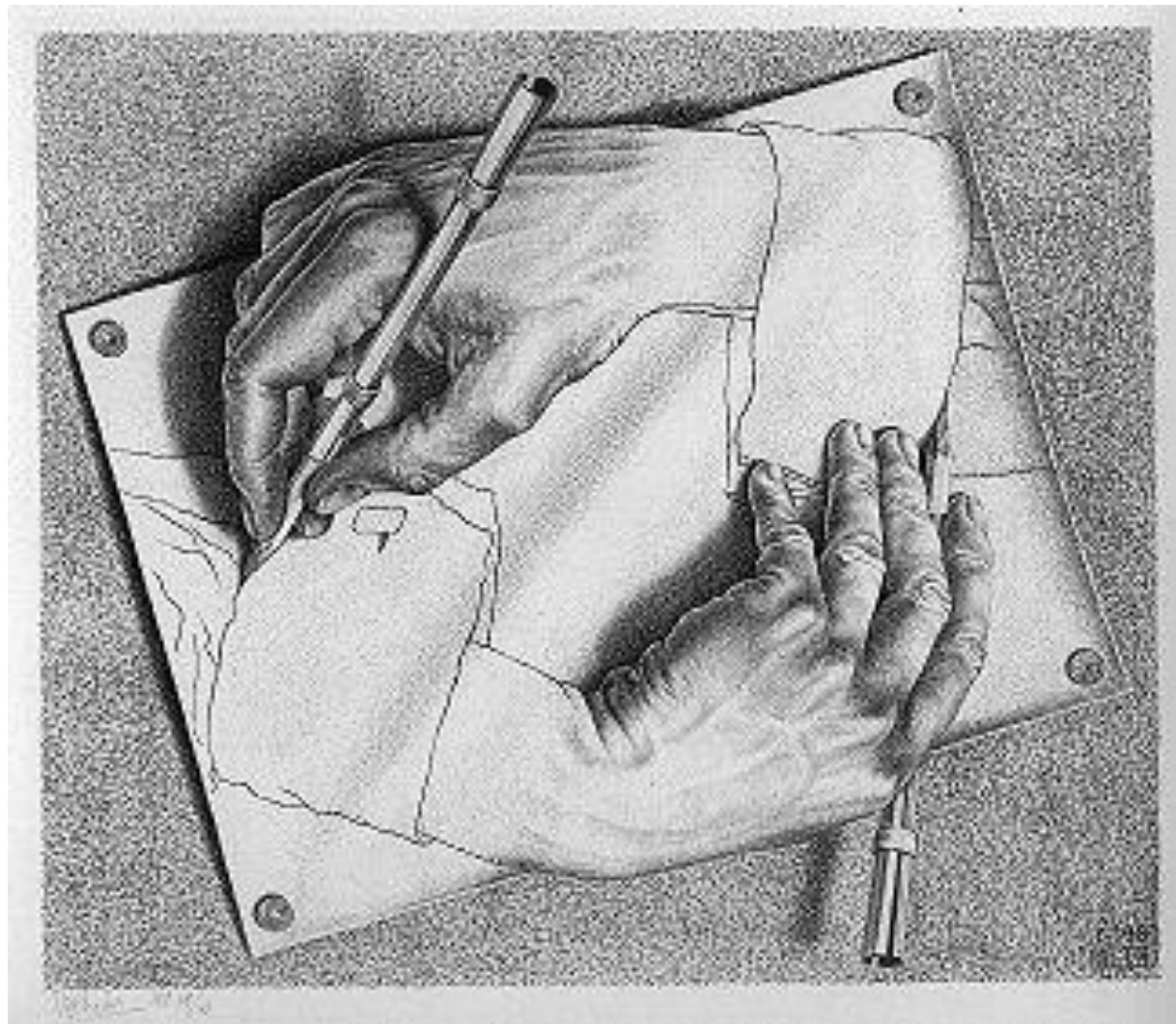
More is going on... [4/4]

The [Codes of Practice](#)(1) and Guidelines(2) for General-Purpose AI (GPAI) models | by August 2025

- The guidelines are not **binding**.
- The AI Act and its Codes of Practice require GPAI/foundation model providers to assess these **risks**, document data sources, and **prevent** misuse. **Transparency** about capabilities and constraints together with copyright is critical.
- Code of practice, if **approved** by AI Office and the Board may **reduce administrative burden** for providers and serve as a benchmark for regulatory compliance.
- The [consultation](#) is open until May 22 2025.

Key takeaways

- **No**, legal aspects of biometrics in the EU have not been resolved.
- Keep track of the **growing** corpus of case law, regulations and guidelines, DPA decisions
- Also, **technological developments-SOTA**...(e.g., SMPC or FHE)
- **AI literacy** is crucial, and also a need for **collaboration** among experts (keep the **legal** team in the loop)



“Drawing Hands”

M. C. Escher

1948

<https://mcescher.com/gallery/back-in-holland/#>

Thank you for your attention!



Abdullah Elbi
Legal Researcher- LinkedIn
KU Leuven CiTiP
Abdullah.elbi@kuleuven.be

This work is supported by:

- The European Union's Horizon 2020 research and innovation programme under the **PopEye** project.
- The Norwegian Research Council-funded **SALT** project.

