Facial recognition in healthcare: Doctor, take a look at me

Vera Lúcia Raposo (黎慧華)

Faculdade de Direito, Universidade de Coimbra /Faculty of Law, Coimbra University

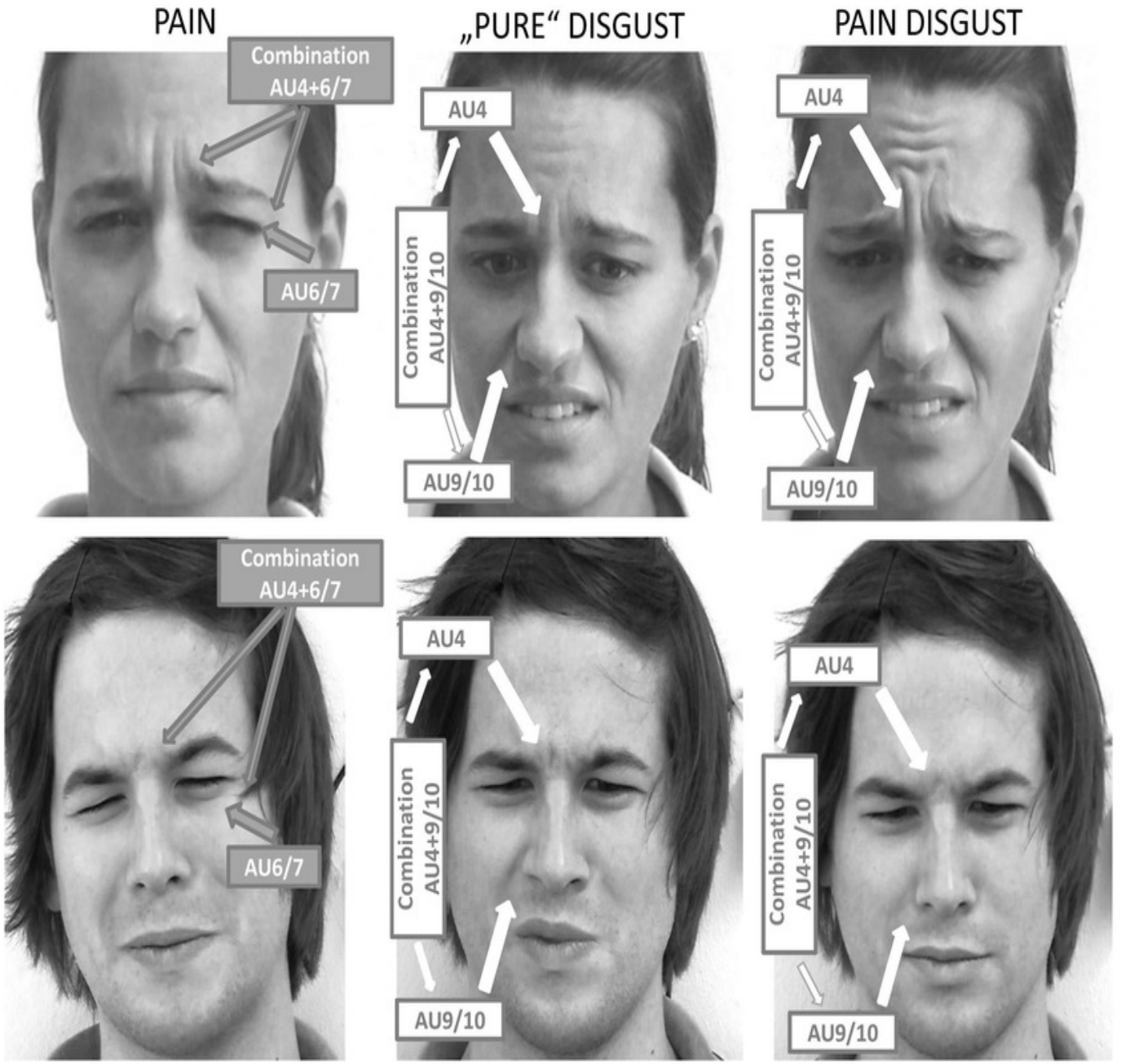
vera@fd.uc.pt

Possible uses of FRT in healthcare

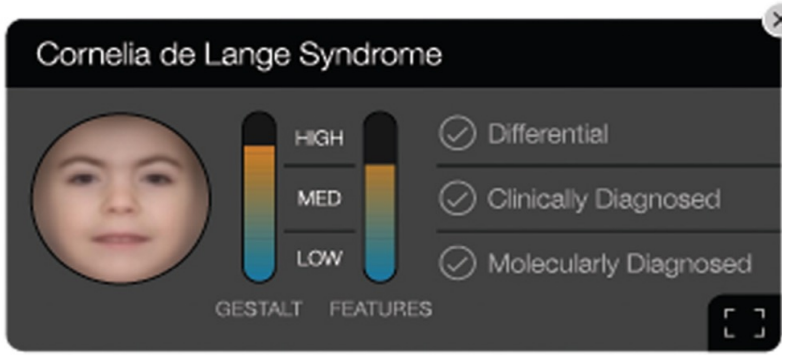
Facial characterisation

To impute reactions and feelings to a person by analysing the face and its micro-expressions.

- ✓ To track how patients react to physical and emotional pain (the case of doctor's burnout)
- ✓ Confirm that the patient took the medication
- ✓ Monitor outpatients (smartphone scan)
- ✓ Help patients with an autism spectrum disorder recognize emotions in others



Diagnose of medical conditions



- ✓Identification of rare genetic conditions (diagnose autism spectrum disorders, Cushing's syndrome, Cornelia de Lange syndrome)
- ✓Identification of more common medical conditions (the 'health mirror' as a tool of telemedicine).
- ✓Prediction of risk factors: smoking (wrinkles around the mouth); alcoholism (larger nose); excessive exposure to the sun (brown spots and wrinkling)

Identification of a person

Authentication/verification (confirming that the person is whom he/she claims to be)

Identification/recognition (confirming that the person is whom we believe he/she is).

- Patient check-in: patients facing difficulties communicating (unconscious patients, children, elderly patients, patients with mental incapacities)
- Prevent preventing identity theft
- Track the patient medical record
- Give the patient access to health information (medical exams, medical files)
- Avoid mistaken identities, namely in urgent situations and/or when the patient is in an unconscious state.
- Control entries: access to places considered restricted areas (patients, relatives, health staff)
- Exit control: patients with mental diseases, children (baby kidnapped)

Legal challenges in the EU

Compliance with data protection norms (GDPR)

Biometric data

Personal data

Sensitive data

The legal ground for data processing

Legal ground for data processing

Personal data (Article 6 GDPR)

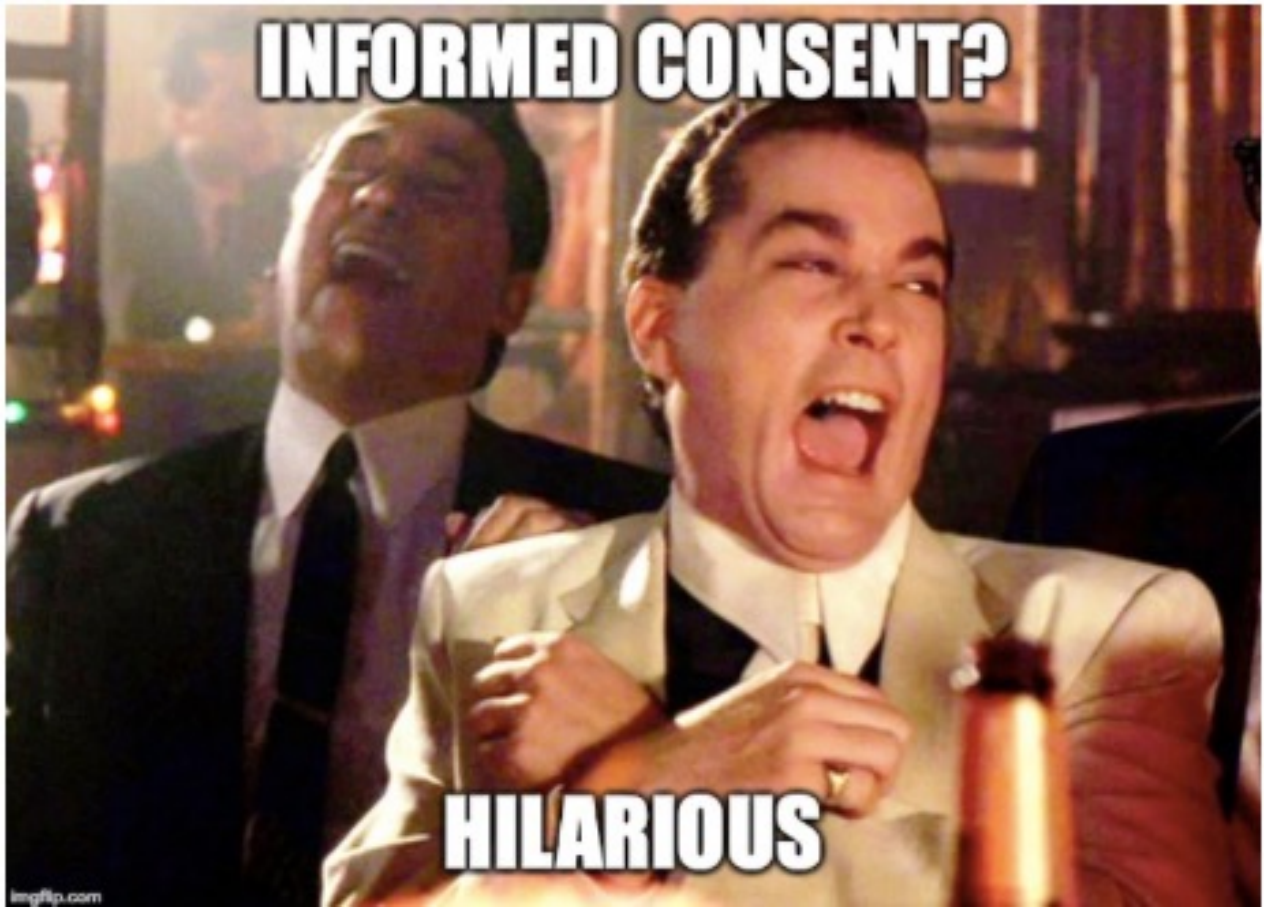
+

Sensitive data (Article 9 GDPR)

Consent?

- What to collect consent from unknown individuals?
- How to obtain an affirmative action for consent?
- How to comply with information requirements?
- How to demonstrate consent was collected?

The issue of voluntariness



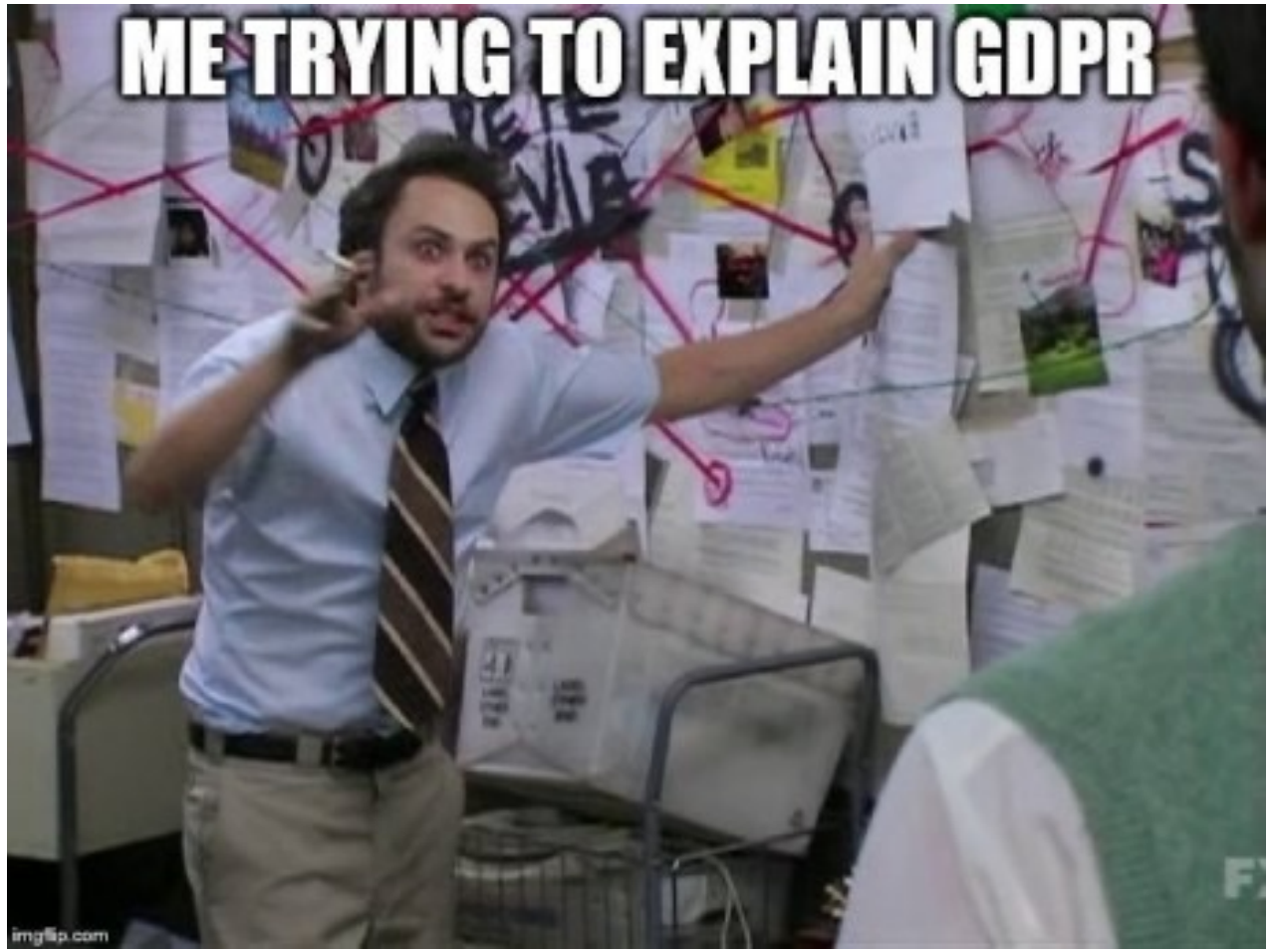
When FR is a mechanism used to provide medical care

- Article 6/1/b (performance of a contract),
- 6/1/d and 9/2/c (protection of vital interests of the data subject),
- 9/2/h (preventive or occupational medicine).

When medical care is not involved:

- The legitimate interest ground, as set forth in Article 6/1/f.

Want about article 9?



Compliance with the Medical Devices Regulation

Article 2(1) MDR ‘instrument, apparatus, appliance, software, implant, reagent, material or other article’

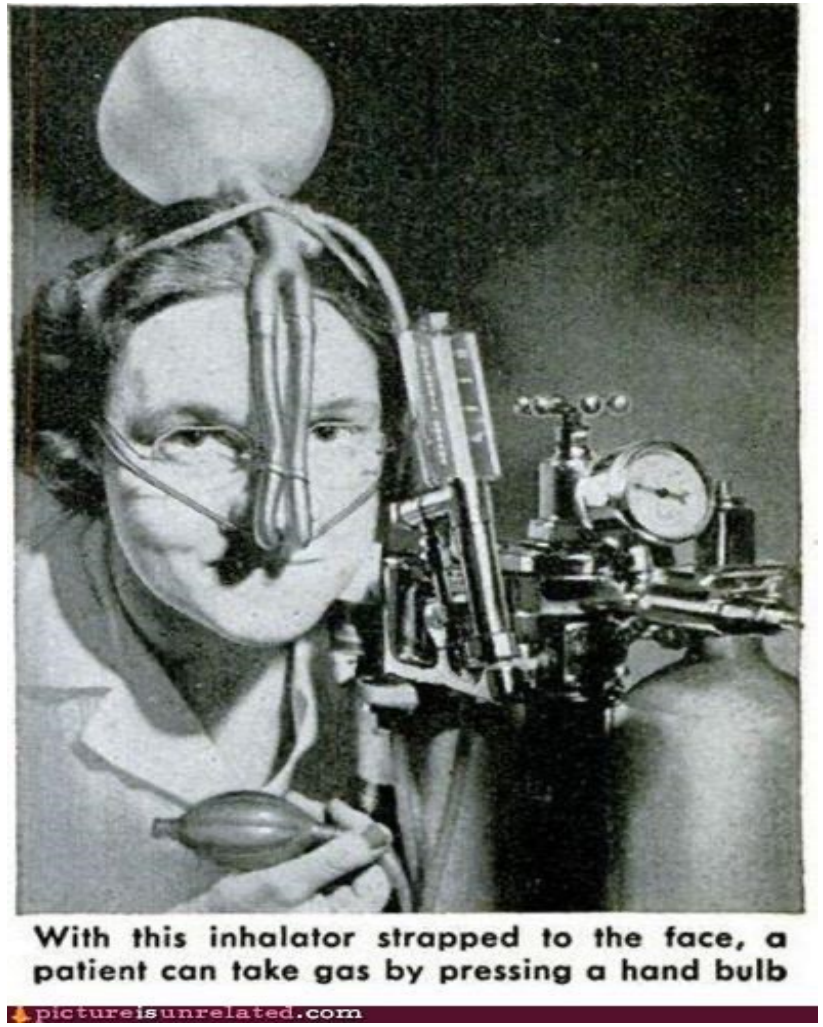
↓

Aimed for any of the very broad list of purposes

↓

When FR is used to provide healthcare, it can be considered a medical device

Compliance with the Medical Devices Regulation



A conformity assessment (Articles 2(40) and 52 of the MDR) is required before the device is launched into the market

demonstrating that the requirements (General Safety and Performance Requirements -GSPRs) are fulfilled.

Only a positive assessment allows the CE marking of conformity (Article 20 of the MDR).

Article 51 of the MDR: different classes of medical devices, according to the respective level of risk: I, IIa, IIb and III.

Rule 11 of the MDR

As a rule, software will be considered class IIa. However:

- when those medical decisions can lead to '*serious deterioration of a person's state of health or a surgical intervention*' - class IIb.
- when the medical decisions are taken based on that software can lead to '*death or an irreversible deterioration of a person's state of healt*h' - class III

FR to monitor the presence and intensity of pain:

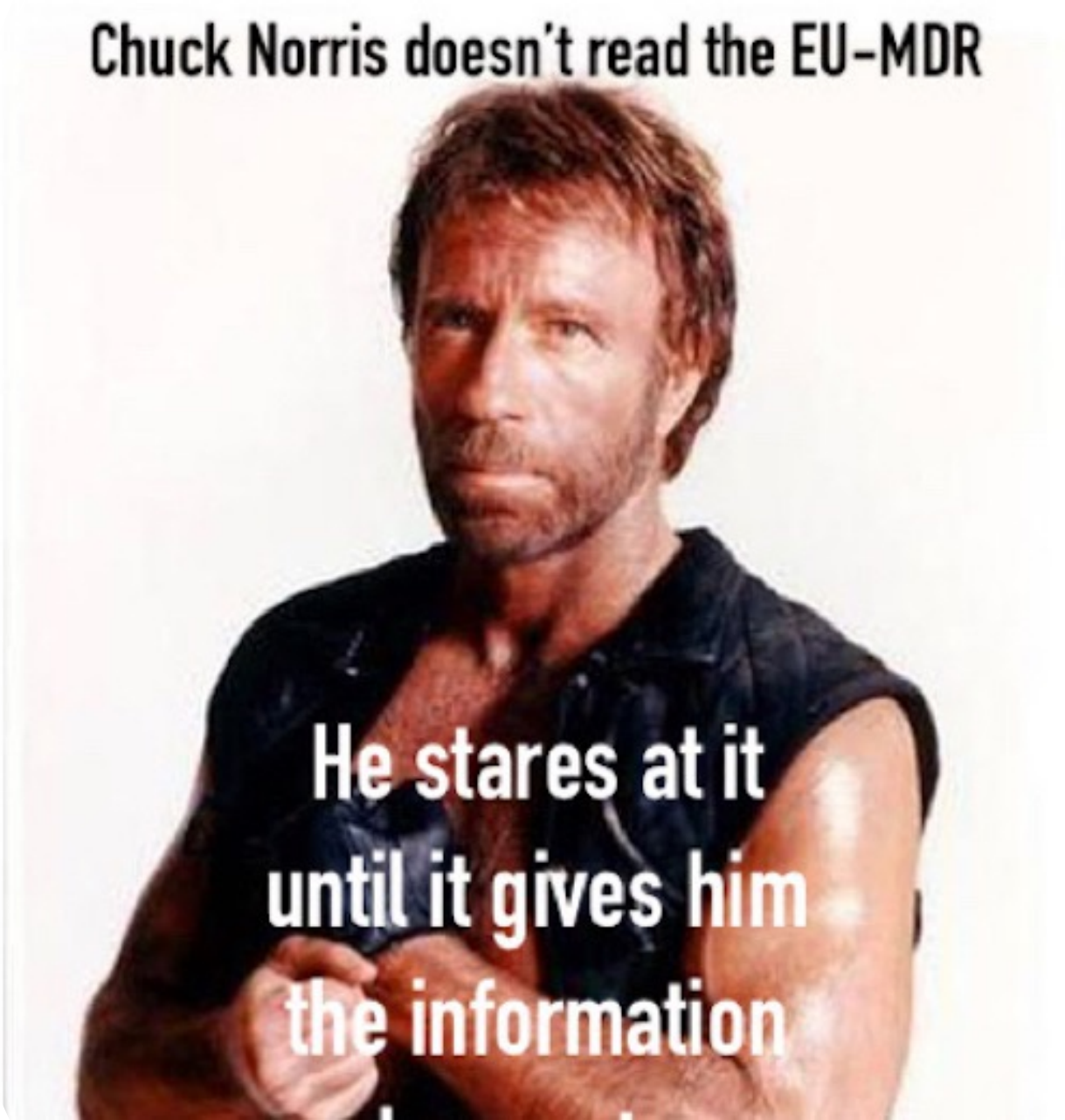
- software intended to 'monitor physiological processes' - class IIa
- unless some forms of pain are considered 'vital physiological parameters, where the nature of variations of those parameters is such that it could result in immediate danger to the patient' - class IIb

The intervention of notified bodies: for class IIa devices and higher (and some class I devices)

Facial recognition as a medical device

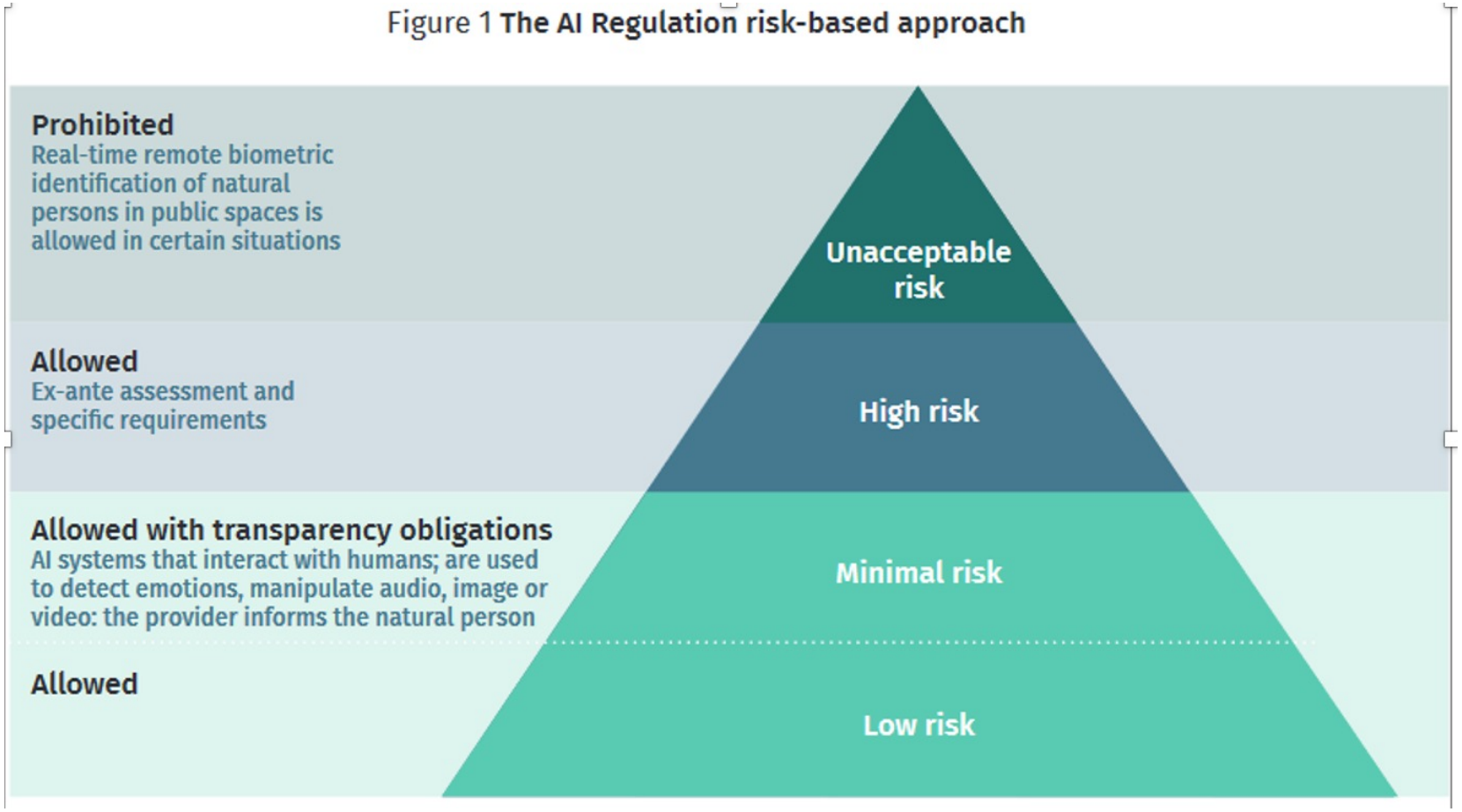
↓

Legal complexity



Compliance with the future AI Regulation

Figure 1 **The AI Regulation risk-based approach**



The kind of uses envisaged in healthcare settings are allowed, as high-risk technology.

The classification as high risk can be justified in two ways:

- FR used for medical purpose is a medical devices (Article 8 and point 11 and 12 of Annex II of the Draft Act)
- FR intended for the ‘‘real-time’ and ‘post’ remote biometric identification of natural persons’ can have an adverse impact on people’s safety and/or their fundamental rights (Recital 33, Article 6(2) and Annex III, point 1(a) of the Draft Act)

Ex-ante control

Conformity assessment: precondition for the grating of the CE marking of conformity (commercialisation):

- ✓ Systems of risk assessment and risk mitigation;
- ✓ use high-quality datasets to train the system;
- ✓ maintain regular activity logs to allow traceability;
- ✓ provide users with sufficient information;
- ✓ assure human oversight;
- ✓ guarantee the robustness, security and accuracy of the system;
- ✓ keep detailed documentation to allow authorities to allow the authorities in charge to assess compliance with the legal requirements

The same assessment as for medical devices?

Ex post control

Reporting of serious incidents and malfunctions by providers of high-risk AI systems (article 61 of the Draft Act).

Control carried out by market surveillance authorities (Article 65 of the Draft Act),

Ultimately, the ex-post control can lead to the withdrawal of the AI system from the market.

The current legal scenario is too complex

- Potential overlaps (conformity assessment)
- Conflicting requirements ('complete datasets' and the GDPR).

A legal puzzle, where not all pieces fit together, is a legal hurdle for developers and users, and might undermine its use in healthcare.

Vera Lúcia Raposo (2022) (Do not) remember my face: uses of facial recognition technology in light of the general data protection regulation, Information & Communications Technology Law, DOI: 10.1080/13600834.2022.2054076

Vera Lúcia Raposo (黎慧華)

Faculdade de Direito, Universidade de Coimbra /Faculty of Law, Coimbra University

vera@fd.uc.pt

https://www.linkedin.com/in/vera-l%C3%BAcia-raposo-9a000822/

Twitter: @Vera_Lucia_Rap